ACTUALIDAD JURIDICA IBEROAMERICANA

IDIBE
Instituto de Derecho Iberoamericano

tirant lo blanch

Cátedra de Derecho Notarial de la Universidad de Alicante

ACTUALIDAD JURÍDICA IBEROAMERICANA / EDICIÓN SEMESTRAL / AGOSTO 2024 / VALENCIA-ESPAÑA

Publicación de circulación Internacional
Actualidad Jurídica Iberoamericana
https://www.revista-aji.com

Editan:
Instituto de Derecho Iberoamericano.
C/ Luis García Berlanga, núm. 7, 1-15 Valencia, España. 46023.
Correo Electrónico: contacto@idibe.org
web: www.idibe.org

Tirant lo Blanch.
C/Artes Gráficas, 14, 46010 Valencia (España).
Telf. +34 963 61 00 48.
Correo electrónico: tlb@tirant.com
web: www.tirant.com

ISSN 2386-4567

Actualidad Jurídica Iberoamericana se encuentra indexada en los siguientes índices de calidad: SCOPUS (Q3), CIRC ("B"), ANVUR (clase "A"), RRDe (Q1), IDR (C3), LATINDEX y MIAR.

Así mismo se encuentra incluida en los siguientes catálogos: Dialnet, RODERIC, Red de Bibliotecas Universitarias (REBIUN), Ulrich's, Dulcinea, Elektronische Zeitschriftenbibliothek (EZB) y Ores Scientific Plattaform.

Impreso en España
Diagramación: Elias On - elias.on@live.com

SUMARIO

21

DIGITALIZACIÓN Y ALGORITMIZACIÓN DE LA JUSTICIA: NUEVOS RETOS, DESAFÍOS Y OPORTUNIDADES

Directoras: Ana Montesinos y Diana Marcos

PARTE II: ALGORITMIZACIÓN DE LA JUSTICIA E INTELIGENCIA ARTIFICIAL

RECENSIONES

D. Jesús Palomares Bravo
Investigador Predoctoral en Departamento de Derecho Civil, Universidad de Málaga, España

Dra. Carla Pernice
Ricercatore di Diritto dell'Economia, Universidad Luigi Vanvitelli, Italia

Dr. Rosario Petruso
Professore Associato di Diritto Comparato, Universidad de Palermo, Italia

Dra. Monica Pucci
Assegnista di ricerca, Università degli Studi di Perugia, Italia

Dra. Isabel Rabanete Martínez
Profesora Ayudante Doctora de Derecho Civil, Universidad de Valencia, España

Dr. Marco Rizzuti
Ricercatore di Diritto Privato, Universidad de Florencia, Italia.

D. Juan Carlos Rocha Valle
Notario y Defensor Público en el área del Derecho Civil, Nicaragua

Dr. Valerio Rotondo
Professore Associato di Diritto Privato, Universidad de Molise, Italia

Dra. Romina Santillán Santa Cruz
Profesora Ayudante Doctora de Derecho Civil, Universidad de Zaragoza, España

Dr. Eduardo Taléns Visconti
Profesor Titular de Derecho del Trabajo,Universidad de Valencia, España

Dra. Maria Inês Viana de Oliveira Martins
Professora Auxiliar na Facultade de Direito, Universidad de Coimbra, Portugal

Dr. Calogero Valenza
Assegnista di Ricerca, Università de La Sapienza, Italia

Dra. Sara Zubero Quintanilla
Profesora Contratada Doctora de Derecho civil, Universidad Complutense de Madrid, España

PRESENTACIÓN

Para nosotras es un honor poder presentar este número monográfico de la revista Actualidad Jurídica Iberoamericana, titulado "Digitalización y algoritmización de la justicia: nuevos retos, desafíos y oportunidades". Y lo es por dos motivos. El primero de ellos es que es fruto del Congreso Internacional "Digitalización y algoritmización de la justicia: nuevos retos, desafíos y oportunidades", celebrado con un rotundo éxito los días 26 y 27 de octubre del pasado año 2023 en la Universidad Católica de Valencia "San Vicente Mártir" con la intervención de un gran número de destacados expertos en la materia. Y el segundo es que alberga los últimos resultados de la investigación llevada a cabo en el seno del Proyecto "Claves para una justicia digital y algorítmica con perspectiva de género" (expediente: PID2021-123170OB-I00), financiado por el Ministerio de Ciencia e Innovación, en la medida en que en dicho Congreso participaron los integrantes del mencionado equipo.

Ya sea en forma de Congreso Internacional o de Proyecto nacional, para nosotras es un orgullo haber liderado un grupo de tan excelentes investigadores de los que tanto hemos aprendido, con los que nos unen lazos académicos y cada vez más lazos personales, y con los que hemos tenido la ocasión de compartir gratificantes experiencias académicas. Un grupo caracterizado por su internacionalidad e interdisciplinariedad, integrado por miembros de universidades españolas (Universitat de València, Universidad Católica de Valencia, Universidad del País Vasco, Universidad de Córdoba) y extranjeras (Universidad de Leicester, Universidad Central de Chile, Universidad de Kobe y Universidade Federal do Espírito Santo). Estamos enormemente satisfechas de todo lo realizado y de lo que, con toda seguridad, se desarrollará en la duración restante del Proyecto con igual éxito.

Nos gustaría igualmente destacar la participación de aquellos relevantes juristas que tanto saben sobre digitalización e inteligencia artificial y que, aunque no pertenecen al mencionado Proyecto, han hecho un esfuerzo para participar en el presente monográfico. Entre ellos figura quien fue nuestra Directora de tesis, la tan apreciada Dra. Silvia Barona Vilar, junto a Lorenzo Cotino Hueso, Adrián Palma Ortigosa, Juan José Castelló Pastor, Rosa Cernada Badía, Marina Sancho López y Marta Cantos Pardo.

La obra, de carácter interdisciplinar (procesal, administrativo, constitucional, internacional y civil), se compone de veintitrés excelentes trabajos con un denominador común: el elemento digital o empleo de medios electrónicos en el ámbito de la justicia. Mientras diez de las obras tratan la digitalización de esta,

el resto analiza el uso de la disruptiva inteligencia artificial. Y dichos estudios se efectúan a la luz de las más recientes normas sobre la materia, como son:

1) En España, el Real Decreto-ley 6/2023, de 19 de diciembre, por el que se aprueban medidas urgentes para la ejecución del Plan de Recuperación, Transformación y Resiliencia en materia de servicio público de justicia, función pública, régimen local y mecenazgo, que introduce -por lo que ahora interesa destacar- trascendentales medidas de fomento y uso de las tecnologías de la información y comunicación e inteligencia artificial en el ámbito de la Administración de Justicia. Dicho Real Decreto-ley ha sido convalidado por el Pleno del Congreso de los Diputados el 10 de enero del presente año y, tras acordarse por mayoría, está siendo tramitado como Proyecto de Ley por el procedimiento de urgencia.

El mencionado Real Decreto-ley 6/2023 constituye una revolución procesal para la ciudadanía desde el punto de vista de la justicia digital, que ha sido abordada, con carácter general, por María José Catalán Chamorro y Miren Josune Pérez Estrada y, en particular, en lo que al carácter electrónico del primer emplazamiento o citación del demandado se refiere, por Diana Marcos Francisco. Y siendo importante el empleo de medios electrónicos en los distintos órdenes jurisdiccionales, no podemos descuidar sistemas de ODR inexplorados como los empleados para resolver conflictos derivados de contratos ilícitos en los mercados de la *Dark Web*, que de forma innovadora analiza Pablo Cortés.

2) Y, en el ámbito de la Unión Europea, destacan:

2.1) El Reglamento (UE) 2020/1784, del Parlamento Europeo y del Consejo de 25 de noviembre de 2020, relativo a la notificación y traslado en los Estados miembros de documentos judiciales y extrajudiciales en materia civil o mercantil ("notificación y traslado de documentos"), y su contribución al impulso de la digitalización de la cooperación judicial en materia civil o mercantil en la Unión Europea (vid. obra de Guillermo Palao Moreno);

2.2) La Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas para prevenir y combatir el abuso sexual de los menores (COM/2022/209 final) (vid. obra de Elena de Luis García)

2.3) Y la Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión (COM/2021/206 final), cuyo texto consensuado ha sido aprobado por el Parlamento Europeo en primera lectura el 13 de marzo y al que, aún más recientemente (21 de mayo), acaba de dar luz verde el Consejo.

En esta sede son reseñables las obras que versan sobre el uso de sistemas de inteligencia artificial de identificación biométrica (vid. obras de Silvia Barona Vilar y José Francisco Etxeberria Guridi), sobre el uso de dicha inteligencia en el marco establecido por el Real Decreto-ley 6/2023 (y su actual modificación en el Congreso), en relación con el Anexo III del citado Reglamento de Inteligencia Artificial respecto de la justicia (vid. obra Lorenzo Cotino Hueso), sobre la autoridad notificante y los organismos notificados del repetido Reglamento (vid. obra Adrián Palma Ortigosa), así como el resto de obras que, desde distintos prismas, abordan el estudio de la inteligencia artificial.

Y adviértase que entre tales trabajos no falta la perspectiva comparada (vid. los artículos de Takuya Hatta, que analiza la respuesta japonesa a la digitalización de la justicia civil; Valesca Raizer, que presenta la "Guia de Boas Práticas para a Cooperação Jurídica Internacional para as Américas" en la era digital, y Pablo Contreras, que trata la regulación de la inteligencia artificial en América Latina). También se aborda el estudio de la posible aplicación de inteligencia artificial para afrontar importantes problemas sociales o aminorar sus efectos, tales como la violencia de género (vid. obras de Ana Montesinos García y Raquel Borges Blázquez) incluso en el Metaverso (vid. estudio de Elisa Simó Soler y Hernán López Hernández), la trata de personas (vid. trabajo de María Barraco) u otras dificultades que sufren diferentes colectivos vulnerables (vid. obras de Ana Isabel Blanco García y Sebastian Bozzo Hauri y Juan Carlos Vidal Rojas). Ello constituye una muestra de la imprescindible sensibilización y toma de conciencia por los problemas sociales y búsqueda de soluciones.

El criterio en que nos hemos basado para estructurar las aportaciones es la distinción entre obras atinentes al empleo de medios digitales y las que abordan el estudio de algoritmos y sistemas de inteligencia artificial, ordenadas a su vez por orden alfabético.

No pueden faltar nuestros agradecimientos al Doctor De Verda por su confianza y la oportunidad de publicar las conferencias, ponencias y otras obras en esta prestigiosa Revista.

Para acabar, y como no podía ser de otra forma, reiteramos nuestros agradecimientos a todos los participantes en esta obra monográfica -con aportaciones pioneras en el marco de las citadas nuevas normas-, sin quienes no habría sido posible: ¡muchas gracias a todos y a todas!

Ana Montesinos y Diana Marcos
Valencia, 29 de mayo 2024.

PARTE I:
DIGITALIZACIÓN DE LA JUSTICIA

LA REVOLUCIÓN PROCESAL PARA LA CIUDADANÍA TRAS EL RDL 6/2023 A TRAVÉS DE LAS APLICACIONES DE LA ADMINISTRACIÓN DE JUSTICIA DIGITAL*

THE PROCEDURAL REVOLUTION FOR CITIZENS AFTER RDL 6/2023 THROUGH THE APPLICATIONS OF THE DIGITAL ADMINISTRATION OF JUSTICE

Actualidad Jurídica Iberoamericana Nº 21, agosto 2024, ISSN: 2386-4567, pp. 16-41

* Estudio redactado en el marco del Proyecto "Claves para una justicia digital y algorítmica con perspectiva de género", PID2021-123170OB-I00 financiado por MCIN/ AEI/10.13039/501100011033.

María José
CATALÁN
CHAMORRO

ARTÍCULO RECIBIDO: 29 de mayo de 2023
ARTÍCULO APROBADO: 1 de julio de 2024

RESUMEN: La irrupción del Real Decreto 6/2023 ha tenido un impacto sin precedentes en la vida jurídica de la ciudadanía. Por un lado, le da carta de naturaleza a aplicaciones informáticas preexistentes, a las que se le aumentan funcionalidades y se les reviste de legalidad. Y, por otro lado, se mejora el acceso a la justicia de la ciudadanía de manera telemática. Sin embargo, quedan retos por superar de los que se tendrá que ocupar el CTEAJE como es la eterna problemática de la interoperabilidad entre los sistemas.

PALABRAS CLAVE: Justicia electrónica, acceso a la justicia, carpeta ciudadana, sede judicial electrónica, datos en justicia.

ABSTRACT: *The introduction of Royal Decree 6/2023 has had an unprecedented impact on the legal life of citizens. On the one hand, it gives a legal status to pre-existing computer applications, but increases their functionalities and gives them a legal status. On the other hand, it improves citizens' access to justice electronically. However, there are still challenges to overcome that the CTEAJE will have to deal with, such as the eternal problem of interoperability between systems.*

KEY WORDS: *E-justice, access to justice, citizen's wallet, electronic judicial office, data in justice.*

I. INTRODUCCIÓN.

El pasado 20 de diciembre de 2023 los operadores jurídicos fuimos sorprendidos por la publicación en el BOE del Real Decreto-ley 6/2023, de 19 de diciembre, por el que se aprueban medidas urgentes para la ejecución del Plan de Recuperación, Transformación y Resiliencia en materia de servicio público de justicia, función pública, régimen local y mecenazgo. También denominado por la prensa como Real Decreto ómnibus debido al gran número de normas que vino a modificar.

No obstante, el área del Derecho más afectada por este Real Decreto ha sido el Derecho Procesal ya que ha modificado más de una centena de artículos de la Ley de Enjuiciamiento Civil y más de una treintena de la Ley de Enjuiciamiento Criminal. Además de producir profundas modificaciones en la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, en la Ley 36/2011, de 10 de octubre, reguladora de la jurisdicción social y en varios artículos de la Ley 15/2015, de 2 de julio, de la Jurisdicción Voluntaria e incluso modificar preceptos de la jurisdicción militar.

Todo ello, sin dejar atrás los grandes cambios que esta norma supone para la oficina judicial y el personal que en ella trabajan. Debido principalmente a la instauración de la celebración telemática de manera preferente y genérica de todos los actos procesales. Esto ha revolucionado los formatos de los procesos a golpe de Real Decreto.

En este sentido, debemos hacer referencia a la herramienta normativa por la que ha optado el ejecutivo, que como podemos fácilmente advertir ha sido mal utilizada, ya que la urgencia de la entrada en vigor de estos cambios tan trascendentales para el ordenamiento jurídico español es difícilmente defendible políticamente e inexplicables jurídicamente. Sin embargo, el ejecutivo ha preferido aprobar in extremis y por la mínima una norma trascendental para la justicia en los próximos años por la vía de la urgencia y sin debatir su contenido y términos en las Cortes Generales con los consecuentes errores que la misma contiene[1].

1 Ver, por ejemplo: Fierro Rodríguez, D.: "En busca del perdido apartado 5 del artículo 169 de la Ley de Enjuiciamiento Civil según el Real Decreto- ley 6/2023", *Diario LA LEY*, 14 de febrero de 2024, núm. 10446,

• María José Catalán Chamorro
Profesora. Ayudante Doctor de Derecho procesal, Universidad de Córdoba. Correo electrónico: maria.jose.catalan@uco.es

Así las cosas, podemos decir que nos encontramos ante una tormenta perfecta que ha hecho convulsionar la realidad jurídica de todos los juzgados y tribunales de nuestro país.

Si bien, a pesar de la trascendencia de las reformas introducidas en la LEC y en la LECrim, en el presente trabajo nos centraremos en la parte inicial de la norma, en el libro primero, sobre todo en lo referente a las Medidas de Eficiencia Digital y Procesal del Servicio Público de Justicia que ocupan aproximadamente una centena de artículos. Y que relacionaremos con la realidad actual de los juzgados y las aplicaciones informáticas puestas en marcha por el servicio público de justicia a las que esta norma viene a refrendar legislativamente y su relevancia para el acceso a la justicia de la ciudadanía. No estudiaremos, por tanto, las tan interesantes Medidas de Eficiencia Procesal del Servicio Público de Justicia -correspondientes al Título VIII del Libro I de la norma- debido a la necesidad de concreción del presente trabajo y donde se modifican las diferentes leyes procesales para armonizar la regulación procesal civil, penal, contencioso-administrativa y social con el contexto de la tramitación electrónica, aunque veremos algunos matices de estas reformas.

En definitiva, en el presente trabajo intentaremos descifrar los primeros artículos del Real Decreto 6/2023 poniéndole nombre a cada aplicación que lo desarrolla y conociendo la trascendencia de su contenido para la vida diaria de millones de ciudadanos españoles.

1. Contexto.

Tras la caducidad de los tres proyectos de Ley impulsados por el anterior ejecutivo -recordemos Proyecto de Ley de medidas de eficiencia procesal del servicio público de Justicia, Proyecto de Ley de Medidas de Eficiencia Digital del Servicio Público de Justicia y el Proyecto de Ley Orgánica de eficiencia organizativa del servicio público de Justicia, por la que se modifica la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, para la implantación de los Tribunales de Instancia y las Oficinas de Justicia en los municipios[2]-. Y que a pesar de que las negociaciones y el debate de los proyectos se encontraban en un estadio avanzado, se vieron varados debido a la abrupta convocatoria de elecciones generales. Esta triada de proyectos, enraizados en el ambicioso Plan de Justicia 2030 intentaron modernizar el sistema de la Administración de justicia y crear al mismo tiempo una justicia

Sección Tribuna.

2 Ref. 121/000097, Publicado en el Boletín Oficial De Las Cortes Generales, Legislatura XIV, Serie A: Proyectos De Ley 22 de abril de 2022.
Ref. 121/000116 Publicado en el Boletín Oficial De Las Cortes Generales, Legislatura XIV, Serie A: Proyectos De Ley 12 de septiembre de 2022.
Ref.121/000098. Publicado en el Boletín Oficial De Las Cortes Generales, Legislatura XIV, Serie A: Proyectos De Ley 31 de enero de 2023.

más inclusiva, eficiente, sostenible y accesible para todos los ciudadanos que se relacionasen con ella, tanto presencial como telemáticamente.

Tras las elecciones generales de julio de 2023, no sería hasta finales de noviembre del mismo año cuando se publicase la composición del nuevo ejecutivo. Y a pesar de ser del mismo color que el anterior, desconocíamos si el nuevo responsable de justicia rescataría los proyectos enunciados supra y en qué términos. Lo más lógico era volver a introducir en las cámaras los antiguos proyectos a fin de seguir con el debate y aprobarlos a través de leyes orgánicas tal y como estaban planteados al inicio. Sin embargo, no se optó por ese camino nomotético, sino que se publicó de manera sorpresiva un Real Decreto Ley -como indicábamos supra- con una mezcolanza de los tres proyectos enunciados, dejando atrás preceptos importantes y combinando en una misma norma cuestiones muy dispares de nuestro Derecho.

Posiblemente esta urgencia pudo venir motivada por la necesidad de justificar la ejecución de inversión de 410 millones de euros de los Fondos de recuperación europeos Next Generation EU[3] que estaban previstos destinar a la transformación digital de la Justicia. Proyectos, que previamente habían sido aprobados de forma unánime por todas las administraciones con competencias en Justicia[4].

2. Antecedentes.

En la disposición derogatoria única del presente Real Decreto Ley 6/2023 se establece la derogación expresa de la Ley 18/2011, de 5 de julio reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia, así como de cualesquiera otras normas de igual o inferior rango en lo que contradigan o se opongan a lo dispuesto en el citado real decreto-ley.

Estos son principalmente la Ley 18/2011 y el Real Decreto 1065/2015, de 27 de noviembre, sobre comunicaciones electrónicas en la Administración de Justicia en el ámbito territorial del Ministerio de Justicia y por el que se regula el sistema LexNET a los que debemos agradecerle haber contribuido de manera muy importante a establecer las bases férreas y claras del actual sistema de tecnologías de la información y la comunicación en la Administración de Justicia.

Así las cosas, hace ya más de una década que se legislaron conceptos como el Punto de Acceso General de la Administración de Justicia; la Sede Judicial Electrónica, u organismos tan consolidados como el Comité técnico estatal de la

3 Así se ha denominado la estrategia española para canalizar los fondos destinados por Europa a reparar los daños provocados por la crisis del COVID-19 a través de reformas e inversiones, construir un futuro más sostenible.

4 Olmedo, M.: "La Justicia avanza en digitalización e Innovación", *Diario LA LEY*, 6 de febrero de 2024, núm. 10440, Sección Tribuna.

Administración judicial electrónica (en adelante, CTEAJE) o el Esquema Judicial de Interoperabilidad y Seguridad. Todos ellos continúan su desarrollo en la nueva normativa donde se les amplían las competencias y funcionalidades para mejorar el entramado tan complejo de competencias públicas y hacer una justicia más eficiente a través de una mejora en los tiempos de respuesta respecto de las actuaciones automatizadas y proactivas. Todo ello, sin contar con la gran revolución que supuso para la vida de todos los operadores jurídicos la obligatoriedad en el uso de LexNET a partir de enero de 2016 para todas las comunicaciones con los juzgados y tribunales de nuestro país. Y aunque ahora nos parece muy cómodo, en su momento supuso una gran conmoción, casi traumática para los operadores jurídicos obligados a comunicarse a través de esta aplicación con los juzgados.

Esta norma ha sido base para el desarrollo de leyes como la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público o la Ley 42/2015, de 5 de octubre, de reforma de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil por la que se introdujeron de manera obligatoria las subastas judiciales electrónicas.

Todo ello, sin olvidar el gran papel que tuvo esta normativa durante la época más dura de la pandemia de la COVID-19 cuando esta norma sirvió al servicio público de Justicia de base legislativa para poder seguir funcionando durante las semanas más críticas. Aunque posteriormente fue completada con la publicación de la Ley 3/2020, de 18 de septiembre, de medidas procesales y organizativas para hacer frente al COVID-19 en el ámbito de la Administración de Justicia y que introdujo importantes mejoras respecto del Real Decreto-ley 16/2020, de 28 de abril, del mismo nombre.

Pero fue sobre todo esta crisis de la COVID-19 la que hizo patentes las deficiencias y lagunas existentes en nuestros sistemas de gestión procesal electrónicos y cuando realmente el ejecutivo tomó nota sobre los aspectos que urgían cambiar de nuestro sistema de administración de justicia digital para adaptarlo a la sociedad actual. Así las cosas, la celebración de vistas y de diferentes actos procesales mediante presencia telemática constituyen a día de hoy parte de la actividad cotidiana del servicio público de Justicia y es principalmente a estas a las que viene a dar carta de naturaleza el Real Decreto 6/2023.

II. LA INTEROPERABILIDAD.

Sin duda, el primer caballo de batalla al que se enfrenta esta norma es hacer posible la tan ansiada interoperabilidad entre los diferentes sistemas de justicia

electrónica de las diferentes comunidades autónomas y el sistema judicial central[5]. Esto haría posible que un ciudadano -sin importar la región en la que resida o la región donde radique el proceso judicial en el que se encuentre involucrado- pueda acceder a todos los datos de estos procesos a través de su Carpeta Justicia. También beneficiaría a los funcionarios de la Administración de Justicia que podrían tener acceso al expediente judicial electrónico completo de un proceso radicado en otro juzgado o tribunal. Ya que, hasta ahora a pesar de tener un expediente digitalizado, en caso de que este asunto fuese elevado a otro órgano como puede ser Tribunal Supremo, Audiencia Nacional u otro juzgado de otra CC.AA. este debía ser impreso y remitido en correo postal para posteriormente volver a ser digitalizado en el órgano de destino.

La nueva norma indica en la Disposición final novena, en concreto en su apartado 5 que "Las Comunidades Autónomas que aún no cuenten con tales sistemas o servicios, o que, contando con los mismos, aún no hayan operado su plena integración con los nodos, servicios o sistemas comunes del Ministerio de la Presidencia, Justicia y Relaciones con las Cortes deberán, en todo caso, llevar a cabo su plena aplicación e integración el 30 de noviembre de 2025". Sin embargo, podemos fácilmente advertir que una vez más este plazo se verá incumplido, a pesar de que todavía queda tiempo para su finalización.

Y es que, si nos fijamos en los orígenes de la interoperabilidad ésta figura aparece por primera vez en el anexo de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos[6] y posteriormente en el Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

Pero la problemática en el gabinete de Justicia llegó junto con la instauración de la tan anhelada e inacabada en su implantación Nueva Oficina Judicial. Especialmente tras la entrada en vigor de la anteriormente comentada Ley 18/2011 donde se instituyó la importancia de la interoperabilidad de los sistemas de gestión procesal informatizada y su adaptación al Esquema Judicial de Interoperabilidad y Seguridad[7]. No obstante, el ideal de la interoperabilidad sigue dando mucho que

5 Para la gestión procesal de los procesos judiciales contamos con distintas aplicaciones de gestión procesal en cada Administración con competencias en la Administración de Justicia. Así, contamos con la aplicación del Ministerio de Justicia, Minerva; la aplicación del Ministerio Fiscal, Fortuny. Sin dejar atrás a las aplicaciones de las Comunidades Autónomas con competencias en medios materiales y personales de la Administración de Justicia donde podemos citar la aplicación de Adriano en Andalucía una de las más avanzadas, Atlante en Canarias, Cicerone en Valencia que ha trabajado duramente para mejorar su interoperabilidad, Justizia. eus en el País Vasco, Libra en Madrid, e-justícia.cat en Cataluña tras su renovación por la precedente Themis, Avantius en Navarra, Vereda en Cantabria o Minerva en Asturias y Galicia, entre otras. Ver más en: Catalán Chamorro, M.J.: *La justicia digital en España: Retos y desafíos*, Tirant Lo Blanch, 2023, pp. 83-90.

6 Bueno De Mata, F.: "La Justicia avanza en digitalización e Innovación", *Diario LA LEY*, 6 de febrero de 2024, núm. 10440, Sección Tribuna.

7 Ver más sobre este particular en Bases del Esquema judicial de interoperabilidad y seguridad, disponible en:https://www.cteaje.gob.es/documents/185545/188120/CTEAJE-BIS-INF-MJU-Bases+del+EJIS+v+1+0.

hablar y por lo que trabajar en la actualidad. Si bien, debemos poner de relieve que esta problemática no es que no se haya podido resolver por motivos legales o técnicos, sino que se trata de una falta de compromiso y voluntad política[8] por parte de todas las Comunidades Autónomas, especialmente aquellas que tienen cedidas las competencias de Justicia en cuanto a los recursos humanos y materiales, y más concretamente aquellas que tienen históricamente la voluntad de diferenciarse del resto de España. Por ello, solo cuando todas las administraciones autonómicas y centrales se pongan a remar en el mismo sentido podremos hablar de una interoperabilidad real de los sistemas de gestión procesal informatizada en nuestro país[9].

Actualmente, nos encontramos con una España a diferentes velocidades en lo que concierne al acceso digital al expediente judicial electrónico, pero también respecto de la dotación de los juzgados con medios humanos y materiales. Por ello, el legislador consciente de que este Real Decreto obliga a las administraciones públicas con competencias en medios materiales y personales de la Administración de Justicia a implantar y desarrollar una buena batería de medidas, orientadas sobre todo a garantizar el derecho fundamental de acceso a la Justicia en igualdad de condiciones a toda la ciudadanía en todo el territorio del Estado, introduce la coletilla "siempre que sea posible" a lo largo de toda la norma.

Por consiguiente, el legislador pone el foco en el impulso de la cogobernanza, donde todas las comunidades autónomas deberán esforzarse para remar a favor y que ello revierta en un mejor acceso a todas las aplicaciones, que la nueva Administración de Justicia digital pone en marcha. No obstante, a día de hoy todavía encontramos muchas comunidades autónomas donde el expediente digital es inexistente e incluso los procedimientos ni siquiera están digitalizados.

III. EL NUEVO ORGANIGRAMA: CTEAJE Y CONSEJO CONSULTIVO.

El CTEAJE puesto en marcha con la Ley 8/2011 ha realizado durante todos estos años un trabajo muy discreto pero esencial para mejorar la interoperabilidad. Así lo avalan datos como que en estos últimos 3 años este órgano ha mantenido 842 reuniones[10]. Con la entrada en vigor del nuevo Real Decreto 6/2023 se renueva esta institución a la que se le amplían las competencias y funciones.

Así, este Comité técnico estatal de la Administración judicial electrónica se reestablece como órgano de cooperación en materia de Administración judicial

pdf/27bcb4b5-2bde-a976-6c52-af1305f85059, visitado el día 8 de febrero de 2024.

8 Bueno De Mata, F., "La Justicia avanza", cit.

9 *Ídem.*

10 Olmedo, M., "La Justicia avanza", cit.

electrónica y en la nueva norma no varía su composición. Si introduce dos fines de este órgano donde se reafirma la idea de la cogobernanza y la coordinación del desarrollo de la transformación digital de la Administración de Justicia.

No obstante, en cuanto a las funciones se detallan y amplían mucho más. Llama la atención que este órgano tendrá como cometido definir y validar la funcionalidad y seguridad de los programas y aplicaciones que se pretendan utilizar en el ámbito de la Administración de Justicia, con carácter previo a su implantación, ya que antes no se precisaba de esta validación. Además será el encargado de impulsar y coordinar la elaboración y ejecución de las iniciativas de actuación y planes conjuntos, acuerdos y convenios, en aras a lograr la transformación digital de la Administración de Justicia y promover la puesta en marcha de servicios interadministrativos integrados y la compartición de infraestructuras técnicas y de los servicios comunes, que permitan la racionalización de los recursos de tecnologías de la información y la comunicación a todos los niveles, evitándose así duplicidades que hasta ahora han sido la tónica general.

Sigue siendo primordial el mantenimiento del Esquema Judicial de Interoperabilidad y Seguridad para buscar, por un lado, la interoperabilidad total de todas las aplicaciones informáticas al servicio de la Administración de Justicia. Y por el otro lado, en materia de ciberseguridad judicial, mantener la seguridad de los sistemas, estableciendo el marco organizativo a través del Subcomité de seguridad, la política de seguridad y promoviendo su desarrollo normativo, definiendo y estableciendo criterios de valoración de referencia que permitan a las Administraciones prestacionales determinar el nivel de seguridad de cada dimensión de los sistemas de información de juzgados, tribunales y fiscalías y los niveles de riesgos de estos.

Así mismo, el CTEAJE se deberá coordinar con la Conferencia Sectorial de Justicia y se crea el Comité de Dirección para la Digitalización de la Administración para la coordinación y colaboración constante entre la Administración General del Estado y sus organismos y entidades de Derecho Público vinculadas o dependientes.

Sin embargo, se plantea como un gran avance en el nuevo Real Decreto la creación del Consejo Consultivo para la Transformación Digital de la Administración de Justicia del que formarán parte las organizaciones sindicales; asociaciones profesionales de jueces y juezas, fiscales y letrados y letradas de la Administración de Justicia; los Consejos Generales de la Abogacía, la Procura y los Graduados Sociales, así como asociaciones y organizaciones Empresariales, incluso de empresas de electrónica, tecnologías de la información, telecomunicaciones y digitalización; el Colegio Oficial de Registradores de la Propiedad y Mercantiles de España; el Consejo General del Notariado y la Federación Española de Municipios y

Provincias. Además de la Secretaría General de Administración Digital que deberá ser la entidad coordinadora. Todo ello sin perjuicio de otras organizaciones que se determinen. Aunque al legislador se le ha olvidado incluir en la norma que la finalidad de este Consejo será la de escuchar a todos los sectores implicados u obligados a relacionarse con la Administración de Justicia electrónica, para así crear normativas que se adapten a las necesidades de todos y no constituyan un perjuicio para estos. No obstante, todo esto se deberá desarrollar debidamente de manera reglamentaria, por lo que aún no estamos cerca de conocer las primeras voces de este Consejo.

IV. SERVICIOS ELECTRÓNICOS DE LA ADMINISTRACIÓN DE JUSTICIA ORIENTADOS AL CIUDADANO.

A pesar de que la norma establece solo derechos para los ciudadanos y ciudadanas ante la justicia digital, si existe -aunque no lo nombre la norma- el deber de personarse telemáticamente cuando así lo disponga la ley procesal aplicable al caso y el juez o jueza no dicte orden en contrario respecto del proceso que se trate. Si bien, los y las profesionales que se relacionen con la Administración de Justicia, si tienen categóricamente el deber de utilizar los medios electrónicos, las aplicaciones o los sistemas establecidos por las administraciones competentes en materia de Justicia. Así mismo se reconoce el uso obligatorio de medios e instrumentos electrónicos por los trabajadores de la Administración de Justicia y todo ello se detalla en los artículos 5 a 7 del Real Decreto 6/2023.

Así las cosas, la citada norma viene a dar carta de naturaleza a aplicaciones que o bien existían a través de proyectos piloto o ya estaban recogidas en la anterior Ley 18/2011 pero cuyas competencias y funcionalidades se habían ampliado más allá de lo que se disponían la norma. Por ello, es necesario que pongamos un poco de orden en la amalgama de aplicaciones que están en marcha y que a la lectura de la nueva norma parece se superponen unas con otras.

1. Carpeta Justicia.

A la vista de los éxitos que ha cosechado la Carpeta Ciudadana para la Administración General del Estado, el sector Justicia ha querido establecer una réplica de esta, pero para que los ciudadanos puedan a golpe de clic conocer el estado de cada uno de los procesos judiciales en los que participa. Es importante detallar que esta Carpeta Justicia actúa a modo de foto fija, un visor del momento en el que el ciudadano accede a la misma. De modo que esta no guarda o almacena toda la información judicial sobre una persona, sino que, al consultarla, el sistema busca en el ecosistema judicial toda la información sobre esta persona. Ello con la

finalidad de que el ciudadano no tenga que ir buscando sede por sede el estado de cada uno de sus procesos.

Dentro de esta Carpeta justicia podemos consultar la situación de los apoderamientos Apud Acta realizados, consultar el estado de los expedientes judiciales, así como de los edictos y las resoluciones judiciales dictadas respecto de la persona que accede. De manera muy intuitiva se ha incluido una agenda de señalamientos, que permite al ciudadano visualizar sus señalamientos, a la vez que también lo pueden consultar los funcionarios de la Administración de Justicia y evitar así citaciones que se solapen entre sí para una misma persona. Así mismo, desde esta aplicación se puede solicitar cita previa para acudir a cualquier servicio del juzgado y también se puede acceder y gestionar las cuentas de Depósito y Consignaciones Judiciales. Todo ello junto con la posibilidad de utilizar el visor del expediente judicial electrónico HORUS. Finalmente, el ciudadano (ya sea persona física, persona jurídica o profesional de la Justicia como abogados, procuradores y graduados sociales) podrá solicitar los certificados digitales de antecedentes penales; de ausencia de delitos de naturaleza sexual; de matrimonio; de nacimiento y de defunción.

Para el acceso a la Carpeta Justicia no se precisa más que la ya conocida identificación mediante el sistema seguro de identificación con las administraciones públicas Cl@ve y sus variantes Cl@ve PIN y Cl@ve Permanente o utilizar el DNI-electrónico, así como cualquier certificado electrónico reconocido.

Estos servicios hacen que esta Carpeta Justicia sea útil para los ciudadanos, pero inmensamente más útil para los abogados y procuradores, al poder acceder a toda la información sobre sus clientes a golpe de clic. No obstante, aún queda un arduo trabajo por realizar en cuanto a la accesibilidad, sobre todo para personas con discapacidades intelectuales y para las personas mayores, ya que se deberán adaptar a lectura fácil los contenidos de estas herramientas digitales para que toda la ciudadanía pueda acceder en igualdad de condiciones a las mismas. Amén de que estas aplicaciones tendrían una especial funcionalidad para la ciudadanía si se reformulasen los Juzgados de Paz en Oficinas Judiciales Municipales como planteaba el Proyecto de Ley de Eficiencia Organizativa, donde los funcionarios pudiesen atender a la ciudadanía ante las dudas que se les plantearán con el uso de estas nuevas aplicaciones[11].

2. Sede Judicial Electrónica.

Así las cosas, la descripción de sede electrónica en la norma no se separa mucho de la dictada en la Ley 18/2011 a pesar del gran cambio tecnológico al que

11 "Justicia avanza en el desarrollo de la Carpeta Justicia recogiendo la opinión de los profesionales y la ciudadanía" en *Diario LA LEY de* 5-2-2024.

hemos asistido en este tiempo. Si bien, la norma no habla de sede en singular sino en plural, ya que las administraciones con competencias en justicia podrán elaborar otras sedes judiciales electrónicas para realizar otros trámites (artículo 9.3 del RD. 6/2023). De manera que, desde la Carpeta Justicia se nos habilitan como enlaces de interés las distintas sedes judiciales habilitadas en todo el territorio nacional. Aquí se distinguen, por un lado, la Sede Judicial Territorio Ministerio con competencia para trámites con el Tribunal Supremo, la Audiencia Nacional y los órganos jurisdiccionales de las Comunidades Autónomas de Extremadura, Castilla la Mancha, Castilla y León, Islas Baleares, Región de Murcia, Ceuta y Melilla, así como las comunidades con convenio de colaboración en vigor actualmente Principado de Asturias y Comunidad Autónoma de La Rioja. Y, por otro lado, las sedes judiciales electrónicas de las comunidades autónomas que tienen transferidas las competencias de justicia en recursos materiales y personales, donde encontramos las Sedes Judiciales de Andalucía; Aragón; Canarias; Cantabria; Cataluña; Galicia; Asturias; Madrid; Navarra; País Vasco y Valencia.

En este punto, llama poderosamente la atención, una vez visitas todas las sedes autonómicas, que a pesar de cumplir todas con el contenido mínimo dictado por la norma en su artículo 10, la apariencia, el formato e incluso el contenido de cada sede es totalmente diferente a las demás. Desconozco si puede ser ventajoso para el ciudadano o profesional que al acceder a cada sede sea consciente de que ha cambiado de entorno digital, pero creo que puede ser más confuso, sobre todo para aquellos que tengan que usar diferentes sedes en su proceder.

Por lo general los trámites más relevantes que se pueden realizar en las distintas sedes electrónicas son aproximadamente los mismos, aunque dicta mucho la presentación de una sede a otra. Así, por ejemplo, si visitamos la sede electrónica del Territorio Ministerio al acceder a su catálogo distingue, entre trámites con una breve descripción de cada uno y los servicios ofrecidos por la sede.

En cuanto a los trámites aquí encontramos la cita previa anteriormente comentada o el acceso a las Cuentas de Depósitos y Consignaciones Judiciales desde donde el ciudadano o profesional podrá realizar los pagos que se les exigen judicialmente. Además de facilitarles en virtud de las modificaciones de la Ley 16/2022, de 5 de septiembre, de reforma del texto refundido de la Ley Concursal, el formulario para plantear una propuesta del Plan de Reestructuración de la deuda para la comunicación a los acreedores públicos y un modelo oficial del Plan de reestructuración (art. 684 Ley Concursal), así como acceder al formulario para dar trámite al procedimiento monitorio en la jurisdicción social con el fin de que el ciudadano pueda reclamar deudas dinerarias al empresario empleador. Como vemos trámites judiciales que el ciudadano puede llevar a cabo sin necesidad de estar asistido de abogado y procurador. Sin embargo, desde estos apartados no

podemos más que descargar información, pero no se da curso a ninguno de sus trámites, ya que para ello deberemos acceder al servicio de presentación de documentos.

Así las cosas, en cuanto a los servicios ofrecidos por la sede judicial del territorio justicia son realmente intuitivos y fáciles en su acceso. En este apartado podemos siempre que tengamos algún proceso abierto, acceder al visor del Expediente Judicial Electrónico HORUS, consultar los distintos estados del expediente, solicitar una copia del expediente judicial electrónico, consultar los actos de comunicación que nos han sido expedidos, además de verificar, a través del Código Seguro de Verificación (CSV), toda la documentación sobre un proceso concreto. Asimismo, podremos consultar los señalamientos a los que estamos citados e incluso suscribirnos a una alerta automática que se nos remitirá a nuestro correo electrónico o dispositivo móvil a través de SMS para avisarnos de futuros señalamientos.

Sin embargo, el rol más relevante y activo para el ciudadano se introduce con la posibilidad de presentar escritos ante un órgano jurisdiccional; iniciar procedimientos monitorios online; contestar electrónicamente a un requerimiento de un órgano judicial; solicitar la ejecución de un procedimiento por parte de una administración pública; presentar dictámenes periciales directamente al órgano jurisdiccional o solicitar apoderamientos apud acta.

Además, nos encontramos en el momento de mayor transparencia de la historia de la justicia para con el ciudadano, ya que a golpe de clic este tiene acceso a todos los edictos Judiciales y el acceso a todas las resoluciones que se hayan dictado en las que aparezca involucrado, igualmente se tiene acceso a pujar en todas las subastas judiciales que se realizan en todo el territorio nacional y puede remitir todas las quejas y sugerencias que tenga con la sede judicial electrónica.

En este sentido, es importante reseñar que encontramos sedes judiciales autonómicas muy similares a la descrita del Territorio Ministerio como es la sede electrónica de Andalucía o la de Madrid que contando con los mismos elementos pueden resultar un poco menos intuitivas para el ciudadano. Sin embargo, las sedes judiciales electrónicas de Aragón o Cantabria están prácticamente por construir desde cero para las personas físicas[12]. Y mientras la sede electrónica de Navarra presta información, pero no da acceso a realizar ningún trámite telemático.

En el otro extremo de la balanza, es decir con sedes judiciales electrónicas más avanzadas o con más servicios que la sede del territorio Ministerio encontramos por ejemplo la Sede Judicial País Vasco que incluso ya tiene implementada la

12 A fecha de redacción de este trabajo en febrero de 2024.

aplicación EpaiDigitala que permite a la ciudadanía acceder a un juicio o actuación virtual mediante Webex. Además, la sede vasca incluye derivaciones a servicios como el servicio de asistencia a la víctima para el asesoramiento si has sido víctima de un delito; el servicio de mediación hipotecaria; información o formularios para solicitar una orden de protección o solicitar una valoración de los daños en caso de accidente de tráfico. Muy intuitivas y con mayor número de trámites telemáticos son las sedes judiciales valenciana y sobre todo la gallega que facilita el acceso al procedimiento de jurisdicción voluntaria en materia de personas, al procedimiento de conciliación, procedimiento de consignación judicial e incluso da la posibilidad de iniciar el procedimiento de ejecución de título judicial (civil/social). Como nota diferenciadora la sede judicial electrónica canaria permite realizar denuncias telemáticamente, trámite que deberá ser implementado por el resto de sedes en los próximos meses en atención a la nueva redacción del artículo 266 de la LECrim.

Sin duda la sede judicial electrónica que dicta más diferencias respecto de las anteriormente comentadas es la catalana. Esta sede, con la voluntad de ser más intuitiva se estructura no por procedimientos, servicios o trámites como el resto, sino que trata de responder a las preguntas más frecuentes que se realizan los ciudadanos cuando tienen que acceder a la justicia. De modo que se estructura a través de un apartado que intenta responder a la pregunta genérica ¿qué hacer si…? - Y esta se va completando con las distintas situaciones ante las que se puede encontrar un ciudadano. Por ejemplo, que hacer si me ponen una multa de tráfico; me seleccionan como jurado; se produce una detención; muere un familiar; necesito orientación jurídica; necesito un abogado y no puedo pagarlo; necesito un procurador; tengo problemas con la guarda y custodia de los hijos; soy insolvente; pierdo o me roban la cartera; soy víctima de distintos tipos de delito o soy testigo en un proceso penal. También responde a trámites donde el ciudadano demanda determinados servicios como inscribirse como pareja estable; adoptar a un niño; cancelar antecedentes penales; llegar a un acuerdo; asistir a una vista judicial; otorgar un poder; cambiar el nombre o apellido; pedir el libro de familia; pedir la devolución de una tasa, pedir la nacionalidad española; un certificado; una cita previa en un juzgado o una pericial extrajudicial. Así mismo, respecto de un proceso judicial concreto se permite consultar el estado del expediente del ciudadano; de sus señalamientos, sus resoluciones o el estado de su petición de asistencia jurídica gratuita. Y así hasta un total de 55 trámites con sus respectivas respuestas a cada situación de manera diferenciada.

Como debilidades de este sistema podemos apuntar que no todos tienen respuesta de manera telemática, es decir, no en todos los casos se da trámite telemático al asunto, sino que en la mayoría de las ocasiones se llega simplemente a un apartado informativo. Y en los casos en los que se da lugar a una tramitación

telemática, no en todos los casos se utiliza el mismo modo de acceso seguro a través de los certificados digitales y sistemas Cl@ave anteriormente indicados, sino que en ocasiones la administración catalana requiere el acceso a través de su propio sistema de autenticación del Consorci Administració Oberta de Catalunya.

En definitiva, nos encontramos ante una España, ya no solo a diferentes velocidades en cuanto a la sede electrónica judicial, sino que además parece una orquesta tocando diferentes partituras a la vez. Una torre de babel que cada vez tiene una solución más complicada. Y es que lo informático no entiende de autonomías, sino que entiende de datos y números que deben compaginarse y converger para poder hacer realidad esa tan ansiada interoperabilidad.

3. Punto de Acceso General de la Administración de Justicia.

Así las cosas, en este punto vemos como se siguen superponiendo las estructuras o repitiéndose los portales desde los que se puede acceder a la sede judicial electrónica. El Punto de Acceso General de la Administración de Justicia nace como cajón de sastre para recoger en un único portal todas las aplicaciones disponibles para el uso no solo por la ciudadanía, sino también por la judicatura, fiscalía, registros civiles, unidades administrativas y peritos. Así mismo, este portal permite filtrar las aplicaciones por los órganos jurisdiccionales o las Comunidades Autónomas a las que está destinada. Por supuesto también permite su conexión con la sede judicial electrónica y la carpeta justicia. No obstante, este portal no es de nueva creación, ya que también se contemplaba en la anterior Ley 18/2011 y el contenido de su regulación no ha cambiado en lo esencial.

Todo ello, como indica la norma con el objetivo de asegurar la completa y exacta incorporación de la información y accesos publicados en éste, de manera interoperable con los posibles puntos ubicados en los portales habilitados por cada administración competente. Es sorprendente cuando la norma indica que este portal lo que persigue es garantizar el acceso universal y claridad de la información con especial atención a los contenidos dirigidos a colectivos vulnerables, especialmente a niños, niñas y adolescentes, que pudieran ser de su interés. Ya que esta amalgama de aplicaciones y portales, no hacen más que complicar su entendimiento incluso para quienes somos conocedores de los procesos judiciales y sus trámites. Así mismo, pretender que este portal sea accesible para los niños y niñas no creo que sea lo más adecuado, sino que se deberán habilitar servicios especiales físicos y telefónicos para facilitar el acceso a la justicia, no tanto de los niños sino de los colectivos vulnerables, especialmente las personas mayores que son las grandes olvidadas en las aplicaciones actuales de justicia digital.

Este portal debería situarse como el punto de partida de todas las aplicaciones de justicia digital comentadas hasta este momento, pero la Ley ha querido

introducirlo en último lugar como cajón de sastre como indicábamos supra. Y es que en este portal confluyen un total de setenta y cuatro aplicaciones disponibles para distintas acciones. No obstante, la ciudadanía tan solo tiene acceso a diecinueve de ellas según el portal, de las cuales son bastantes menos, ya que algunas de estas no son ni de uso, ni se le permite tampoco el acceso al ciudadano.

Si bien, conviene dar visibilidad a una aplicación que ha pasado bastante desapercibida pero que brilla por la facilidad en su uso intuitivo, como es la denominada Sub-sede Electrónica[13]. En ella, el ciudadano podrá realizar un elenco de procedimientos muy limitados, pero de tramitación muy sencilla como puede ser solicitar certificaciones de las inscripciones de los Registros Centrales de violencia de género, violencia doméstica, medidas cautelares, requisitorias o sentencias no firmes. U otro tipo de solicitudes como las de cancelación de antecedentes penales; apostillado de documento público firmado digitalmente; devolución de ingresos indebidos de tasas; certificados expedidos por el Registro Central de Titularidades Reales; solicitud de informes periciales a los Institutos de Medicina Legal y Ciencias Forenses; solicitudes al Registro de fundaciones y al Registro Civil para la rectificación de errores.

El resto de las aplicaciones a las que puede acceder la ciudadanía son principalmente portales divulgativos del ámbito de la justicia como es la web del Comité Técnico Estatal de la Administración Judicial Electrónica (CTEAJE); la web del Portal Justicia 2030 o el Portal del Servicio Público de Justicia. Si bien, merece la pena destacar el portal EduJusTIC que ofrece formación en forma de cursos gratuitos y online en abierto para toda la ciudadanía con el objetivo de compartir y difundir los contenidos digitales de la Administración de Justicia e impulsar la transformación digital del ecosistema justicia. Desde este portal podremos realizar cursos para conocer mejor la aplicación de la carpeta justicia, de la sede judicial electrónica, Lexnet o incluso sobre cibercriminalidad.

4. Portales de datos.

Hasta ahora, las fórmulas utilizadas por el CGPJ para realizar su estadística eran cuasi decimonónicas. Estas estadísticas se realizan fundamentalmente a través de la recopilación de datos juzgado por juzgado y temática por temática. El buen hacer de esta sección del CGPJ hace que estas estadísticas sean las más útiles y fiables del panorama jurídico a la hora de realizar cualquier estudio académico de rigor. Sin embargo, debido al arduo trabajo que ellas conllevan sus ítems y sus cuestiones son limitadas a las más relevantes.

Hoy, en la era de la inteligencia artificial y del Big data, el ejecutivo se ha atrevido a dejar que estas dos herramientas pasen a beber de la información generada por

13 Disponible en: https://sede2.mjusticia.gob.es/, visitada el día 18 de febrero de 2024.

nuestro sistema judicial con la finalidad de aprovechar la información disponible para optimizar procesos, identificar tendencias, mejorar la eficiencia y la toma de decisiones informadas. Y esto es lo que se ha denominado la justicia orientada al dato. De esta manera se podrán divisar más fácilmente los problemas relativos a la interoperabilidad entre todos los sistemas y operadores de la Administración de justicia y así tomar decisiones basadas en métricas consistentes y análisis de la información disponible. Así mismo, estas herramientas serán capaces de orientar las posibilidades de mejora, optimización e incluso la automatización de procesos.

Este tipo de herramientas ya han sido utilizadas en otras administraciones públicas como pueden ser las fuerzas y cuerpos de seguridad del Estado, la sanidad en la etapa de la COVID-19 o la Dirección General de Tráfico ya que permite detectar cuellos de botella o aquellos puntos negros sobre los que haya que invertir mayores recursos humanos, materiales o tecnológicos para abordar esas cargas de trabajo de manera más eficiente[14]. Actualmente nos encontramos utilizando una inteligencia artificial asistencial, es decir, que nos asiste para aconsejarnos en tareas cotidianas de la Administración de Justicia, lo que no sabemos es si esta ola de inteligencia artificial en la Justicia avanzará hasta la inteligencia artificial decisional en la que permitamos que estos sistemas tomen parte y decidan de algunas cuestiones con mayor o menor enjundia dentro de nuestros procesos.

En este punto, a los poderes públicos les hace falta una profunda reflexión sobre el "quo vadis" de la inteligencia artificial aplicada a la justicia. Ya que la relevancia constitucional de este tipo de tecnologías[15] aplicadas a ámbitos tan sensibles como las decisiones jurisdiccionales o el uso de los datos previos emanados de resoluciones judiciales para marcar el futuro de las resoluciones futuras puede chocar frontalmente con derechos constitucionales tan fundamentales como el derecho a la tutela judicial efectiva o el derecho a un juez ordinario predeterminado por la ley.

A priori lo que se pretende es procesar automáticamente los datos, de manera que estos análisis de la información con carácter estadístico permitan aplicar políticas públicas que minoren la conflictividad o que permitan aplicar políticas de mitigación de sus efectos. Y todo ello siempre con el máximo respeto a la protección de los datos de carácter personal, y el acceso a la información protegida, en general. No obstante, debemos ser también conscientes de la multitud de ciberataques que han sufrido las Administraciones a lo largo de la historia y más en estos últimos tiempos en los que se invierte una gran parte del presupuesto en nuevas aplicaciones, pero poco en la protección de la información de estas. Así las cosas, no cabe más que confiar en los procesos de la anonimización y

14 Bueno De Mata, F.: "La Justicia avanza", cit.

15 Ídem.

seudonimización que se mencionan en el texto legislativo y que estos surtan los efectos deseados.

En esta línea, el Ministerio de Justicia ha creado el proyecto "La justicia en datos"[16] que intenta presentar de manera ordenada, abierta y accesible el conjunto de datos oficiales relacionados con la Administración de Justicia y el Poder Judicial en España. La relevancia se sitúa en el apartado de "la justicia orientada al dato", donde además de poder acceder a catálogos de datos, también se nos permite conocer los detalles de estos intercambios masivos de datos de los que nos habla la norma 6/2023 y que se basa en tres pilares principales. En primer lugar, da cuentas de los llamados "Lagos de datos o Data warehouse" que se describe como un modelo de colaboración entre administraciones y organismos para transferir y obtener datos en un entorno de colaboración y corresponsabilidad, donde por ejemplo se podrán ver las consultas al expediente judicial electrónico realizadas por cada comunidad autónoma y cada jurisdicción. Por otro lado, un "Cuadro de mandos" destinado a la explotación estadística de la información que de modo muy visual y a través de tablas permitirán mejorar la toma de decisiones de políticas públicas basadas en la evidencia. Por ejemplo, en cuanto a la entrada de asuntos y a las medidas acordadas. Y finalmente, la explotación de la información georreferenciada que permitirá hacer visualizaciones avanzadas relativas a determinadas áreas o temáticas y que analiza el territorio desde el nivel de los municipios y también se puede estudiar la posibilidad de realizar operaciones avanzadas. Ejemplo de ello son los datos facilitados por la Fiscalía General del Estado y que pueden descargarse desde este portal de datos de la justicia sobre delitos informáticos[17].

Por consiguiente, podemos concluir que con este portal hoy, el acceso a los datos judiciales es más sencillo, intuitivo, visual pero la transparencia del dato con los ciudadanos no es total, ya que por la redacción de la norma y por la información volcada en este portal de datos de la justicia habrá datos que los poderes públicos se guarden para sí. Con la finalidad de mejorar las políticas públicas, pero de las que no tengamos constancia la ciudadanía.

5. Algunas aplicaciones que facilitan el acceso a la justicia.

A lo largo de las diferentes sedes electrónicas judiciales encontramos distintas aplicaciones, algunas de ellas muy interesantes para los ciudadanos que acceden a la justicia por sí mismos, esto es, sin necesidad de estar asistido de abogado y/o procurador. Sin embargo, el sistema de multiplicidad de sedes hace que cada territorio tenga unas aplicaciones diferentes y esto da lugar a distintas ventajas

16 Disponible en: https://datos.justicia.es/, visitado el día 20 de febrero de 2024.

17 Ver ejemplo en: https://datos.justicia.es/delitos-informaticos, visitado el día 20 de febrero de 2024.

comparativas. En este contexto resaltaremos algunas aplicaciones que, aunque todas no sean de uso genérico en todo el territorio español convendría su extensión a todos los ciudadanos por su utilidad práctica.

A) Sistema de Comparecencias Apud Acta electrónico.

Ya hemos nombrado anteriormente la posibilidad de otorgar apoderamientos apud acta de manera electrónica. Donde el ciudadano, a través de su sede electrónica puede solicitar apoderamientos genéricos o limitados, así como retirarlos sin necesidad de acudir presencialmente al juzgado para que el Letrado de la Administración de Justicia de fe pública. De este modo, no solo nos ahorramos la tasa que se le paga al notario por otorgar el poder notarial de turno que se le emite al procurador que nos vaya a representar en el juzgado, sino que también podremos ahorrarnos el viaje y la cita al juzgado con el LAJ de turno, pudiendo realizar este trámite desde nuestro domicilio y en cualquier día de la semana y hora del día. Si bien necesitaremos previamente haber concertado el otorgamiento de este poder con un procurador que vaya a aceptar el encargo y que nos facilite sus datos colegiales para su nombramiento. Este apoderamiento apud acta para procurador si está extendido en casi todo el territorio nacional.

Sin embargo, existe también un sistema de comparecencias, pionero en las Islas Canarias y que no ha tenido réplicas en el resto del territorio español, que permite que el Letrado de la Administración de justicia pueda dar fe pública ante comparecencias en remoto. De modo que tras la identificación biométrica y segura desde el smartphone del compareciente se deja constancia de la "personación del mismo".

Si bien, debemos subrayar el uso que se le ha dado en esta comunidad Autónoma a esta aplicación. Ya que es incluso más delicada de lo que a priori podríamos pensar, debido a que se está utilizando para sustituir, la personación física en los días marcados por la autoridad judicial cuando se acuerda una medida cautelar, por una identificación telemática a través de la biometría previamente acreditada. Si bien, no tenemos datos de su alcance y desarrollo desde el año 2021 que el gobierno canario publicitó la implantación de la misma como proyecto piloto[18].

B) Escritorio Virtual de Inmediación Digital (EVID).

En una línea similar pero destinada a las comparecencias judiciales más genéricas y en especial pensado para los trámites que realizan en el ejercicio de

18 Disponible en: https://www3.gobiernodecanarias.org/noticias/el-gobierno-canario-implanta-un-sistema-de-comparecencias-judiciales-a-distancia-y-con-identificacion-biometrica/, visitado el día 6 de marzo de 2024.

sus funciones los funcionarios de la oficina judicial encontramos la aplicación EVID. Y aunque esta circunscrita solo en algunas provincias[19] -a la redacción de este trabajo- su utilidad se extiende a numerosos actos procesales.

En primer lugar, se le remite una comunicación específica al ciudadano para realizar la conexión, además de permitirle que presente a través de esta plataforma la documentación que tenga prevista adjuntar para dicho trámite. De modo que el funcionario puede acceder a la documentación presentada antes de la atención, para hacer esta visita lo más ágil posible.

En segundo lugar, durante el momento de la atención telemática el funcionario le dará inicio al trámite a través de la videoconferencia, con el preceptivo control de la grabación y será este el encargado de la administración del turno de palabra. Así mismo, se podrán intercambiar formularios electrónicos para dar el consentimiento respecto de la actuación administrativa pertinente e incluso se podrá intercambiar documentación y firmarla por los cauces de firma electrónica permitidos.

Y, en tercer lugar, una vez finalizada la atención por el funcionario pertinente este procederá al almacenamiento de toda la documentación aportada por el ciudadano, la grabación del acto y el justificante de celebración. Así mismo quedará constancia de la generación de huellas y evidencias criptográficas de las interacciones.

Si bien, desconocemos en qué punto quedarán estas dos aplicaciones descritas hasta ahora tras la entrada en vigor del Real Decreto 6/2023, ya que este solo se pronuncia respecto de los requisitos técnicos que deberán contener los llamados puntos de acceso seguro, es decir, los dispositivos desde los cuales nos vamos a conectar con los juzgados para estas comparecencias telemáticas. Así mismo, se deberá aclarar si las comparecencias se deberán realizar no solo desde puntos acreditados como seguros en cuanto al dispositivo utilizado, sino también en un llamado por la norma lugar seguro. Si ambos fuesen requeridos de manera yuxtapuesta estas aplicaciones serán instaladas en dispositivos disponibles en los lugares denominados seguros. Entre ellos se citan la oficina judicial correspondiente al tribunal competente, o cualquier otra oficina judicial o fiscal, y las oficinas de justicia en el municipio -que no están desarrolladas en ninguna norma-, sin indicar expresamente los juzgados de paz, con lo que en este extremo estaríamos en el mismo punto de partida previo a la norma en cuanto a las dificultades de accesibilidad para los ciudadanos que pretendan realizar trámites con la Administración de Justicia de manera telemática.

19 Albacete, Asturias, Ávila, Badajoz, Burgos, Cáceres, Ceuta, Ciudad Real, Cuenca, Guadalajara, Huelva, Islas Baleares, Jaén, Las Palmas de Gran Canaria, León, Madrid, Málaga, Melilla, Murcia, Navarra, Palencia, Salamanca, Santa Cruz de Tenerife, Segovia, Soria, Teruel, Toledo, valencia, Valladolid y Zaragoza.

La norma también establece como puntos seguros los Registros Civiles pero limitado su uso a las actuaciones relacionadas con su ámbito y por lo tanto con capacidad para asuntos muy concretos. También son lugares seguros instituciones públicas como el Instituto Nacional de Toxicología y Ciencias Forenses y los Institutos de Medicina Legal circunscrito a las intervenciones judiciales previstas para los Médicos Forenses, Facultativos, Técnicos y Ayudantes de Laboratorio, situaciones que ya se dan en la práctica y para lo que la norma tan solo vendría a dar carta de naturaleza. Así mismo se indican las sedes de las Fuerzas y Cuerpos de Seguridad del Estado limitadas estrictamente para la intervención de sus miembros. O las sedes oficiales de la Abogacía del Estado, del Servicio Jurídico de la Administración de la Seguridad Social y de los Servicios Jurídicos de las Comunidades Autónomas de nuevo a disposición para la intervención de los miembros de tales servicios. Igualmente, es habitual en la práctica de los juzgados asistir a intervenciones telemáticas desde los Centros penitenciarios, órganos dependientes de Instituciones Penitenciarias, centros de internamiento de extranjeros y centros de internamiento de menores, para las personas internas y funcionarios públicos, siempre que el declarante no sea parte perjudicada en el proceso. No obstante, se prevé la posibilidad de aumentar el número de lugares seguros a otros que se puedan prever en futuros reglamentos que desarrollen la norma para todo el territorio nacional[20].

Es importante subrayar que las personaciones ante el órgano judicial por videoconferencia deben cumplir con determinados requisitos recogidos en el artículo 60 del Real Decreto 6/2023. Así las cosas, una vez la oficina judicial o fiscal haya comprobado la identidad de las personas intervinientes en las actuaciones realizadas por procedimientos electrónicos a través de los datos básicos de identificación que hayan sido aportados previamente por ellas, nos gustaría poner de relieve dos requisitos de la norma por la singularidad de los mismos. Por un lado, la prohibición en la intervención por videoconferencia del empleo de sistemas o aplicaciones que alteren o distorsionen la imagen y el sonido transmitido, con excepción de aquellas que hayan sido previamente acordadas por el órgano judicial debido a la necesidad de salvaguarda de la identidad por tratarse de testigos o peritos protegidos o agentes policiales. Y, por otro lado, se resalta también la importancia de que los intervinientes en una videoconferencia deben observar las mismas normas de decoro, vestimenta y respeto exigidas en las actuaciones realizadas presencialmente en las salas de vistas y en las sedes de los tribunales, oficinas judiciales y oficinas fiscales. Aunque no especifica si los abogados deben usar la toga en los actos procesales en los que actúen a través de videoconferencia.

20 Ver más sobre esta problemática en: Rodríguez Lainz, J.L.: "Las actuaciones procesales por videoconferencia en el proceso penal tras la publicación del Real Decreto-Ley 6/2023", *Diario LA LEY*, 13 de marzo de 2024, núm. 10465, Sección Tribuna.

No obstante, todo apunta que hasta que el CTEAJE realice y entre en vigor el Reglamento que desarrolle las características técnicas que deben de contener estos puntos y lugares seguros se podrán seguir utilizando los sistemas de comunicación bidireccional homologados, como el usualmente utilizado en la práctica de los juzgados y tribunales Cisco Webex. Esta aplicación cumple con los requisitos requeridos en el artículo 62.2, ya que permite la transmisión segura de las comunicaciones y la protección de la información, además de permitir y garantizar la identificación de los intervinientes, y cumplir los requisitos de integridad, interoperabilidad, confidencialidad y disponibilidad de lo actuado[21].

C) Consulta de Señalamientos online.

Más allá de los señalamientos a los que tenemos acceso a través de la sede judicial electrónica porque hayamos sido citados como parte, en el afán por mejorar la transparencia de la Administración de Justicia el Ministerio también nos permite conocer determinados datos de los señalamientos de cada juzgado y tribunal de nuestro país. Aunque hasta la fecha tan solo podamos conocer los datos de las provincias de Albacete, Ávila, Badajoz, Burgos, Islas Baleares, Cáceres, Ciudad Real, Cuenca, Guadalajara, León, Murcia, Palencia, Salamanca, Segovia, Soria, Toledo, Valladolid y Zamora. Y también respecto de la Audiencia Nacional en los órdenes Contencioso/Administrativo y Social[22].

En primer lugar, el acceso se divide en un enlace específico para Letrados de la Administración de Justicia y profesionales y otro enlace para el público general que podrá acceder a través del sistema Cl@ave o con certificado digital. Así, la ciudadanía podrá conocer los señalamientos segmentados por tipo de acto o diligencia (juicio, vistas, audiencia previa, comparecencia ante el juez o tribunal, conciliación, diligencias de pruebas u otros) y además conocer el estado del acto (si está señalado, anulado o suspendido). Además, se podrá estudiar la evolución semanal de los señalamientos (donde podemos observar que generalmente las vistas se concentran de lunes a jueves fundamentalmente) y el tramo horario que más afluencia de actos tenga (en el panorama general también podemos ver que el tramo entre las 10 y las 12 horas son los que más señalamientos tienen). Finalmente podemos ver la sala en la que están señalados los actos, el tipo de acto y la jurisdicción a la que pertenece.

No obstante, cabe plantearse las posibles implicaciones que tiene para el poder judicial que el poder ejecutivo controle, realice conteo y conozca determinados datos del ámbito judicial y cómo esto puede repercutir a largo plazo en una

21 Ídem.

22 Disponible en: https://sedejudicial.justicia.es/-/consulta-de-senalamientos, visitado el día 9 de marzo de 2024.

limitación de la independencia de este poder que siempre ha reinado durante toda la democracia. De modo que podríamos estar ante un arma de doble filo, donde, por un lado, se viste de transparencia e información para el ciudadano y, por otro lado, sea una herramienta de control por parte del ejecutivo respecto de la producción del poder judicial. Amén de la dudosa aplicabilidad de esta información para el ciudadano de a pie. Ya que conocer el volumen de asuntos que tiene un juzgado y el señalamiento del tipo de procesos no revela mucho respecto de la implicación de los ciudadanos ante la justicia ordinaria.

D) Otras aplicaciones recientes que mejoran el acceso a la justicia a los ciudadanos.

Existen tres aplicaciones informáticas de uso en todo el territorio nacional que queremos referenciar por las implicaciones tan importantes que tienen para la vida de los ciudadanos a pesar de que no forman parte del articulado del Real Decreto 6/2023 comentado en el presente trabajo.

En primer lugar, cabe hacer mención a la ardua tarea de digitalización que se está llevando a cabo en el ámbito del Registro Civil. En este caso, a pesar de no ser una aplicación que pueden utilizar los ciudadanos, sino que está circunscrita al uso por parte de los funcionarios de los registros civiles DICIREG es una plataforma adaptada al nuevo modelo de Registro Civil. Esta nueva estructura se encuadra a través de expedientes abiertos por medios electrónicos y permiten la inscripción de todos los hechos relativos al estado civil de las personas que deban acceder al Registro. De modo que la publicidad de la información registral se organiza directamente en formato digital y se posibilita el acceso telemático de la ciudadanía siempre a través de su identificación electrónica. Esta nueva fórmula proporciona un registro electrónico en el que se practican asientos informáticos; se organiza la publicidad y se da fe de los hechos y actos del estado civil.

El objetivo es pasar de un sistema de registros por asientos a una hoja de vida por cada ciudadano, ya que a pesar de que el inicio y el fin de esa hoja sea la misma para todos (nacimiento y defunción), en la actualidad la variedad de aspectos a asentar por los ciudadanos quedan más claros si tienen una hoja propia, ya que hoy se puede contraer matrimonio y divorciarse varias veces, cambiar el nombre, el orden de los apellidos, el sexo, etc. No obstante, para la implantación de DICIREG en todo el territorio español aún queda bastante tiempo debido a la delicadeza con la que se deben traspasar los datos del formato papel al formato digital[23].

En segundo lugar, la incidencia del portal de subastas en la sociedad española ha cambiado el paradigma de unas subastas sobre las que siempre ha planeado la sombra de las dificultades para acceder tanto a la información de los bienes

23 Ver más en: Catalán Chamorro, M.J.: *La justicia digital*, cit., pp. 153-155.

sometidos a subasta, como al acceso a la propia puja y donde los pujantes solían ser habitualmente los mismos en determinados partidos judiciales. A través del portal público de subastas electrónicas, puesto en marcha en octubre de 2015, se permite al ciudadano, una vez registrado en el mismo, intervenir en cuantas subastas desee y permite realizar desde esta misma plataforma el depósito necesario para participar en las subastas judiciales y las administrativas que tenga por conveniente. Y todo ello desde la comodidad de su domicilio y sin tener que desplazarse en ningún momento a las sedes u oficinas para realizar las pujas. Además, con el sistema de alertas le permitirá recibir notificaciones sobre determinadas subastas de bienes en las que se haya mostrado interesado. Este portal ha contribuido en gran medida a dar transparencia a este tipo de transacciones.

Y, en tercer lugar, referenciamos la importancia de la plataforma de Liquidación de Bienes[24] que se promociona como un portal público electrónico para la publicación de activos de las microempresas en liquidación. De modo, que el propietario de estas microempresas en situación de quiebra incluirá un catálogo integrado por los bienes de su patrimonio que hayan sido añadidos a través de comunicación mediante el formulario de solicitud de apertura del propio deudor al Servicio Electrónico de Microempresas. Esto se llevará a cabo justo tras la apertura de un procedimiento concursal especial de liquidación para microempresas. Salvo para aquellos supuestos excepcionales de bienes o derechos, cuya transmisión se prevea a través de un sistema diferente en el plan de liquidación. Así, será el propio deudor el que utilizará la plataforma en línea de liquidación de bienes procedentes de procedimientos especiales de liquidación.

Sin embargo, esta plataforma no ha tenido el éxito pretendido, bien sea por el desconocimiento de la misma por parte de las autoridades judiciales o por la dificultad para su uso por los propios empresarios liquidadores. Además, debemos de poner de relieve la necesidad de conectar esta plataforma con el portal público de subastas para que la ciudadanía pueda conocer de todos los bienes que se encuentran en liquidación a través de un mismo canal.

V. CONCLUSIONES.

A pesar de los enormes avances que supone la entrada en vigor del Real Decreto 6/2023 para millones de españoles que podrán acceder a la justicia y visualizar sus trámites judiciales desde la comodidad de su domicilio, tras el análisis realizado en el presente trabajo queda un poso de incertidumbre o de desconcierto, ya que la norma parece inacabada. Si bien, es cierto que esta norma

24 Disponible en: https://plabi.justicia.es/, visitado el día 12 de marzo de 2024.

vendrá seguida de diferentes desarrollos reglamentarios que terminarán de cerrar los flecos que esta deja.

No obstante, si tuviésemos que poner una crítica importante a lo aquí estudiado posiblemente sea la falta de claridad ante lo que la doctrina británica denomina "journey", es decir el viaje o camino que el ciudadano debe recorrer para hacer realidad sus pretensiones. Ya que procedimentalmente ante tal amalgama de aplicaciones, la tónica general será que ante cualquier trámite específico el ciudadano se pierda entre las aplicaciones, trámites y formularios que hemos ido viendo a lo largo del trabajo.

No obstante, la oportunidad de que los propios ciudadanos comparezcan y actúen sin asistencia letrada y sin representación procesal y poniéndoles a su disposición de forma libre y gratuita los medios e instrumentos precisos para ejercer los derechos reconocidos en el artículo 5 del citado Real Decreto-Ley, es un gran avance. Además, está previsto en la norma que la ciudadanía cuente con asistencia y orientación sobre su utilización. Aunque no queda del todo claro quien estará al cargo de este cometido, si el propio personal de las oficinas judiciales en las que se ubique el domicilio de las personas necesitadas de asistencia o bien, si serán sistemas electrónicos incorporados al propio medio o instrumento en formato de chatbots. Estos sistemas automáticos alimentados con inteligencia artificial suelen ser lo más habitual en este tipo de aplicaciones, sin embargo, esto no suele ser lo más resolutivo. Por lo que en el caso de optar por estos sistemas de chatbot sería conveniente complementarlo con al menos una línea telefónica con una persona física dedicada a asistencia al ciudadano en la administración de justicia digital. No obstante, estos servicios de atención telefónica deben actuar con los criterios de seguridad[25] y con las posibilidades técnicas existentes para facilitar a los ciudadanos y ciudadanas en todo lo posible las relaciones con la Administración de Justicia en lo que se refiere a estos nuevos trámites electrónicos judiciales.

Todo ello, junto con la labor de información presencial que tienen previstos los puntos de información electrónicos ubicados en los edificios judiciales. Sin embargo, todas estas previsiones si se pretenden hacer a coste cero o con poco presupuesto podrán suponer el fracaso estrepitoso de todo el sistema de justicia electrónica accesible al ciudadano que se pretende poner en marcha.

25 Este extremo se ha convertido en un tema controvertido debido al vertiginoso avance de las tecnologías en la Administración de Justicia. Ver más en: López García-Nieto, I.: "¿Es posible llevar a la práctica en los juzgados los postulados teóricos establecidos en el Real Decreto Ley 6/23 de 19 de diciembre?", *Diario LA LEY,* 22 de febrero de 2024, núm. 10452, Sección Tribuna.

BIBLIOGRAFÍA

"Justicia avanza en el desarrollo de la Carpeta Justicia recogiendo la opinión de los profesionales y la ciudadanía", *Diario LA LEY,* 5 de febrero de 2024.

Bueno De Mata, F.: "La Justicia avanza en digitalización e Innovación", *Diario LA LEY*, 6 de febrero de 2024, núm. 10440, Sección Tribuna.

Catalán Chamorro, M.J.: *La justicia digital en España: Retos y desafíos*, Tirant Lo Blanch, Valencia, 2023.

Fierro Rodríguez, D.: "En busca del perdido apartado 5 del artículo 169 de la Ley de Enjuiciamiento Civil según el Real Decreto- ley 6/2023", *Diario LA LEY*, 14 de febrero de 2024, núm. 10446, Sección Tribuna.

López García-Nieto, I.: "¿Es posible llevar a la práctica en los juzgados los postulados teóricos establecidos en el Real Decreto Ley 6/23 de 19 de diciembre?", *Diario LA LEY*, 22 de febrero de 2024, núm. 10452, Sección Tribuna.

Olmedo, M.: "La Justicia avanza en digitalización e Innovación", *Diario LA LEY*, 6 de febrero de 2024, núm. 10440, Sección Tribuna.

Rodríguez Lainz, J.L.: "Las actuaciones procesales por videoconferencia en el proceso penal tras la publicación del Real Decreto-Ley 6/2023", *Diario LA LEY*, 13 de marzo de 2024, núm. 10465, Sección Tribuna.

DERECHO FUNDAMENTAL AL DEBIDO PROCESO Y PRESUPUESTOS EUROPEOS: EL ROL DE LA UNIÓN EUROPEA EN APOYO A LA EFICIENCIA DIGITAL DE LA JUSTICIA*

FUNDAMENTAL RIGHT TO DUE PROCESS AND EUROPEAN BUDGET: THE ROLE OF THE EUROPEAN UNION IN SUPPORTING THE DIGITAL EFFICIENCY OF JUSTICE

Actualidad Jurídica Iberoamericana Nº 21, agosto 2024, ISSN: 2386-4567, pp. 42-69

* Este trabajo ha sido escrito en el marco del proyecto de investigación "Global Commons in the Global European Strategy: a specific revision of Human Rights, Security and consideration the sea as an invaluable resource" (expediente 612053-EPP-1-2019-1-ES-EPPJMO-CHAIR), Jean Monnet Chair de la Comisión Europea, Education, Audiovisual, and Culture Executive Agency.

Rosa
CERNADA
BADÍA

ARTÍCULO RECIBIDO: 29 de mayo de 2023
ARTÍCULO APROBADO: 1 de julio de 2024

RESUMEN: La eficiencia de la justicia constituye en la actualidad una medida de la efectividad del derecho fundamental al debido proceso. En su consecución, las políticas de digitalización resultan fundamentales para descongestionar los tribunales redundando en una mayor calidad de la Administración de Justicia. Consciente de las bondades de la incorporación de la tecnología a la Administración de justicia, la Unión Europea desarrolla una notable política regulatoria y presupuestaria en apoyo a la digitalización de la Justicia cuyo impacto en la eficiencia judicial pude ser objeto de medición. El esfuerzo institucional es significativo pero la cuantificación y valoración de sus efectos se enfrenta a dificultades metodológicas que invitan a perfeccionar los sistemas de análisis de la eficiencia de la Justicia.

PALABRAS CLAVE: Debido proceso; digitalización; justicia en red; presupuestos europeos; eficiencia judicial; espacios globales comunes.

ABSTRACT: *The efficiency of justice is currently a measure of the effectiveness of the fundamental right to due process. In order to achieve this, digitalization policies are essential to decongest the courts, resulting in a higher quality of the Administration of Justice. Aware of the benefits of incorporating technology into the Administration of Justice, the European Union is developing a notable regulatory and budgetary policy to support the digitization of Justice, the impact of which on judicial efficiency can be measured. The institutional effort is significant, but the quantification and assessment of its effects faces methodological difficulties that invite to improve the systems of analysis of the efficiency of Justice.*

KEY WORDS: *Due process; digitalisation; e-justice; European budget; judicial efficiency; global commons.*

I. INTRODUCCIÓN.

El derecho al debido proceso hunde sus raíces en la Inglaterra medieval del siglo XIII en la que vio la luz la Carta Magna de Juan sin Tierra. En particular, en su cláusula 39 en la que se recoge el derecho a un proceso "de acuerdo con el derecho de la tierra". Locución que Eduardo III redefiniría casi un siglo y medio después en la definitiva cláusula 29 como derecho a un debido proceso. Ocho siglos más tarde, este derecho con terminología más o menos coincidente[1] se ha extendido en las diferentes formas de gobierno propias del Estado de Derecho[2] pero requiere de una actualización en su maridaje con los nuevos tiempos. Ya no se trata sólo del derecho a ser oído antes de ser juzgado, ni se circunscribe a expresar la sumisión a Derecho de la decisión del juzgador. En una sociedad en la que la justicia resulta un "componente fundamental para la vida de las personas (…) y para el desempeño económico"[3], la eficiencia de la justicia pasa a ser una medida de la efectividad del derecho fundamental que nos ocupa, un indicador de la evolución del Estado de Derecho y un pilar del desarrollo económico

1 Derecho a la tutela judicial efectiva en el artículo 24 de la Constitución española o garantías judiciales en la Carta Interamericana de Derechos Humanos, tal y como se desprende la de la interpretación de la Corte Interamericana de Derechos Humanos. Vid. Landa Arroyo, C.; Arangüena Fanego, C. y Ferrer Mc-Gregor, E.: "El derecho al debido proceso", en AA.VV.: *El diálogo entre los sistemas europeo y americano de derechos humanos* (ed. por F.J. García Roca; P.A. Fernández Sánchez; P. Santolaya Manchetti y R.L. Canosa Usea), 2012, Civitas, Cizur Menor (Navarra), 2012, p. 314.

2 En Francia, por ejemplo, el derecho al debido proceso se considera incorporado en el clásico artículo 16 de la Declaración de Derechos del Hombre y del Ciudadano de 1789, en el que el Conseil constitutionnel entiende reconocidas las grandes garantías procesales: derecho al recurso, derecho a un proceso público en el ámbito penal o derecho a una un proceso equitativo. Vid. Pinon, S.: "El sistema constitucional en Francia", *Revista de Derecho constitucional europeo*, 2010, núm. 14, pp. 23-24.

3 Pastor Prieto, S. y Rodríguez López, V.: "Dos dimensiones de la eficiencia de la justicia", *Economistas*, 2005, núm. 105, ejemplar dedicado a: La eficiencia de los servicios públicos: viejos problemas, nuevos enfoques, p. 103.

• Rosa Cernada Badía
Profesora de Derecho administrativo, Universidad Católica de Valencia "San Vicente Mártir". Correo electrónico: rosa.cernada@ucv.es

en la medida que coadyuva a la seguridad jurídica, en su función de inspección contractual en las relaciones civiles y de protección de los intereses privados frente a una hipotética acción expropiatoria del Estado[4].

En este nuevo escenario, la incorporación de la tecnología como personaje sobrevenido puede actuar como tabla de salvación para los saturados tribunales o constituir un fallido "Deus ex machina", al engendrar incoherencias en el propio sistema judicial a pesar de su vocación redentora orientada a mejorar los sistemas de gestión de la oficina judicial y a optimizar los tiempos requeridos por la Administración de Justicia.

II. DIGITALIZACIÓN, EFICIENCIA DE LA JUSTICIA Y DERECHO AL DEBIDO PROCESO.

1. La eficiencia de la justicia, su compleja definición y su necesaria relación con la garantía del derecho al debido proceso.

Uno de los objetivos de la digitalización de la justicia pasa por promover la eficiencia en la Administración de Justicia. Esto es así, precisamente, porque la digitalización contribuye a lograr el adecuado equilibro entre medios y fines al que remite la noción de eficiencia en el marco del fenómeno de desmaterialización[5] de los procesos. Y en particular, a hacer factible el derecho al debido proceso[6] tan maltrecho en la dimensión temporal, esto es, en el derecho a un proceso sin dilaciones indebidas reconocido en el artículo 24 de la Constitución española[7] o el derecho a un proceso dentro de un plazo razonable conforme lo declara el artículo 47 de la Carta de Derechos Fundamentales de la Unión Europea[8] o el artículo 6 del Convenio Europeo de Derechos Humanos[9].

Sin embargo, y con carácter general, a nadie se le escapa que la eficiencia aplicada a la justicia requiere una delimitación específica en la medida en que se encuentra condicionada por el objeto de la Administración de Justicia y por la heterogénea estructura administrativa que le sirve de base. En este sentido,

4 Mora-Sanguinetti, J.S.: "Justicia y economía: la eficiencia del sistema judicial en España y sus impactos económicos", *Papeles de economía española*, 2021, núm. 168 (ejemplar dedicado a: La calidad de las instituciones y la economía española), pp. 66-67.

5 Arangüena Fanego, C.: "Perspectivas de la e-Justicia en Europa", en AA.VV.: *Presente y Futuro de la e-Justicia en España y en la Unión Europea*, (coord. por C. Senés Montilla), Thomson Reuters Aranzadi, Cizur Menor (Navarra), 2010, p. 76.

6 Pérez Estrada, M.J.: "La justicia digital como eje de la modernización de la justicia", *Justicia: Revista de Derecho procesal*, 2002, núm. 2, p. 136.

7 "BOE" núm. 311, de 29 de diciembre de 1978.

8 "DOUE" núm. 202, de 7 de junio de 2016.

9 Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, hecho en Roma el 4 de noviembre de 1950, y enmendado por los Protocolos adicionales números 3 y 5, de 6 de mayo de 1963 y 20 de enero de 1966, respectivamente, "BOE" núm. 243, de 10 de octubre de 1979.

la relación entre eficiencia y justicia no ha sido pacífica desde una perspectiva doctrinal[10], en la medida en que se ha venido a considerar como medida de justicia, como un elemento o instrumento de la justicia o como concepto que, si bien camina sendas paralelas, axiológicamente no se injerta en la idea de justicia.

En todo caso, la eficiencia de la justicia se ha venido a referir al cumplimiento de los fines de la Administración de Justicia con el menor consumo de recursos públicos, sin caer en la identificación entre eficiencia y productividad[11], toda vez que la medida de la eficiencia de la justicia no debe incurrir en un mero economicismo. Por lo tanto, debe mantener el foco en su consideración como elemento clave del Estado de Derecho, de garantía del derecho al debido proceso.

En este sentido, explica Ortells[12] que la eficiencia de la justicia conlleva una doble exigencia: una primera de más compleja objetivación, que supone el respecto a las garantías procesales fundamentales y la correlativa emisión de una resolución judicial correcta; y una segunda exigencia de determinación a priori más sencilla, que pasa por cuantificar los costes directos e indirectos que genera la tramitación de los procesos y la duración de estos.

2. La compleja medida de la eficiencia de la justicia.

Una de las cuestiones clave en el análisis de la justicia en términos de política económica radica en la determinación de los criterios para una justicia eficiente. Esta cuestión no se circunscribe al sector justicia, sino que forma parte de la reflexión general sobre la medida de la eficiencia de los servicios públicos, como criterio de contención del gasto público y de sostenibilidad de los servicios en necesario maridaje con la apuesta pública por la calidad de los servicios. Sin embargo, en su aplicación a la justicia, esta labor presenta contornos muy específicos, que ponen de manifiesto la dificultad de medir la eficiencia.

Con carácter general, a la hora de valorar la eficiencia de la justicia los criterios clásicamente examinados por los analistas son los ya citados que pasan por la determinación de los costes (directos, indirectos u ocultos) y particularmente la duración de la tramitación de los procesos en la medida en que, en clásico

10 Al respecto puede citarse la conocida confrontación entre Dworkin, Posner y Calabresi a la hora de determinar la relación entre eficiencia y Justicia en el marco del análisis económico del Derecho. Vid. Dworkin, R.: "Why Efficiency? - A Response to Professors Calabresi and Posner", *Hofstra Law Review*, 1980, Vol. 8, núm. 3, Artículo 5, disponible en: http://scholarlycommons.law.hofstra.edu/hlr/vol8/iss3/5, último acceso 9 de marzo de 2024.

11 Lorizioa, M. y Gurrieri, A.R.: "Efficiency of Justice and Economic Systems", *Procedia Economics and Finance*, 2014, núm. 17, p. 105, disponible en: https://www.sciencedirect.com/science/article/pii/S2212567114008843?via%3Dihub, último acceso 10 de marzo de 2024.

12 Ortells Ramos, M.: "La eficiencia de la justicia civil: evaluación y medios de mejora", en AA.VV.: *La administración de justicia en España y en América: José Martín Ostos (liber amicorum)*, (coord. por E.C. Pérez-Luño Robledo y M.L. Domínguez Barragán; dir. por P. Martín-Ríos y M.A. Pérez Marín), Editorial Astigi, Sevilla, 2021, pp. 1419-1421.

aforismo atribuido a Séneca, "nada se parece tanto a la injusticia como la justicia tardía". Estos criterios pueden ser enriquecidos con otros como la predictibilidad o la independencia de las decisiones judiciales[13].

Por consiguiente, un adecuado estudio de la eficacia requiere analizar las distintas facetas que van componiendo el concepto y, a ser posible, relacionarlas con una finalidad valorativa. En este ejercicio se pone de manifiesto que la mayor asequibilidad del análisis cuantitativo de la justicia adquiere matices de indudable complejidad cuando se da el inevitable salto de la constatación al diagnóstico, es decir, de la descripción cuantitativa de los datos a la valoración de las causas de la ineficiencia y las posibilidades de mejora. Esta dificultad sobrevenida viene promovida, en gran medida por el sesgo ideológico[14] en la definición de una justicia eficiente[15] y la brecha en la percepción oficial, doctrinal y social de la Administración de Justicia[16].

Por lo que respecta al ámbito europeo, los estudios fundamentales en el proceso de medición y valoración de la eficiencia en la justicia son: i) en la Unión Europea, el cuadro de indicadores de la justicia, en el marco general de instrumentos que evalúan el Estado de Derecho en Europa y; ii) en el ámbito del Consejo de Europa, los informes anuales sobre los sistemas judiciales de la Comisión Europea para la Eficiencia de la Justicia del Consejo de Europa (en adelante, CEPEJ). Todo ello, sin perjuicio de otros sistemas de medición tanto de ámbito nacional[17] como internacional[18].

13 Mora-Sanguinetti, J.S.: "Justicia y economía", cit., p. 67.

14 En este sentido, puede citarse la paulatina incorporación de elementos valorativos a la cuantificación de la eficacia, centrados en las personas y sus circunstancias socioeconómicas. Una perspectiva clave para el diagnóstico de causas de la ineficacia de la justicia en países en vías de desarrollo y las propuestas de reformas legislativas inclusivas que atiendan al fomento del acceso a la justicia a sectores vulnerables de la población. Vid. Just Governance Group: "Medición del acceso a la justicia", *CoPraxis*, 2014, núm. 6, disponible en: https://justgovernancegroup.org/wp-content/uploads/2021/02/Co-Praxis_06_Es.pdf, último acceso 10 de marzo de 2024.

15 Al respecto, el Comité Económico y Social Europeo en la Observación general 4.3 de su dictamen a la Estrategia europea de e-Justicia trasciende la mera eficiencia y recupera el protagonismo del valor de la Justicia y del respeto a los derechos fundamentales de los ciudadanos. Vid. Comité Económico y Social Europeo: Dictamen sobre la "Comunicación de la Comisión al Consejo, al Parlamento Europeo y al Comité Económico y Social Europeo: Hacia una estrategia europea en materia de e-Justicia (Justicia en línea)"COM(2008) 329 final (2009/C 318/13), 30 de septiembre-1 de octubre de 2009.

16 Alcoceba Gil, J.M.: "Sobre la eficacia como medida", *Diario La Ley,* 2022, núm. 10196, Sección tribuna, pp. 2, 3 y 12.

17 En este aspecto resulta necesaria la referencia al trabajo estadístico y al ejercicio de transparencia del Consejo General del Poder Judicial español, tanto en la publicación de datos como de informes específicos en la materia. Pueden consultarse aquí, último acceso 11 de marzo de 2024.

18 Por ejemplo, en el ámbito de la OCDE. Vid. AA.VV.: "The Economics of Civil Justice: New Cross-country Data and Empirics", *OECD Economics Department Working Papers*, OECD Publishing, Paris, 2013, núm. 1060, disponible en: https://doi.org/10.1787/5k41w04ds6kf-en, último acceso 11 de marzo de 2024. Asimismo, pueden citarse otros estudios específicos de alcance regional, así en el ámbito de la Corte interamericana de Derechos Humanos o del Centro de Estudios de Justicia de las Américas (CEJA). Vid. AA.VV.: *Reporte CEJA ®. Estado de la Justicia en América Latina bajo el COVID-19 Medidas generales adoptadas y uso de TICs en procesos judiciale*s, Centro de Estudios de Justicia de las Américas - Global Affairs Canadá, mayo 2020, disponible en: https://biblioteca.cejamericas.org/handle/2015/5648, último acceso 25 de marzo de 2024.

Uno de los aspectos clave para comprender y evaluar los estudios disponibles en la materia es la valoración de la metodología utilizada y la disponibilidad de los datos. Con carácter general en la medición de la eficiencia de los servicios púbicos se parte de dos perspectivas: la presentación de indicadores de gestión, que suponen cuantificaciones parciales de aspectos concretos del servicio (metodología que se corresponde con los estudios europeos citados) o el intento de ofrecer un índice global de la eficiencia, de configuración teórica más compleja, pero que ha motivado propuestas significativas, como la basada en el uso envolvente de datos (DEA)[19]. En todo caso, la dificultad que plantea la medición de la eficacia en el ámbito europeo viene determinada precisamente por la heterogeneidad de los sistemas judiciales implicados e incluso de la distribución territorial del poder que genera dificultades a la hora de obtener determinados datos, como reconocen los propios estudios. Asimismo, la metodología utilizada suscita no pocas reservas en la medida en que la heterogeneidad de los sistemas no puede ser plasmada de forma cuantitativa en los parámetros de comparación de los Estados, de forma que pueden servir de sustento para análisis cualitativos erróneos[20].

Partiendo pues del reconocimiento de las limitaciones de los instrumentos de medición de la eficiencia de la justicia disponibles en la actualidad, el presente estudio aborda un aspecto específico de la cuantificación de los costes en la definición de una justicia eficiente en Europa. En particular, se dedica a examinar las medidas concretas de digitalización impulsadas en el ámbito europeo con el fin de promover una justicia eficiente y proponer un intento de valoración en la correlación entre digitalización y eficiencia. Todo ello, desde la perspectiva del refuerzo del derecho al debido proceso que inspira estas medidas de digitalización, tal y como ha manifestado, entre otras instituciones, el Consejo Consultivo de Jueces Europeos en su opinión sobre Justicia y Tecnologías de la información, en la que reconoce la oportunidad de la digitalización en la medida en que las tecnologías aplicadas a la justicia sirvan para facilitar el acceso a la justicia y para reforzar las garantías del derecho a un debido proceso, entre las que cita la imparcialidad, la independencia judicial, la equidad y la duración razonable de los procedimientos[21].

19 Pedraja Chaparro, F.M. y Salinas Jiménez, J.: "¿Es posible medir la eficiencia de los servicios públicos?, *Economistas,* 2005, núm. 105 (Ejemplar dedicado a: La eficiencia de los servicios públicos: viejos problemas, nuevos enfoques), p. 86.

20 Onţanu, E. A. y Velicogna, M.: "The challenges of comparing EU Member States judicial data", *Oñati Socio-Legal Series*, 2021, Vol. 11, núm. 2, pp. 446-480, disponible en: https://opo.iisj.net/index.php/osls/article/view/1180, último acceso 26 de marzo de 2024.

21 Consejo Consultivo de Jueces Europeos: Opinión núm. (2011) 14 "Justicia y Tecnologías de la Información", adoptada por el CCJE en su 12ª Reunión plenaria celebrada en Estrasburgo, 7-9 de noviembre de 2011, Apartado B.5, texto en inglés disponible en: https://rm.coe.int/168074816b, último acceso 23 de marzo de 2024.

III. DIGITALIZACIÓN DE LA JUSTICIA EN LOS ESTADOS MIEMBROS DE LA UNIÓN EUROPEA: PANORAMA GENERAL.

El desarrollo de políticas públicas que atienden a la eficiencia digital de la justicia en Europa se encuentra condicionado por el particular entramado competencial en materia de justicia que comparten Estados miembros y Unión Europea. En efecto, en virtud del artículo 4.2.j) del Tratado de funcionamiento de la Unión Europea (en adelante, TFUE)[22] y merced a las competencias específicas de la Unión en la creación de un espacio de Libertad, Seguridad y Justicia, la Unión Europea y los Estados miembros ostentan competencias compartidas en materia de justicia en los términos concretados en el Título V de la Tercera Parte del TFUE, artículos 67 a 89.

Específicamente la digitalización de la justicia como política específica se acomete a través de dos medidas fundamentales: la legislación y la financiación, dado que el objetivo de alcanzar la eficiencia digital de la justicia requiere de un marco regulatorio y de un soporte económico para la implantación de las medidas acordadas. A tal efecto, se procederá a ofrecer un panorama de la digitalización europea de la justicia en clave nacional para, seguidamente, abordar de la cuestión del rol de la Unión Europea en la materia.

1. El impulso legislativo y presupuestario a la digitalización de la justicia en el ámbito nacional.

Atendida la heterogeneidad de Estados miembros que conforman la Unión Europea y las diferentes sensibilidades en torno a la configuración de los procesos y el protagonismo de la tecnología en su desarrollo, la Comisión Europea ha examinado la digitalización nacional de la justicia en el cuadro de indicadores de la Justicia de 2023[23], con datos hasta 2021. Como punto de partida, evalúa la existencia de una regulación específica en materia de digitalización de la Justicia en los diferentes Estados miembros. Al efecto, distingue la Comisión Europea los Estados con propuestas adoptadas en materia de uso de las tecnologías de la información y la comunicación (en lo sucesivo TIC) en el sistema judicial y las que se encuentran en fase de negociación. Del estudio se pone de manifiesto que una amplia mayoría de Estados miembros ha adoptado medidas o se encuentran en fase de negociación, en concreto 18 Estados sin perjuicio de la actividad legislativa o reglamentaria de ámbito infraestatal en países de corte federal como Alemania.

22 "DOUE" núm. 83, de 30 de marzo de 2010.

23 Comisión Europea: comunicación de la comisión al parlamento europeo, al consejo, al banco central europeo, al comité económico y social europeo y al comité de las regiones Cuadro de Indicadores de la Justicia en la UE de 2023 COM/2023/309 final, p. 9.

A este respecto, conviene recordar que la relación entre las TIC y la regulación es muy particular. Así lo reconoce la CEPEJ en su último informe anual de los sistemas judiciales[24], en el que identifica dos tendencias básicas: i) regular primero para desplegar sistemas TIC a partir de esta regulación, por ejemplo, como ocurre en el caso francés y; ii) el camino opuesto, de implementar primero la tecnología, para después regular el fenómeno. El prototipo sería Letonia o Finlandia.

En todo caso, ambas tendencias terminan convergiendo en la medida en que en el primer caso se implementan progresivamente los sistemas TIC y en el segundo se terminan regulando los sistemas primeramente implantados. En todo caso, y con carácter general, desde 2020 los Estados promueven la adopción de normas procesales para la digitalización de trámites, en particular sobre el uso de la videoconferencia y la prueba digital. Con carácter general, los resultados son positivos, en 8 Estados se permite la tramitación digital de forma principal[25] y en 19 para algunas situaciones. Países como Francia o Luxemburgo tienen margen de mejora en lo que se refiere a la extensión de estas medidas a todos los asuntos. En el caso español, se presenta un alto nivel de regulación y digitalización[26].

Asimismo, la oportunidad que supone la digitalización de la justicia se puso de manifiesto por la Comisión Europea en su Comunicación sobre la digitalización de la justicia[27] de 2020, en la que reconoce la necesidad de que la Unión Europea acelere las reformas nacionales para digitalizar la gestión de asuntos judiciales, el intercambio de información entre partes y el fomento de un acceso sencillo a la justicia, sin perder de vista que la eficacia de los sistemas nacionales redunda en una más eficiente cooperación judicial transfronteriza.

El impulso legislativo no se limita estrictamente a regular los procesos específicos de digitalización, esto es, los procesos de incorporación de las tecnologías a los procesos judiciales. Debe recordarse que la eficacia digital se promueve asimismo con la toma de decisiones organizativas, administrativas o de cualquier otro carácter[28] que aseguren la armónica implantación de la tecnología en

24 Consejo de Europa-CEPEJ: *European judicial systems - CEPEJ Evaluation report – 2022 Evaluation cycle (2020 data)*, 5 de octubre de 2022, p. 115, disponible en: https://rm.coe.int/cepej-report-2020-22-e-web/1680a86279, último acceso 28 de marzo de 2024.

25 Por ejemplo, en Alemania puede citarse la paulatina introducción de herramientas de tramitación electrónica mediante instrumentos normativos diversos que ha culminado en la posibilidad de comunicarse electrónicamente con los órganos judiciales, presentar documentos o recibir notificaciones electrónicas, entre otros elementos de digitalización de los procesos. Vid. Pérez Ragone, A.: "Justicia civil en la era digital y artificial: ¿hacia una nueva identidad", *Revista Chilena de Derecho*, 2021, Vol. 48, núm. 2, p. 205.

26 Fruto del progresivo proceso de digitalización de la Justicia española en el que se enmarca la aprobación del Real Decreto-ley 6/2023, de 19 de diciembre, por el que se prueban medias urgentes y para la ejecución del Plan de Recuperación, Transformación y Resiliencia en materia de servicio público de justicia, función pública, régimen local y mecenazgo, " "núm. 303, de 20 de diciembre de 2023.

27 Comisión Europea: Comunicación de la Comisión al Parlamento europeo, al Consejo, al Comité Económico y Social europeo y al Comité de las Regiones: La digitalización de la justicia en la UE: Un abanico de oportunidades {SWD(2020) 540 final}, de 2 de diciembre de 2020.

28 Landa Arroyo, C.; Arangüena Fanego, C. y Ferrer Mc-Gregor, E.: "El derecho al debido", cit., p. 328.

la Administración de justicia. En este sentido, la propia estrategia de digitalización de la Unión Europea incluye las políticas de justicia electrónica en la política general de administración electrónica. Por lo tanto, una adecuada evaluación de las políticas de digitalización de la justicia requiere valorar medidas de digitalización administrativa general como las relativas a las políticas o medidas de protección de datos, identificación electrónica[29], ciberseguridad, etc. Y en este sentido, tampoco conviene desdeñar la importancia de la dimensión privada del sector justicia y los efectos que las reformas legislativas provocan en las profesiones jurídicas liberales (abogados, procuradores, graduados sociales, así como también los Registros o el notariado[30]).

Por su parte, y por lo que se refiere a los presupuestos nacionales de digitalización de la justicia, debe destacarse que en ocasiones los Estados no son capaces de deslindar el presupuesto para justicia del más específico de digitalización, especialmente en el caso de Estados descentralizados. En el ámbito del Consejo de Europa, con los últimos datos disponibles de 2020, se ha medido el porcentaje de presupuesto TIC sobre el presupuesto de Justicia, con un fuerte impulso de Eslovaquia, Irlanda, Dinamarca, Finlandia u Holanda[31].

2. *Statu quo* de la digitalización de la justicia en clave nacional.

Por lo que se refiere al statu quo de la digitalización en el sector justicia, más allá de impulso legislativo, disponemos de datos recientes en el cuadro de indicadores de la justicia de junio de 2023[32]. En particular, el estudio destaca en materia de publicidad activa sobre el sistema judicial la mejora respecto a otros años, ya que 26 Estados miembros ofrecen información en línea sobre su sistema judicial. En algunos casos, como la compensación para las víctimas, la publicidad es generalizada. Sin embargo, se dan diferencias entre los países. En todo caso,

29 Por ejemplo, el futuro Reglamento sobre Identidad digital europea, cuyo texto final fue aprobado por el Parlamento europeo el 29 de febrero de 2023. Vid. Parlamento Europeo: Resolución legislativa del Parlamento Europeo, de 29 de febrero de 2024, sobre la Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se modifica el Reglamento (UE) núm. 910/2014 en lo que respecta al establecimiento de un Marco para una Identidad Digital Europea (COM(2021)0281 – C9-0200/2021 – 2021/0136(COD)), disponible en: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0117_ES.html, último acceso 26 de marzo de 2024.

30 En este sentido, pueden citarse no pocos trabajos en la materia como: Calvo Vidal, I.A.: *Digitalización de la función notarial e intervención a distancia*, Bosch, Las Rozas (Madrid), 2020; Nieto Carol, U.: "Constitución en línea de sociedades limitadas", en AA.VV.: *La Digitalización en el Derecho de Sociedades. Estudio de Derecho de Sociedades. Colegio Notarial de Valencia* (dir. por U. Nieto Carol), Tirant lo Blanch, Valencia, 2024, pp. 73-174; Llopis Benlloch, J.C.: "El documento notarial electrónico", *Cuadernos de derecho transnacional*, 2023, Vol. 1; núm. 15, pp. 1090-1107; Palao Moreno, G.: "La digitalización de los registros civiles y la circulación internacional de sus certificaciones: Regulación internacional y europea", en AA.VV.: *Nuevos horizontes de la movilidad internacional de personas en el siglo XXI. Libro homenaje a la profesora Mercedes Moya Escudero* (dir. por R. Rueda Valdivia), Tirant lo Blanch, Valencia, 2023, pp. 395-420.

31 Consejo de Europa-CEPEJ: "European judicial", cit., p. 113.

32 En este apartado se analizan los resultados del Cuadro de Indicadores de la Justicia 2023 relativos a la digitalización de procesos. Vid. Comisión Europea: Cuadro de Indicadores", cit., p. 51-67.

conviene destacar que España cumple con todos los ítems, junto a Alemania, Irlanda, Letonia, Holanda, Lituania, Polonia y Suecia.

Respecto al uso de tecnologías digitales por los órganos jurisdiccionales, se ha generalizado la posibilidad de trabajo remoto, así como el uso de la videoconferencia, que se expandió principalmente tras la pandemia. En cambio, el uso de tecnologías punteras (particularmente blockchain e inteligencia artificial) es mucho más limitado. Sorprende que todavía en algunos Estados como Francia o Grecia no estén habilitados sistemas de reparto electrónico de asuntos.

Por su parte la posibilidad de entablar comunicaciones electrónicas tanto entre órganos jurisdiccionales como con el Ministerio Fiscal se encuentra generalmente implantada, en línea con la estrategia de e-justicia europea. Y responde asimismo a la tendencia que observa el Consejo de Europa en los datos de 2020. Sin embargo, algunos Estados presentan un grado de implantación parcial, como es el caso de Francia o Grecia. Asimismo, todavía un tercio de los Estados no permite la comunicación entre fiscales y abogados defensores.

Por lo que se refiere a la tramitación en línea se observa un desarrollo desigual dependiendo de las jurisdicciones. Así en asuntos civiles y mercantiles una amplia mayoría de Estados permite presentar una demanda o incoar procedimientos de forma telemática; en cambio en materia penal, la disponibilidad de soluciones digitales es limitada.

Por último, la publicación de sentencias en primera y segunda instancia ha experimentado una leve mejora, manteniéndose estable la publicación de sentencias en instancias superiores. En relación con esta cuestión resulta clave el establecimiento de sistemas que estandaricen modelos de lectura por máquina, que permite la interoperabilidad y el acceso a resoluciones judiciales. Se observa una tendencia a incorporar medidas, en particular basadas en inteligencia artificial por ejemplo para favorecer la anonimización y seudonimización del acceso a las sentencias.

El análisis de la digitalización en términos nacionales es positivo en la medida en que se observa una tendencia a incorporar mejoras y herramientas digitales y a ampliar el presupuesto en digitalización. Sin embargo, todavía existe un margen de mejora. La implantación de soluciones TIC es muy heterogénea en las diversas jurisdicciones. Por ejemplo, en Dinamarca, que de acuerdo con los datos 2020 del Consejo de Europa presentaba una diferencia de 3.2 puntos sobre 10 entre la digitalización de los tribunales contenciosos y los penales[33]. En todo caso, este

33 Ibidem, p. 120.

hecho responde a una tendencia generalizada, que implica un mayor margen para la digitalización en el ámbito penal.

Asimismo, los niveles de digitalización varían sobremanera entre los países. Si bien, la tendencia general es a invertir en sistemas de apoyo a la gestión judicial, sistemas de apoyo a la redacción de sentencias (bases de datos de jurisprudencia, antecedentes penales, ayuda a la escritura) y en sistemas de comunicación entre tribunales y profesionales de la justicia y entre partes. En el caso español destaca este último ítem.

IV. EL ROL DE LA UNIÓN EUROPEA EN EL PROCESO DE DIGITALIZACIÓN DE LA JUSTICIA EN EUROPA.

1. Las políticas de digitalización de la justicia en la Unión Europea.

Atendida la relación entre la digitalización y la eficiencia de la justicia, la Unión Europea ha desarrollado una estrategia de digitalización en el ejercicio de sus competencias compartidas con los Estados miembros para el desarrollo del espacio de libertad seguridad y justicia a partir de la estructura que le confiere la Red Judicial Europea en materia civil y mercantil y la Red Judicial Europea en materia penal.

Específicamente, la política de la Unión Europea de digitalización de la Justicia[34] parte del Programa de la Haya[35] adoptado en el Consejo Europeo de 4 y 5 de noviembre de 2004 para el periodo 2004-2009. Durante su aplicación se sentaron las bases para el futuro desarrollo de la política europea de e-Justicia, en particular, por la celebración de la conferencia internacional "Work on e-Justice" celebrada en Bremen del 29 al 31 de mayo de 2007, en la que se debatieron entre otras cuestiones, aspectos que permitirían mejorar el aspecto transnacional de la Justicia en Europa, como el portal de e-justicia, los sistemas de comunicación entre las partes y entre registros judiciales nacionales así como los modelos procesales de normalización de ámbito europeo.

La heterogeneidad de la digitalización de los distintos sistemas judiciales europeos condicionó desde un principio las políticas de digitalización europeas basadas en el principio de voluntariedad, cuya vocación de desarrollo quedó

34 Cuyas medidas específicas pueden consultarse en el portal europeo de e-Justicia. Disponible en: https://e-justice.europa.eu/home.do?action=home&plang=es, último acceso 31 de marzo de 2024.

35 "DOUE" núm. C 53, de 3 de marzo de 2005, Programa de la Haya: consolidación de la libertad, la seguridad y la justicia en la Unión Europea, disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52005XG0303(01), último acceso 22 de marzo de 2024.

asentada en los primeros años del siglo XXI. Su valoración partió del informe[36] que el Grupo de Trabajo del Artículo 29[37] realizó en 2007 en el que analizó la digitalización de los sistemas judiciales nacionales de los Estados miembros de la Unión y, a la vista de sus desajustes identificados, estableció principios generales y prioridades[38] que habían de presidir la futura acción europea en materia de digitalización de la justicia como medio de fomento de la cooperación judicial transfronteriza.

A partir de estos antecedentes, el Programa de Estocolmo[39], adoptado por el Consejo Europeo en diciembre de 2009, se refiere de forma expresa a la estrategia de justicia electrónica como medio de impulso y garantía del derecho al debido proceso, en la medida en que garantiza el acceso a la justicia y refuerza la cooperación transfronteriza en materia de justicia. La primera Estrategia Europea en materia de e-justicia o justicia en red se aprobó por la Comisión Europea en 2008[40] con el objetivo primario de "contribuir a que la justicia se administre de forma más eficaz en toda Europa, en beneficio de los ciudadanos" en colaboración con los Estados miembros. A partir de este objetivo general, la Unión desarrolló su primera estrategia e e-justicia mediante el Plan de acción plurianual 2009-2013 relativo a la Justicia en Red europea[41] sobre tres orientaciones específicas: i) la prioridad de los trabajos operativos, en particular para fomentar la aplicación de la normativa europea y promover la eficacia de la justicia y una mayor facilidad de acceso; ii) equilibrar la acción europea y la nacional desde el respeto a los principios de coordinación y de descentralización; y iii) la paulatina incorporación de las TIC a la justicia como herramienta de promoción de la eficacia con el mayor respeto posible al marco jurídico preexistente y las garantías procesales.

A partir de esta primera estrategia, la Unión Europea ha desarrollado su política de e-Justicia europea que se ha encarnado en tres estrategias posteriores (y sus planes de acción) en materia de Justicia en red:

36 Consejo Europeo – Grupo de Trabajo del Artículo 29: *Informe 10393/07 sobre e-Justicia: 393/07 JUR INFO 21 JAI 293 JUST CIV 159 COPEN 8*, disponible en: http://register.consilium.europa.eu/pdf/en/07/st10/st10393.en07.pdf, último acceso 22 de marzo de 2024.

37 Antecedente del actual Comité Europeo de Protección de datos, que lo sustituyó con la entrada en vigor del Reglamento General de Protección de Datos el 25 de mayo de 2018.

38 Desarrollo de los portales de justicia europeos y la interconexión de registros, junto con el desarrollo de determinadas tecnologías específicas como los requerimientos de pago electrónicos.

39 "DOUE" núm. C 115, de 4 de mayo de 2010, Programa de Estocolmo — Una Europa abierta y segura que sirva y proteja al ciudadano, disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:C:2010:115:FULL, último acceso 22 de marzo de 2024.

40 Comisión Europea: Comunicación de la Comisión al Consejo, al Parlamento Europeo y al Comité Económico y Social Europeo. Hacia una estrategia europea en materia de e-Justicia. SEC(2008)1947 SEC(2008)1944. COM/2008/0329 final (no publicado en Diario Oficial), disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52008DC0329, último acceso 22 de marzo de 2024.

41 "DOUE" núm. C 75/1, de 31 de marzo de 2009, disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52009XG0331(01)&qid=1712574900739, último acceso 22 de marzo de 2024.

- Proyecto de estrategia 2014-2018 relativa a la justicia en red europea[42] y el Plan de acción plurianual 2014-2018 relativo a la Justicia en red europea[43];

- Estrategia 2019-2023 relativa a la Justicia en Red Europea[44] y su Plan de Acción 2019-2023 relativo a la Justicia en Red Europea[45];

- Estrategia 2024-2028 relativa a la Justicia en Red Europea, aprobada por el Consejo de la Unión Europea el 17 de noviembre de 2023[46].

Precisamente en el desarrollo del Plan de acción 2019-2023 se ha optado liberadamente por un impulso legislativo que se ha concretado en no pocas normas que están llamadas a condicionar el desarrollo del futuro plan de acción 2024-2028 desde una perspectiva de cumplimiento normativo (trascendiendo así la tradicional voluntariedad del sistema basado en iniciativas específicas). En particular, posibilitará la ejecución, entre otras normas, del Reglamento del sistema e-CODEX[47], los reglamentos sobre notificación y traslado de documentos[48], el reglamento de pruebas electrónicas[49] así como el «paquete de digitalización»[50], todo ello mediante acciones cuya financiación podrá ser promovida por la Unión Europea.

42 "DOUE" núm. C 376/06, de 21 de diciembre de 2013, disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52013XG1221(02)&qid=1712574803961, último acceso 22 de marzo de 2024.

43 "DOUE" núm. C 182/02, de 14 de junio de 2014, disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52014XG0614(01)&qid=1712574747202, último acceso 22 de marzo de 2024.

44 "DOUE" núm. C 96/04, de 13 de marzo de 2019, disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52019XG0313(01)&qid=1712574453201, último acceso 22 de marzo de 2024.

45 "DOUE" núm. C96/05, de 13 de marzo de 2019, disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52019XG0313(02)&qid=1712574601548, último acceso 22 de marzo de 2024.

46 Disponible en: https://data.consilium.europa.eu/doc/document/ST-15509-2023-INIT/es/pdf, último acceso 28 de marzo de 2024.

47 Reglamento (UE) 2022/850 del Parlamento Europeo y del Consejo, de 30 de mayo de 2022, "DOUE" núm. 150, de 1 de junio de 2022.

48 Reglamento (UE) 2020/1784 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2020, relativo a la notificación y traslado en los Estados miembros de documentos judiciales y extrajudiciales en materia civil o mercantil ("notificación y traslado de documentos») (versión refundida) (DO L 405 de 2.12.2020, p. 40).

49 Reglamento (UE) 2023/1543 del Parlamento Europeo y del Consejo, de 12 de julio de 2023, sobre las órdenes europeas de producción y las órdenes europeas de conservación a efectos de prueba electrónica en procesos penales y de ejecución de penas privativas de libertad a raíz de procesos penales (DO L 191 de 28.7.2023, p. 118).

50 Reglamento (UE) 2023/2844 del Parlamento Europeo y del Consejo, de 13 de diciembre de 2023, sobre la digitalización de la cooperación judicial y del acceso a la justicia en asuntos transfronterizos civiles, mercantiles y penales, y por el que se modifican determinados actos jurídicos en el ámbito de la cooperación judicial, "DOUE" núm. 2844, de 27 de diciembre de 2023 y la Directiva (UE) 2023/2843, de Parlamento europeo y del Consejo por la que se modifican diversos instrumentos normativos de la Unión en lo que respecta a la digitalización de la cooperación judicial "DOUE" núm. 2843, de 27 de diciembre de 2023.

2. El impulso presupuestario de la Unión Europea a la digitalización de la justicia.

A) Instrumentos de financiación en el marco de los presupuestos europeos.

Por lo que se refiere a la financiación en la materia objeto de este estudio, los instrumentos utilizados por la Unión Europea son todos aquellos que permitan la transición digital de la justicia y, en particular, los presupuestos relativos no solo a la digitalización, sino también a otros aspectos conexos, que vienen a complementar los instrumentos nacionales de digitalización de la justicia.

Los presupuestos europeos presentan unas notas particulares que los diferencian de los presupuestos de otras instituciones u organismos internacionales[51], específicamente[52]: i) sus dimensiones, que limitan el impacto de la acción presupuestaria europea; ii) su estructura de gastos y el equilibrio entre ingresos y gastos, conforme al artículo 310 del TFUE, que impide el uso del empréstito para financiar déficits presupuestarios; iii) su autonomía financiera merced a la financiación primordial con recursos propios conforme al artículo 311 del TFUE; y iv) su estructura de financiación y su ejecución en un marco financiero plurianual para un periodo mínimo de cinco años, estableciendo límites de pago para cada ejercicio presupuestario, de acuerdo con el principio de anualidad, y límites de compromisos para las diversas categorías de gastos de la Unión. De esta forma, los presupuestos devienen un instrumento clave en la definición y ejecución de las políticas públicas europeas, entre otras, el apoyo a la digitalización de la Justicia, que aquí nos ocupa.

Los presupuestos europeos vigentes parten del siguiente marco legislativo básico conformado, entre otros instrumentos normativos, por: el Marco Financiero plurianual para el periodo 2021-2027[53] que establece un nivel máximo de gasto de 1.074.000 millones de euros[54], el Instrumento de Recuperación[55], el Acuerdo

51 Señaladas por Samblas Quintana, E.: "El presupuesto de la Unión Europea y su integración en el presupuesto español", *Crónica presupuestaria*, 2016, núm. 4, p. 57.

52 Sin perjuicio de otros principios o reglas de interés como la controvertida condicionalidad en teórica defensa del Estado de Derecho. *Vid.* Kölling, M.: "La condicionalidad para la protección del presupuesto de la Unión Europea: ¿una protección del Estado de Derecho o una garantía para los intereses financieros de la UE?", *Revista de derecho constitucional europeo*, enero-junio 2022, núm. 37 (Ejemplar dedicado a: Democracia y Estado de Derecho en la Unión Europea), pp. 87-102.

53 Reglamento (UE, EURATOM) 2020/2093 del Consejo, de 17 de diciembre de 2020, por el que se establece el marco financiero plurianual para el período 2021-2027, "DOUE" núm. L413 I/11, de 22 de diciembre de 2020. Ha sido modificado, la versión consolidada de 1 de enero de 2024, disponible con un mero valor documental en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A02020R2093-20240101, último acceso 24 de marzo de 2024.

54 Así como niveles máximos de otros proyectos o instrumentos especiales como el fondo Europeo de Adaptación a la Globalización o el Instrumento de Flexibilidad para cubrir gastos imprevistos.

55 Reglamento (UE) 2020/2094 del Consejo de 14 de diciembre de 2020 por el que se establece un Instrumento de Recuperación de la Unión Europea para apoyar la recuperación tras la crisis de la COVID-19, "DOUE" núm. L 433I I/23, de 22 de diciembre de 2020.

interinstitucional sobre disciplina presupuestaria[56]; el Reglamento Financiero de 2018[57] y la Decisión sobre Recursos Propios[58].

De acuerdo con este marco legislativo, las políticas de digitalización de la justicia se benefician específicamente del programa "Justicia 2021-2027"[59] que sustituye al anterior programa para el periodo 2014-2020[60]. Si bien es cierto que el programa Justicia es lineal y no se enriquece con contribuciones de otros programas, presenta puntos de conexión o incluso sinergias con otros programas o herramientas presupuestarias europeas en su objetivo de fomentar la digitalización de la Justicia. A estos efectos, puede citarse (entre otros):

- el programa "Europa digital"[61] con 7.500 millones de euros a precios corrientes.

- el Mecanismo de Recuperación y Resiliencia para la Financiación, en el Marco general del Fondo de recuperación ya citado, para apoyar la investigación y reformas nacionales y promover una recuperación sostenible y una transición digital. Está dotado con 672.500 millones de euros y requiere la aprobación de un Plan Nacional de Recuperación y Resiliencia[62];

- el Instrumento de Apoyo Técnico que ofrece, previa solicitud nacional, apoyo técnico a los Estados miembros en la ejecución de las reformas; en particular para preparar los planes de recuperación y resiliencia en el marco del Mecanismo de Recuperación y Resiliencia. Cuenta con una dotación de 864 millones de euros

56 Acuerdo interinstitucional entre el Parlamento Europeo, el Consejo de la Unión Europea y la Comisión Europea, de 16 de diciembre de 2020, sobre disciplina presupuestaria, cooperación en materia presupuestaria y buena gestión financiera, así como sobre nuevos recursos propios, en particular una hoja de ruta para la introducción de nuevos recursos propios, "DOUE" núm. 433 I/28, de 22 de diciembre de 2020, pp. 28-46.

57 Reglamento (UE; Euratom) 2018/1046 del Parlamento Europeo y del Consejo, de 18 de julio de 2018, sobre las normas financieras aplicables al presupuesto general de la Unión, por el que se modifican los Reglamentos (UE) núm. 1296/2013, (UE) núm.1301/2013, (UE) núm. 1303/2013, (UE) núm.1304/2013, (UE) núm. 1309/2013, (UE) núm.1316/2013, (UE) núm. 223/2014 y (UE) núm.283/2014 y la Decisión núm. 541/2014/UE y por el que se deroga el Reglamento (UE, Euratom) núm.966/2012, "DOUE" núm. L193, de 30 de julio de 2018.

58 Decisión (UE, Euratom) 2020/2053 del Consejo, de 14 de diciembre de 2020, sobre los sistemas de recursos propios de la Unión Europea y por la que se deroga la Decisión 2014/335/UE, Euratom "DOUE" núm. L424, de 15 de diciembre de 2020.

59 Reglamento (UE) 2021/693 del Parlamento Europeo y del Consejo de 28 de abril de 2021 por el que se establece el programa Justicia y por el que se deroga el Reglamento (UE) núm. 1382/2013, "DOUE" núm. 156, de 5 de mayo de 2021, pp. 21-38.

60 Reglamento (UE) núm. 1382/2013 del Parlamento Europeo y del Consejo, de 17 de diciembre de 2013, "DOUE" núm. L354/73 de 28 de diciembre de 2013.

61 Reglamento (UE) 2021/694 del Parlamento Europeo y del Consejo de 29 de abril de 2021, por el que se establece el Programa Europa Digital y por el que se deroga la Decisión (UE) 2015/2240 (Texto pertinente a efectos del EEE), "DOUE" núm. 166, de 11 de mayo de 2021, pp. 21-38.

62 El plan español puede consultarse en: Benito Ferrero, M. y Calderero Parlange, C.: "Especificidades presupuestarias de los créditos del Mecanismo de Recuperación y Resiliencia", *Revista española de control externo*, 2021, vol. XXIII, núm. 69, pp. 26-41.

para el período 2021-2027 (a precios corrientes). Por esta vía, por ejemplo, se ha financiado la estrategia de justicia digital de Malta para 2022-2027.

- Los Instrumentos de Política de Cohesión 2021-2027 en el marco del Fondo Europeo de Desarrollo Regional y del Fondo Social Europeo Plus. Todo ello en correlación con las recomendaciones por país del Semestre Europeo[63], que han reconocido la prioridad de la digitalización de la justicia para algunos Estados, como Croacia (2016), Chipre (2017), Bélgica (2018) y Grecia (2020).

- Otras fuentes de financiación que pueden vincularse con la estrategia de digitalización de la justicia por conexión con los aspectos estructurales o la consideración amplia de las políticas administrativas son, entre otros, el Programa Horizonte Europa o el Mecanismo Conectar Europa para infraestructuras digitales.

B) El programa Justicia y sus actuales proyectos de digitalización.

El programa Justicia presenta como objetivo general el desarrollo de un área europea de justicia basada en los valores europeos y en el Estado de Derecho y el fortalecimiento de los derechos fundamentales. Entre sus objetivos específicos destaca, a los efectos de este trabajo, el fomento de la cooperación judicial y del acceso a la justicia, en su caso, mediante herramientas de e-justicia.

La última convocatoria del programa Justicia, para apoyar proyectos transnacionales en los ámbitos de la justicia en red, los derechos de las víctimas y los derechos procesales[64], cuyo plazo de presentación terminó el 4 de octubre de 2023 dispone de un fondo de más de 10 millones de euros. En la actualidad, se están ejecutando 12 proyectos[65] en el marco de las convocatorias 2012 y 2022 del programa Justicia referidos específicamente al ámbito de la justicia electrónica. En concreto, respecto al subprograma "ejustice" de 2021 los siguientes proyectos:

- iSupport Spain para la implantación desde cero en España de la gestión electrónica de expedientes para el cobro transfronterizo de obligaciones de alimentos ("Portal iSupport") y la infraestructura subyacente e-CODEX. Con una dotación de 320.770,49 euros, su ejecución está prevista del 1 junio 2022 a 31 de mayo de 2024.

63 Comisión Europea: *Base de datos de las recomendaciones específicas por país del Semestre europeo*. Disponibles en: https://ec.europa.eu/economy_finance/country-specific-recommendations-database/, último acceso 24 de marzo de 2024.

64 Texto disponible en: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/just/wp-call/2023-2024/call-fiche_just-2023-jacc-ejustice_en.pdf, último acceso 24 de marzo de 2024.

65 Se ofrece un resumen de los proyectos en ejecución del programa e-justice, dentro del programa Justicia 2021-2027, de acuerdo con la información facilitada por la Comisión Europea en su página web oficial, accesible aquí, último acceso 24 de marzo de 2024.

- i-ACCESS MyRights es un sistema que permite mejorar el acceso a la información y la asistencia jurídica en el ámbito de la justicia electrónica para los niños víctimas en la Unión Europea mediante una solución basada en inteligencia artificial. Coordinada desde Hungría, y con una dotación de 789.597,41 euros, participan instituciones de Hungría, Bulgaria, Grecia, Rumanía, Bélgica y Holanda. Su ejecución se prevé del 1 junio 2023 a 31 de diciembre de 2024.

- Implementación de iSupport y de e-CODEX en Suecia, en particular, para su uso por los asistentes sociales. Con una dotación de 449.719,00 euros, su ejecución en 25 meses estaba prevista para el 29 de febrero de 2024.

- Implementación de "Busca un Experto II" en Francia con una dotación de 324.828,85 euros. Su finalidad es integrar a expertos judiciales en el proceso de justicia electrónica y la creación de registros electrónicos de expertos como fase previa de los futuros intercambios electrónicos de peritajes nacionales y transfronterizos. Su ejecución bianual estaba prevista para el 29 de febrero de 2024.

- El proyecto E-Justice ODR Scheme, con una dotación de 522.084,97 euros, se coordina por Italia (European University Institute) con participación de República Checa, Portugal, Holanda y Polonia. Su objetivo es desarrollar el Esquema E-Justice ODR como una herramienta digital que facilitará el acceso a la justicia para las personas, especialmente las personas vulnerables en la resolución extrajudicial de conflictos. Su ejecución estaba prevista para el 31 de enero de 2024.

- CREA2 (con el precedente de CREA (2017-2019) es un proyecto para impulsar el desarrollo de herramientas de inteligencia artificial (que se distribuirán como código abierto[66]) para la resolución extrajudicial de conflictos civiles por aplicación de algoritmos de teoría de juegos (GT) y el establecimiento de una base común europea de derechos disponibles (ECGAR). Está coordinado por Vrije Universiteit Brussel (Bélgica), con participación de Italia, Eslovenia, Lituania, Croacia, Francia y Estonia y una dotación de 710.838,45 euros. Su ejecución está prevista del 1 de junio 2022 al 31 de mayo de 2024.

Por su parte, el subprograma "e-justice 2022" se encuentra financiando los siguientes proyectos:

- Simplificación de la videoconferencia transnacional (cuyo periodo de ejecución comprende del 1 de abril de 2023 al 31 de marzo de 2025), Está coordinado por

66 En línea con el principio operativo f) de la Estrategia europea de Justicia en línea para 2024-2028, con el fin de minimizar costes, contribuir a la transparencia y la interoperabilidad, así como al control de las autoridades judiciales.

el Ministerio de Justicia austríaco, cuenta con una dotación de 671.890,88 euros y con instituciones beneficiarias en Grecia, Polonia, Alemania, España y Portugal;

- POLINE (a ejecutar del 1 de enero de 2024 a 31 de diciembre de 2025) es una herramienta basada en inteligencia artificial para el análisis jurisprudencial en materia del Impuesto sobre el Valor Añadido del Tribunal de Justicia de la Unión Europea y la jurisprudencia nacional. Con una dotación de 684.064,60 euros, está coordinado por la Universidad de Bolonia (Italia) y sus instituciones beneficiarias son, además de italianas, búlgaras y suecas.

- ICANEPO, en ejecución desde el 1 de abril de 2023 hasta el 31 de marzo de 2025, para el desarrollo de comunicaciones electrónicas transfronterizas en materia de órdenes de pago europeas basado en el uso de e-CODEX por las autoridades judiciales nacionales. Coordinado por el Ministerio de Justicia austríaco y con una dotación de 1.338.315,76 euros, participan en el proyecto instituciones de Grecia, Portugal y Holanda.

- Implementación de "Encuentre un abogado II" en Letonia y Bulgaria, bajo la coordinación letona. Está dotado con 404.514,60 euros y su ejecución está prevista del 1 de enero de 2023 al 31 de diciembre de 2024.

- ECRIS-TCN es un proyecto dotado con 359.999,23 euros y coordinado por Francia para mejorar el intercambio de antecedentes penales de nacionales de terceros países a partir de datos biométricos haciendo uso del enfoque Agile. Su ejecución se prevé entre el 1 de enero de 2024 y el 31 de marzo de 2025.

- Desarrollo del ECLI en Lituania en el periodo comprendido entre el 1 de noviembre de 2022 y el 31 de octubre de 2024 con una dotación de 159.113,8 euros.

El examen de los diversos proyectos actualmente financiados por el programa Justicia en el ámbito de la justicia electrónica pone de manifiesto las diversas velocidades en materia de digitalización presentes en los diferentes Estados miembros y el papel clave de las políticas de financiación europea para apoyar proyectos concretos que cristalicen en una mayor homogeneización que redundará, en último término, en una protección más eficaz el derecho al debido proceso en sede nacional y en perspectiva transfronteriza.

C) La ejecución de los presupuestos europeos con impacto en la digitalización de la justicia en desarrollo del Plan de Acción 2019-2023 relativo a la Justicia en red Europea.

Precisamente estas diferentes velocidades en la digitalización comprometen los objetivos de la Unión Europea en materia de justicia en red, cuya finalidad

fundamental es "contribuir a que la justicia se administre de forma más eficaz en toda Europa, en beneficio de los ciudadanos".

Las bondades del desarrollo de estas políticas de e-justicia son de sobra conocidas: el portal europeo de e-justicia, fortalecimiento de estructuras de cooperación, como Eurojust u otras medidas más concretas orientadas a la interoperabilidad como legivoc. Por lo que se refiere al plan de acción, ya en conclusión, establece 26 proyectos prioritarios incardinados en los tres objetivos básicos de la estrategia: el acceso a la información, las comunicaciones electrónicas y la interoperabilidad.

Algunos de estos proyectos han sido culminados o están en vías de serlo. Se observa una mayor facilidad de implantación en aquellos aspectos relativos a la publicidad general o los que operan como preparación para futuros desarrollos técnicos. Así:

- la incorporación de mejoras en el portal europeo de e-justicia (proyecto nº1);

- la fase II del proyecto subastas judiciales, cuya culminación estaba prevista el 30 de noviembre de 2023 por ejecución del proyecto LEILA financiado con más de un millón de euros;

- la interconexión de los registros de propiedad de la Unión Europea (proyecto nº2), que se está llevando a cabo con la creación de la European Land Registry Asociation (ELRA) y el desarrollo de los proyectos IMOLA –Interperability Model of Land Registers-, o CROBECO –Cross Border Electronic Conveyancing.

Asimismo, los proyectos que se alinean con el desarrollo tecnológico nacional presentan una mayor tasa de cumplimiento. Es el caso del proyecto 20 sobre videoconferencia, por el que además ha apostado la Comisión Europea en el "programa Justice" ya citado.

Sin embargo, la heterogeneidad de los Estados plantea retos para la implantación de proyectos específicos. En el caso de los proyectos 6 a 9 sobre acceso a los datos jurídicos, en particular, por ejemplo, las mejoras y la generalización de los identificadores europeos. En este sentido, todavía se encuentra en proceso de introducción el uso de ECLI en algunos países de la Unión, como el caso de Lituania expuesto *supra*.

Otros proyectos pendientes son el establecimiento de "chatbot" o la posibilidad de pago online de tasas judiciales en el portal de "e-justice" o la Fase II del programa encuentra un abogado. Al respecto todavía se está implementando la fase I en algunos Estados de los que todavía no se disponía de información, es

el caso de Bulgaria que recibe más de 200.000 euros del programa Justicia, que culminará en diciembre de 2024.

En todo caso, en la ejecución del plan de acción se han realizado no pocos avances o estudios de interés. En particular, resultan de necesaria referencia dos estudios que se han desarrollado en ejecución del plan: el estudio sobre Justicia Penal Digital[67] y el estudio sobre el Uso de Tecnologías innovadoras en el ámbito de la Justicia[68]. En este segundo, la Comisión Europea analiza casi un centenar de proyectos desarrollados en Europa[69]. La mayoría de estos proyectos (46%) tienen por objeto el tratamiento de grandes volúmenes de datos estructurados y no estructurados para su análisis. Otros proyectos se refieren al tratamiento de vídeo de alto valor (18%), el acceso a la justicia (15%), el cumplimiento de la protección de datos (14%) o Blockchain (17%), entre otros. Y por supuesto, uso de sistemas de inteligencia artificial de riesgo diverso, siendo los proyectos relativos a sistemas de automatización de procesos los más numerosos (34% de los proyectos), sin perjuicio de otros, como los proyectos para anonimización y pseudoanonimización o para optimización de búsquedas.

En el horizonte del periodo 2024-2028, los objetivos confesos de la estrategia de justicia en red europea se orientan a la promoción o mejora de la cooperación judicial digital, la innovación en justicia digital y el acceso a la justicia digital y la eficacia de la justicia digital como vertientes digitales del derecho al debido proceso. Particularmente (entre otras), con medidas concretas para la mejora del Portal de e-Justicia y EUR-Lex en términos de estructura y accesibilidad, la capacitación de usuarios de la justicia y la promoción de tecnologías específicas en materia de gestión procesal (como la automatización robótica y de procesos o el reparto automático de asuntos), la anonimización de resoluciones judiciales o las herramientas de resolución de litigios en línea[70].

V. ¿ES LA DIGITALIZACIÓN EL CAMINO HACIA LA EFICIENCIA DE LA JUSTICIA EN EUROPA?

La acción presupuestaria de la Unión Europea en el apoyo a la digitalización de la justicia resulta clave en la medida en que la digitalización aporta una mayor

67 Comisión Europea – Dirección General de Justicia y Consumidores: *Cross-border digital criminal justice – Final report*, Publications Office, 2020, https://data.europa.eu/doi/10.2838/118529, último acceso 28 de febrero de 2024.

68 Comisión Europea – Dirección General de Justicia y Consumidores: *Study on the use of innovative technologies in the justice field – Final report*, Publications Office, 2020, https://data.europa.eu/doi/10.2838/585101, último acceso 28 de marzo de 2024.

69 Puede consultarse un análisis del estudio en: Cernada Badía, R.: "De la digitalización a la Inteligencia artificial: el porvenir de la Justicia en la Unión Europea" en AA.VV.: *Algoritmos abiertos y que no discriminen en el sector público* (coord. por L. Cotino Hueso y J. Castellanos Claramunt), Tirant lo Blanch, Valencia, 2023, pp. 259-262.

70 Comisión Europea: Estrategia 2024-2028, cit., p. 20.

calidad de la actividad procesal, en particular en las funciones automatizables (como las comunicaciones electrónicas o la tramitación interna) que pueden coadyuvar a descongestionar los tribunales. Sin embargo, el condicionamiento económico y cultural genera velocidades diversas entre los distintos Estados de la Unión Europea, así como diferente implantación por órdenes jurisdiccionales, siendo menor en el penal. Esta cuestión es objeto de atención en la estrategia europea de justicia en red para el periodo 2024-2028 al exigir expresamente la persecución paralela de los objetivos estratégicos en las jurisdicciones civil y penal, con las necesarias adaptaciones que requieren las especialidades de estos órdenes jurisdiccionales.

En consecuencia, del examen de las acciones de financiación y de los principales informes sobre eficiencia de la Justicia en Europa puede concluirse que la digitalización no es sinónimo de eficiencia. En este sentido, y como punto de partida, conviene tener en cuenta que los efectos de la digitalización, como los de las reformas, requieren de un cierto tiempo en manifestarse. El cuadro de indicadores de la Unión analiza esta cuestión. El estudio habla de tendencias positivas que suponen un retorno a los niveles de 2019 tras la debacle que supuso la pandemia. No puede negarse que la digitalización exprés para afrontar los efectos del Covid-19 tuvo mucho que ver en esta recuperación, pero lo cierto es que la reducción de tiempos no es ni generalizada ni aplicable a todos los asuntos. Por tanto, no puede afirmarse que un mayor nivel de digitalización se traduzca de forma necesaria y correlativa en una disminución de la tasa de disposición, es decir, en una correspondiente reducción de duración de los procesos. Sin embargo, las tasas de resolución son elevadas, por lo que la tendencia parece orientar a una mejora progresiva, aunque las tasas de resolución de asuntos pendientes se mantienen estables (en España, se siente cierta a mejora en el ámbito contencioso administrativo).

Pero la efectividad de la digitalización no depende solo de la implantación sino también de otros aspectos fundamentales como la gobernanza de la Justicia o de la implantación de las TIC, la formación técnica de los usuarios y cambio cultural en la forma de trabajo, por ejemplo, a la que se atiende con la Estrategia europea sobre formación judicial 2021-2024 o los objetivos operativos de capacitación para el periodo 2024-2028.

Además, la eficiencia digital está condicionada por los problemas estructurales de la Administración de Justicia de algunos Estados miembros, que se ponen de manifiesto, entre otros, en las recomendaciones del Semestre europeo. Así, por ejemplo, se observa que Estados con fuertes tasas de digitalización como los países bálticos, Austria o Eslovaquia presentan unos niveles de eficiencia adecuados, sin embargo, en Estados como España, con un elevado nivel de digitalización, los

problemas estructurales de saturación de los tribunales se mantienen y, por lo tanto, requieren medidas adicionales (fundamentalmente de orden regulatorio y organizativo) que acompañen a la digitalización[71].

Por todo ello, siendo fundamental la inversión en tecnología para promover una justicia eficiente, la medida de la eficiencia debe relacionar la implementación de tecnologías con otros datos como, por ejemplo, la duración de los procesos, las tasas de litigiosidad o de resolución o la calidad e independencia de las resoluciones judiciales. La medida de estas cuestiones sigue constituyendo un reto, en particular por la complejidad de los sistemas judiciales y el número de variables que afectan a su rendimiento[72]. La metodología oficialmente seguida, que opta por en análisis parcial de indicadores específicos, parece adecuada. Un indicador global de eficiencia se antoja un objetivo todavía demasiado ambicioso, toda vez que la heterogeneidad de los sistemas comparados y la dificultad, en ocasiones, de obtener datos adecuados condiciona, y mucho, la metodología de valoración[73]. Por lo tanto, a pesar de los esfuerzos de orden regional e internacional, conviene seguir trabajando en el desarrollo de sistemas de medición de eficacia que sirvan de apoyo a la adopción de políticas públicas.

En todo caso, conviene destacar la coherencia de las políticas de digitalización de la justicia de la Unión Europea, en la medida en que, de acuerdo con los valores fundacionales y el sistema de competencias de los tratados constitutivos, orienta sus esfuerzos regulatorios y presupuestarios a la promoción del derecho al debido proceso. Un objetivo en consonancia con los principios sustantivos de respeto a los derechos fundamentales y el Estado de Derecho en los que se sustenta la Unión Europea y que sitúa a la persona como centro, como piedra angular de la transformación digital de la Unión.

71 Así, por ejemplo, en el caso de Italia la adopción adecuada de mejores prácticas por parte de los tribunales se ha llegado a proponer como criterio más significativo de mejora de la eficiencia en términos de duración de los procedimientos calculándose una disminución de hasta un tercio del tiempo total para completar un juicio. Vid Peyrache, A. y Zago, A.: "The (in)efficiency of Justice. An equilibrium analysis of supply policies", *CEPA Working Papers Series*, 2020, WP042020, p. 34.

72 Consejo de Europa, "European judicial", cit., p. 121.

73 Por ejemplo, en cuestiones tan básicas como la determinación del concepto de "caso" o "proceso" o su naturaleza, Vid. On□anu, E. A. y Velicogna, M.: "The challenges", cit., p. 464.

BIBLIOGRAFÍA

AA.VV.: *Reporte CEJA ®. Estado de la Justicia en América Latina bajo el COVID-19 Medidas generales adoptadas y uso de TICs en procesos judiciales*, Centro de Estudios de Justicia de las Américas - Global Affairs Canadá, mayo 2020, disponible en: https://biblioteca.cejamericas.org/handle/2015/5648, último acceso 25 de marzo de 2024.

AA.VV.: "The Economics of Civil Justice: New Cross-country Data and Empirics", *OECD Economics Department Working Papers*, OECD Publishing, Paris, 2013, Núm. 1060, https://doi.org/10.1787/5k41w04ds6kf-en, último acceso 11 de marzo de 2024.

Alcoceba Gil, J.M.: "Sobre la eficacia como medida", *Diario La Ley,* 2022, núm. 10196, Sección tribuna, pp. 1-20.

Arangüena Fanego, C.: "Perspectivas de la e-Justicia en Europa", en AA.VV.: *Presente y Futuro de la e-Justicia en España y en la Unión Europea*, (coord. por C. Senés Montilla), Thomson Reuters Aranzadi, Cizur Menor (Navarra), 2010, pp. 29-81.

Benito Ferrero, M. y Calderero Parlange, C.: "Especificidades presupuestarias de los créditos del Mecanismo de Recuperación y Resiliencia", *Revista española de control externo*, 2021, vol. XXIII, núm. 69, pp. 26-41.

Calvo Vidal, I.A.: *Digitalización de la función notarial e intervención a distancia*, Bosch, Las Rozas (Madrid), 2020.

Cernada Badía, R.: "De la digitalización a la Inteligencia artificial: el porvenir de la Justicia en la Unión Europea" en AA.VV.: *Algoritmos abiertos y que no discriminen en el sector público* (coord. por L. Cotino Hueso y J. Castellanos Claramunt), Tirant lo Blanch, Valencia, 2023, pp. 239-264.

Comisión Europea: Base de datos de las recomendaciones específicas por país del Semestre europeo. Disponibles en: https://ec.europa.eu/economy_finance/country-specific-recommendations-database/, último acceso 24 de marzo de 2024.

Comisión Europea – Dirección General de Justicia y Consumidores: *Cross-border digital criminal justice – Final report*, Publications Office, 2020, https://data.europa.eu/doi/10.2838/118529, último acceso 28 de febrero de 2024.

Comisión Europea – Dirección General de Justicia y Consumidores: *Study on the use of innovative technologies in the justice field – Final report,* Publications Office,

2020, https://data.europa.eu/doi/10.2838/585101, último acceso 28 de marzo de 2024.

Comité Económico y Social Europeo: Dictamen sobre la «Comunicación de la Comisión al Consejo, al Parlamento Europeo y al Comité Económico y Social Europeo: Hacia una estrategia europea en materia de e-Justicia (Justicia en línea)» COM(2008) 329 final (2009/C 318/13), 30 de septiembre-1 de octubre de 2009.

Consejo Europeo – Grupo de Trabajo del Artículo 29: *Informe 10393/07 sobre e-Justicia: 393/07 JUR INFO 21 JAI 293 JUST CIV 159 COPEN 8*, disponible en: http://register.consilium.europa.eu/pdf/en/07/st10/st10393.en07.pdf, último acceso 22 de marzo de 2024.

Consejo Consultivo de Jueces Europeos: Opinión núm. (2011) 14 "Justicia y Tecnologías de la Información", adoptada por el CCJE en su 12ª Reunión plenaria celebrada en Estrasburgo, 7-9 de noviembre de 2011, texto en inglés disponible en: https://rm.coe.int/168074816b, último acceso 23 de marzo de 2024.

Consejo de Europa – CEPEJ: *European judicial systems - CEPEJ Evaluation report – 2022 Evaluation cycle (2020 data)*, 5 de octubre de 2022, disponible en: https://rm.coe.int/cepej-report-2020-22-e-web/1680a86279, último acceso 28 de marzo de 2024.

Dworkin, R.: "Why Efficiency? - A Response to Professors Calabresi and Posner", *Hofstra Law Review*, 1980, Vol. 8, núm. 3, Artículo 5, disponible en: http://scholarlycommons.law.hofstra.edu/hlr/vol8/iss3/5, último acceso 9 de marzo de 2024.

Just Governance Group: "Medición del acceso a la justicia", *CoPraxis*, 2014, núm. 6, disponible en: https://justgovernancegroup.org/wp-content/uploads/2021/02/Co-Praxis_06_Es.pdf, último acceso 10 de marzo de 2024.

Kölling, M.: "La condicionalidad para la protección del presupuesto de la Unión Europea: ¿una protección del Estado de Derecho o una garantía para los intereses financieros de la UE?", *Revista de derecho constitucional europeo*, enero-junio 2022, núm. 37 (Ejemplar dedicado a: Democracia y Estado de Derecho en la Unión Europea), pp. 87-102.

Landa Arroyo, C.; Arangüena Fanego, C. y Ferrer Mc-Gregor, E.: "El derecho al debido proceso", en AA.VV.: *El diálogo entre los sistemas europeo y americano de derechos humanos* (editado por F.J. García Roca; P.A. Fernández Sánchez; P. Santolaya Manchetti y R.L. Canosa Usea), Civitas, Cizur Menor (Navarra), 2012, pp. 311-350.

Llopis Benlloch, J.C.: "El documento notarial electrónico", *Cuadernos de derecho transnacional*, 2023, Vol. 1; núm. 15, pp. 1090-1107.

Lorizioa, M. y Gurrieri, A.R.: "Efficiency of Justice and Economic Systems", *Procedia Economics and Finance,* 2014, núm. 17, pp. 104-112, disponible en: https://www.sciencedirect.com/science/article/pii/S2212567114008843?via%3Dihub, último acceso, 10 de marzo de 2024.

Mora-Sanguinetti, J.S.: "Justicia y economía: la eficiencia del sistema judicial en España y sus impactos económicos", *Papeles de economía española*, 2021, núm. 168 (ejemplar dedicado a: La calidad de las instituciones y la economía española), pp. 66-77.

Nieto Carol, U.: "Constitución en línea de sociedades limitadas", en AA.VV.: *La Digitalización en el Derecho de Sociedades. Estudio de Derecho de Sociedades. Colegio Notarial de Valencia* (dir. por U. Nieto Carol), Tirant lo Blanch, Valencia, 2024, pp. 73-174.

Onțanu, E. A. y Velicogna, M.: "The challenges of comparing EU Member States judicial data", *Oñati Socio-Legal Series*, 2021, Vol. 11, núm. 2, pp. 446-480, disponible en: https://opo.iisj.net/index.php/osls/article/view/1180, último acceso 26 de marzo de 2024.

Ortells Ramos, M.: "La eficiencia de la justicia civil: evaluación y medios de mejora", en AA.VV.: *La administración de justicia en España y en América: José Martín Ostos (liber amicorum)*, (coord. por E.C. Pérez-Luño Robledo y M.L. Domínguez Barragán; dir. por P. Martín-Ríos y M.A. Pérez Marín), Editorial Astigi, Sevilla, 2021, pp. 1417-1462.

Palao Moreno, G.: "La digitalización de los registros civiles y la circulación internacional de sus certificaciones: Regulación internacional y europea", en AA.VV.: *Nuevos horizontes de la movilidad internacional de personas en el siglo XXI. Libro homenaje a la profesora Mercedes Moya Escudero* (dir. por R. Rueda Valdivia), Tirant lo Blanch, Valencia, 2023, pp. 395-420.

Parlamento Europeo: Resolución legislativa del Parlamento Europeo, de 29 de febrero de 2024, sobre la Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se modifica el Reglamento (UE) núm. 910/2014 en lo que respecta al establecimiento de un Marco para una Identidad Digital Europea (COM(2021)0281 – C9-0200/2021 – 2021/0136(COD)), disponible en: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0117_ES.html, último acceso 26 de marzo de 2024.

PASTOR PRIETO, S. y RODRÍGUEZ LÓPEZ, V.: "Dos dimensiones de la eficiencia de la justicia", *Economistas*, 2005, núm. 105, ejemplar dedicado a: La eficiencia de los servicios públicos: viejos problemas, nuevos enfoques, pp. 103-114.

PEDRAJA CHAPARRO, F.M. y SALINAS JIMÉNEZ, J. "¿Es posible medir la eficiencia de los servicios públicos?", *Economistas,* 2005, núm. 105 (Ejemplar dedicado a: La eficiencia de los servicios públicos: viejos problemas, nuevos enfoques), pp. 86-94.

PÉREZ ESTRADA, M.J.: "La justicia digital como eje de la modernización de la justicia", *Justicia: Revista de Derecho procesal*, 2002, núm. 2, pp. 133-160.

PÉREZ RAGONE, A.: "Justicia civil en la era digital y artificial: ¿hacia una nueva identidad", *Revista Chilena de Derecho*, 2021, Vol. 48, núm. 2, pp. 203-209.

PEYRACHE, A. y ZAGO, A.: "The (in)efficiency of Justice. An equilibrium analysis of supply policies", *CEPA Working Papers Series*, 2020, WP042020, pp. 1-46.

PINON, S.: "El sistema constitucional en Francia", *Revista de Derecho constitucional europeo*, 2010, núm. 14, pp. 17-74.

SAMBLAS QUINTANA, E.: "El presupuesto de la Unión Europea y su integración en el presupuesto español", *Crónica presupuestaria*, 2016, núm. 4, pp. 54-68.

UN ANÁLISIS DE LOS PROCESOS DE RESOLUCIÓN DE LITIGIOS SOBRE CONTRATOS ILÍCITOS EN LOS MERCADOS DE LA RED OSCURA*

AN ANALYSIS OF THE DISPUTE RESOLUTION PROCESSES FOR ILLICIT CONTRACTS IN DARK WEB MARKETS

Actualidad Jurídica Iberoamericana Nº 21, agosto 2024, ISSN: 2386-4567, pp. 70-103

* Estudio redactado en el marco del Proyecto "Claves para una justicia digital y algorítmica con perspectiva de género", PID2021-123170OB-I00 financiado por MCIN/ AEI/10.13039/501100011033. El autor agradece los comentarios aportados al borrador inicial por la Dra Ana Montesinos García y el Dr Norberto Redondo Melchor. Naturalmente, cualquier posible error en el texto es responsabilidad exclusiva del autor.

Pablo CORTÉS

ARTÍCULO RECIBIDO: 29 de mayo de 2023
ARTÍCULO APROBADO: 1 de julio de 2024

RESUMEN: Este artículo explora cómo los participantes en los mercados de la Red Oscura acceden a herramientas para evitar disputas y sistemas para resolverlas, diseñados para minimizar y resolver disputas surgidas de transacciones ilícitas. Un número creciente de personas recurre a la Dark Web para realizar actividades principalmente ilegales, que incluyen la compra de drogas, la adquisición de ransomware y armas. Los pagos generalmente se realizan a través de un sistema de depósito en garantía ("escrow") que retiene la criptomoneda pagada por compradores anónimos a vendedores anónimos hasta que los compradores confirman su satisfacción con la transacción. Cuando los compradores no están satisfechos y no pueden resolver su queja directamente con el vendedor, pueden iniciar una disputa en la cual típicamente un adjudicador independiente congela el pago depositado y considera las pruebas proporcionadas por las partes, y a menudo también las opiniones de la comunidad del mercado, y determina el resultado de la disputa. El artículo analiza las herramientas y sistemas diseñados para evitar y resolver disputas, cuyo objetivo es fortalecer la confianza en transacciones ilícitas anónimas en los mercados oscuros. Se argumenta que la implementación de estos mecanismos de resolución de disputas están fomentando el desarrollo orgánico de un ecosistema de justicia civil dentro de la Red Oscura.

PALABRAS CLAVE: Resolución Alternativa de Litigios; red oscura; prevención de litigios; arbitraje; mediación.

ABSTRACT: *This paper seeks to unravel how participants in the marketplaces of the Dark Web have access to dispute avoidance tools and dispute resolution systems designed to minimise and settle disputes arising from illicit transactions. A growing number of individuals go the Dark Web to carry out mostly illegal activities, which range from the purchase of illegal drugs to the purchase of ransomware and weapons. Payments typically take place via an escrow system that holds the cryptocurrency paid by anonymous buyers to anonymous sellers until the buyers confirm their satisfaction with the transaction. When buyers are not satisfied and cannot settle their complaint directly with the seller, they can start a dispute whereby typically an independent adjudicator freezes the payment in the escrow and considers the evidence provided by the parties, and often also the views of the marketplace community, and determines the outcome of the dispute. The paper examines the dispute avoidance and resolution tools that seek to enhance trust in anonymous peer to peer illicit transactions, and it argues that these emerging dispute resolution systems are contributing to the organic growth of a civil justice ecosystem for the Dark Web.*

KEY WORDS: *Alternative dispute resolution; dark web; dispute prevention; arbitration; mediation.*

I. INTRODUCCIÓN.

La Red Oscura, conocida también como la *Dark Web* o la *Dark Net*, es la parte de Internet no indexada por los buscadores tradicionales como Google. Sólo es accesible a través de un software especializado, como TOR, que encripta la información y la ubicación de sus usuarios, lo que la convierte en un refugio seguro para la transacción de bienes y servicios ilegales, como drogas, bienes robados, armas, pasaportes falsificados y ransomware,[1] así como servicios, desde campañas de spam, hasta asesinatos por encargo. La combinación de la creciente actividad de la red TOR y el avance de la tecnología de las criptomonedas que también garantizan el anonimato del usuario, ha desempeñado un papel importante en el auge de un comercio ilícito fuera del alcance de las fuerzas del orden público.

Aunque los mercados en la Dark Web operan en un ámbito no regulado, en muchos aspectos funcionan como mercados en línea tradicionales como eBay o Amazon. Sin embargo, a diferencia de Amazon, los administradores del mercado normalmente no venden directamente a los clientes, sino que simplemente ofrecen un espacio virtual para que compradores y vendedores realicen transacciones; y a diferencia de eBay, no hay subastas, ya que todos los artículos a la venta normalmente tienen un precio fijo. Como el número de estas transacciones, al igual que las del comercio electrónico legal, ha aumentado en los últimos años,[2] también ha surgido la necesidad de usar algún tipo de mecanismo de resolución de litigios. Actualmente, la mayoría de los mercados de la Dark Web ofrecen un sistema de reclamación y de resolución de litigios.[3] Además, los mercados más

1 Los ataques de ransomware consisten en la encriptación de los datos del ordenador y la red de la víctima y exigen cripto pagos a través de la Dark Web para mantener el anonimato de los piratas informáticos. Véase Vanian, J.: 'Online criminals have created their pseudo court system on the dark web' *Fortune* (7 diciembre 2021). Véase https://fortune.com/2021/12/07/online-criminals-court-system-dark-web-russian-hackers-ransomware/. En adelante, última vez accedido el 3 de abril de 2024

2 United Nations Office on Drugs and Crime, Global Overview – Drug Demand Drug Supply, Global Drug Report 2022. p. 58. Véase https://www.unodc.org/res/wdr2022/MS/WDR22_Booklet_2.pdf.

3 Holland, A. et al.,: 'The Evolution of Cybercrime: Why the Dark Web is Supercharging the Threat Landscape and How to Fight Back' An HP Wolf Security Report' 2022, pp. 4 y 15. Véase https://threatresearch.ext.hp.com/wp-content/uploads/2022/07/HP-Wolf-Security-Evolution-of-Cybercrime-Report.pdf

• Pablo Cortés
Catedrático Leicester School of Law, University of Leicester (Reino Unido), pablo.cortes@le.ac.uk

grandes del Dark Net tienen miles de usuarios a los que ofrecen un servicio de atención al cliente 24 horas al día, 7 días a la semana.

El pago de las actividades comerciales en la Dark Web se realiza mediante criptomonedas a las que su posible anonimato del usuario permite referirse a ellas como el efectivo digital. Estos cripto-pagos también facilitan la auto-ejecución de las decisiones porque normalmente se entregan a través de un depósito en garantía (llamado servicio de custodia o *escrow*) que retiene el monto de la transacción hasta que el comprador confirma que está satisfecho con la transacción (o hasta que ha pasado el período de tiempo establecido).[4] Si una de las partes no está satisfecha con la transacción, puede iniciar una reclamación que a menudo se resuelve con la asistencia del administrador del mercado que controla el depósito de la transacción.

Por lo tanto, cada vez hay más procesos de resolución de litigios en línea que se emplean habitualmente para resolver disputas entre compradores y vendedores de acuerdo con las normas específicas de cada mercado de la Dark Web y con las condiciones generales de venta acordadas por las partes. Estos procesos frecuentemente aseguran la ejecución de la decisión, no solo a través del sistema de depósito del servicio de custodia (*escrow*), sino también a través del uso de incentivos (ej., la reputación del vendedor se verá afectada por un comentario negativo del comprador) y sanciones (ej., la expulsión de usuarios del mercado), pues es crucial garantizar el cumplimiento extrajudicial de la decisión, ya que naturalmente las partes no pueden acudir a los tribunales nacionales para hacer cumplir el resultado de litigios relacionados con transacciones ilegales. El objetivo de estas herramientas de prevención y resolución de litigios no es otro que aumentar la confianza entre los usuarios que participan en el comercio ilícito, reduciendo al mismo tiempo el riesgo de represalias por parte de las víctimas de transacciones fraudulentas o controvertidas.

A pesar de la existencia de estos sistemas de resolución de disputas, hay una escasez de información disponible sobre estos procesos porque los mercados en la Dark Web no han sido ampliamente estudiados dada la dificultad para acceder a ellos, el anonimato de los usuarios, y los riesgos que implica navegar por la Dark Net.[5] Aunque la bibliografía especializada ha reconocido la existencia de estos servicios de resolución de litigios, actualmente no hay ninguna publicación

4 Ortolani, P.: 'Self-enforcing online dispute resolution: lessons from Bitcoin' Oxf. J. Legal Stud., 2016, vol 36, pp. 595–629.

5 En el momento de escribir estas líneas, sólo conocemos dos trabajos científicos de criminólogos en los que examinan respectivamente los datos de los sistemas de resolución de disputas de dos foros de la Dark Web: el BHF.IO y el Dark0de, de Choi, K-S and Lee, CS,: 'In the Name of Dark Web Justice: A Crime Script Analysis of Hacking Services y the Underground Justice System' *Journal of Contemporary Criminal Justice* 2023, vol. 39, num. 2, p. 201, y Dupont, B., y Lusthaus, J.: 'Countering Distrust in Illicit Online Networks: The Dispute Resolution Strategies of Cybercriminals' *Social Science Computer Review,* 2021, vol. 40 num 4, p. 892.

jurídica que examine los matices de los diferentes procesos de resolución de disputas empleados en la Dark Web, y mucho menos una discusión sobre cómo están surgiendo en forma de un ecosistema de derecho privado en la Dark Web. El presente estudio pretende contribuir a colmar la laguna existente en la investigación y así ampliar la limitada información existente sobre estos sistemas de justicia clandestinos que operan en la Dark Net. Con ello, este es el primer estudio jurídico que analiza el funcionamiento de estos mercados a un nivel macro, centrándose en los diversos procesos de resolución de conflictos empleados en la Dark Web, y argumenta que su crecimiento orgánico está contribuyendo a la aparición de un ecosistema de derecho privado en la Dark Web.

A tal fin, este estudio ofrece un análisis del alcance de las características y el funcionamiento de estos procesos de resolución de litigios basado principalmente en los escasos datos publicados, en el análisis cualitativo de los procesos de resolución de litigios que ofrecen los mercados de la Dark Web, y en los mensajes disponibles en estos mercados y foros donde los usuarios pueden presentar reclamaciones.[6] Al arrojar luz sobre la resolución de litigios en la Dark Web, este estudio pretende mejorar nuestro conocimiento sobre este campo y disipar las ideas erróneas sobre el gobierno anárquico en la Dark Web. Por consiguiente, en primer lugar, se analiza cómo los internautas acceden a la Dark Web. En segundo lugar, se examinan las principales herramientas de prevención de litigios integradas en los mercados de la Dark Web; a saber, los sistemas de reputación, la selección de los vendedores y la emisión de advertencias, especialmente de vendedores fraudulentos y sitios web espejo (*mirror sites*). En tercer lugar, el presente estudio analiza los principales procesos de resolución de litigios empleados en la Dark Web, que se dividen a grandes rasgos en procesos de negociación directa, mediación y adjudicación por parte del *escrow* y de los administradores del mercado. Por último, este estudio sostiene que estos sistemas emergentes de resolución de disputas tratan de aumentar la confianza en estos mercados y la proliferación de las transacciones ilícitas entre los usuarios, y por lo tanto están contribuyendo a la creación de un ecosistema de derecho privado para los ciberdelincuentes.

II. EL ACCESO A LA WEB OSCURA.

1. Los Diferentes Niveles de Internet.

Muchos pueden considerar que Internet y la World Wide Web (es decir, la web) son sinónimos, pero no lo son, ya que la web es sólo una sección de

6 El estudio y acceso a estos mercados en la Dark Web ha sido sometido al proceso de aprobación ética de la Universidad de Leicester.

Internet a través de la cual se puede acceder a la información.[7] Internet también puede utilizarse para otras actividades, como el envío de correos electrónicos, la transferencia de archivos o las videoconferencias.

Para explicar qué es la Dark Web, y en qué se diferencia de la Red Clara o la Clear Web, hay que distinguir los tres niveles de la Red: la Red Superficial (*Surface Web*), la Red Profunda (*Deep Web*) y la Red Oscura (*Dark Web*). La Red Superficial, también conocida como Red Pública (*Public Web*) o Red Clara (*Clear Web*), es la parte de la Red a la que se puede acceder a través de navegadores normales y motores de búsqueda.[8] Esto se debe a que los sitios web accesibles a través de estos navegadores están indexados, como muchas páginas web populares, mercados en línea, y plataformas de vídeos. Sin embargo, se calcula que sólo alrededor del 4% de Internet es accesible a través de la Red Superficial.[9]

A continuación, está la Red Profunda, también llamada la Red Invisible u Oculta (*Invisible* o *Hidden Web*), que representa la mayor parte de Internet. La Deep Web incluye los sitios que requieren que las partes se registren, y cuando el contenido que no ha sido indexado por los buscadores tales como Google, como la mayor parte de la información contenida en sitios de redes sociales, bancos, proveedores de correo electrónico y bases de datos legales como Lexis Nexis y Westlaw. Dentro de la Deep Web también hay redes privadas, conocidas como Intranets, que se construyen para las organizaciones de los usuarios, como universidades, administraciones públicas y grandes empresas.

Por último, la Dark Web, también conocida como Red Oscura, es una sección de la Deep Web que garantiza el anonimato de las partes y a la que sólo se puede acceder mediante un software especial porque su contenido se ha ocultado intencionadamente. En consecuencia, una red privada y segura que utiliza un protocolo criptográfico, a la que sólo puede acceder un grupo selecto de personas y no los navegadores de Internet normales, también sería un ejemplo de Dark Web. Sin embargo, la Dark Web es mucho más lenta que la Surface Web porque utiliza los canales traseros de Internet, y por la misma razón los sitios de la Dark Net no son tan ricos en imágenes como los mercados de la Surface Web. Al igual que en la Deep Web, el contenido de los sitios de la Dark Web no está indexado. No está claro, sin embargo, qué parte de la Deep Web está ocupada por contenidos de la Dark Web, y qué parte de la Dark Web se utiliza para actividades legales o ilegales.

7 Finklea, K.: 'Dark Web', Congressional Research Service, 7-5700, R44101 (10 marzo 2017) p. 2. Véase https://a51.nl/sites/default/files/pdf/R44101%20(1).pdf. Chertoff, M. y Simon, T.: 'The Impact of the Dark Web on Internet Governance and Cyber Security, Global Commission on Internet Governance', Paper Series: No. 6 febrero 2015.

8 DeNicola, L.: 'What is the Dark Web?' *Experian - Cybersecurity* (12 mayo 2021). Véase https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/.

9 Ibid.

La Dark Web fue creada originalmente por el Laboratorio de Investigación Naval de Estados Unidos para proporcionar un mecanismo de comunicaciones privadas en línea al personal militar y a los espías.[10] El gobierno estadounidense decidió publicar el código para que a los espías les resultara más fácil ocultarse y permitir que otras personas, especialmente aquellas cuyos gobiernos restringen el uso de Internet, pudieran comunicarse de forma anónima. Por lo tanto la Red Oscura es un baluarte para la libertad de expresión en países como China, Siria, Afganistán y Korea del Norte. Así se creó la red TOR como navegador de código abierto y el Gobierno Federal de EE.UU. sigue siendo su principal financiador.[11] Por lo tanto, paradójicamente, el Gobierno de EE.UU. creó y financia la TOR, el cual permite acceder a la Dark Web donde la actividad ilícita prolifera entre usuarios anónimos que corren muy poco riesgo de ser detectados por las fuerzas de seguridad.

2. Entrar en la Dark Web.

La mayoría de los usuarios de la Dark Web acceden a ella a través de la red TOR.[12] TOR son las siglas de "The Onion Router", que hace referencia a las capas de encriptación que resemblan a una cebolla con el fin de proporcionar anonimato y privacidad a sus usuarios.[13] Para entrar en la Dark Web los usuarios necesitan primero instalar el navegador TOR, de acceso libre y uso legal. Las direcciones de los sitios de la Dark Net accesibles a través de la red TOR terminan en ".onion". En la red TOR, cada nodo sustituye la dirección IP del usuario por la suya propia y elimina secuencialmente una capa de cifrado. Por último, el servidor final, conocido como nodo de salida, descifra completamente su solicitud y la transmite al sitio deseado. Por consiguiente, las partes externas no pueden averiguar la dirección IP original ni establecer una conexión rastreable con sus actividades en línea. Esto se debe a que los sitios .onion no están en ningún registro central similar a como ICANN mantiene los nombres de dominio de la Web Clara. A pesar de ello, se han conocido casos en los que TOR ha revelado la dirección IP real del usuario a hackers especializados y servicios secretos como la Agencia de Seguridad Nacional (NSA) y el servicio secreto inglés (GCHQ).[14] Por eso, la mayoría de los usuarios de la Dark Net también emplean el cifrado de una Red Privada Virtual (VPN) para

10 Davies, G.: 'Shining a light on policing of the Dark Web: an analysis of UK investigatory powers' *Journal of Criminal Law,* 2020, vol. 84 num 5, 408.

11 Jardine, E.: 'The Dark Web Dilemma: Tor, Anonymity and Online Policing' *Global Commission on Internet Governance Paper Series,* 2015, vol. 21, p. 6. Véase https://ssrn.com/abstract=2667711.

12 The Onion Router Project. Véase https://www.torproject.org/projects/torbrowser.html.en.

13 Finklea: 'Dark Web', cit. p. 2. Chertoff, M. y Simon, T.: 'The Impact of the Dark Web on Internet Governance and Cyber Security, Global Commission on Internet Governance', cit.

14 Electronic Frontier Foundation, 'GCHQ Leak: A Potential Technique to Deanonymise Users of the TOR Network' UK Top Secret Strap1 Comint, OPC-M/TECH.B/61 (13 June 2011). Véase https://www.eff.org/document/20141228-speigel-potential-technique-deanonymise-users-tor-network. Aminuddi, M., Zaaba, Z., Samsudin, A., Zaki, F. y Anuar, N.: 'The rise of website fingerprinting on Tor' *Journal of Network and Computer Applications,* 2023, p. 212.

ocultar la ubicación de su dirección IP y mantener la privacidad de sus actividades de navegación.

Aunque en la Dark Net hay foros y mercados que contienen actividades ilegales, también hay sitios legales, incluso de organismos públicos, como la CIA, que en 2019 lanzó su propio sitio para permitir comunicaciones seguras y anónimas con los usuarios de la Dark Web.[15] Del mismo modo, otros grandes medios de noticias, como el New York Times y el Washington Post, también tienen presencia en la Dark Web para permitir comunicaciones anónimas con informantes.[16] Incluso Facebook tiene ahora su propio sitio .onion, que en 2016 declaró tener más de un millón de usuarios.[17] Por lo tanto, la Dark Web no solo se utiliza para el comercio ilícito, sino que también la utilizan periodistas, informantes, disidentes y, en general, usuarios de Internet que no quieren ser rastreados. De hecho, Edward Snowden utilizó TOR para denunciar la vigilancia generalizada llevada a cabo por el Gobierno de Estados Unidos mediante la publicación de miles de documentos clasificados por la NSA.[18] La amplia repercusión y difusión de estas revelaciones tuvo un efecto dominó en el aumento de usuarios en la Dark Web.[19]

El presente artículo se centra en los mercados ilícitos donde los usuarios aprovechan su anonimato para comprar y vender una inquietante gama de bienes y servicios, como drogas, armas, falsificaciones, datos privados, pornografía infantil, *ransomware*, el alquiler de sicarios o la contratación de campañas de spam. Sin embargo, muchos mercados establecen restricciones sobre lo que se puede vender, y a menudo prohíben la venta de ciertos artículos que tienen más probabilidades de llamar la atención de las fuerzas de seguridad, como pornografía infantil, armas, fentanilo y asesinatos por encargo.[20]

Los mercados de la Dark Web también se conocen como criptomercados porque utilizan criptomonedas como Bitcoin y Monero que, especialmente la última, ofrecen un grado de anonimato en las transacciones. El anonimato se logra porque las transacciones se asocian con direcciones de billetera públicas, no con identidades personales directamente. Sin embargo, el anonimato no es completo. Las transacciones son públicas y permanentes en la cadena de bloques de Bitcoin, permitiendo que, con análisis suficiente y bajo ciertas circunstancias, se puedan

15 The Tor site of the CIA is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.

16 Véase https://www.nytimesn7cgmftshazwhfgzm37qxb44r64ytbb2dj3x62d2lljsciiyd.onion/ y washingtonpost.securedrop.tor.onion. Todos los enlaces acabados en .onion son accesibles exclusivamente desde la Dark Web a través de TOR.

17 Véase facebookwkhpilnemxj7asaniu7vnjjbiltxjqhye3mhbshg7kx5tfyd.onion. Véase Hoffman, W.: 'Facebook's Dark Web .Onion Site Reaches 1 Million Monthly Tor Users' (22 abril 2016). Véase https://www.inverse.com/article/14672-facebook-s-dark-web-onion-site-reaches-1-million-monthly-tor-users.

18 Croy, A.: *The Dark Web: The Covert World of Cybercrime*, Greenhaven Publishing LLC, 2018, p. 30.

19 Doyle, E.: *The Dark Web*, Greenhaven Publishing LLC, 2019, p. 56.

20 Véase for example Nemesis, the Royal Market y ASAP Market.

rastrear a sus participantes. Por ejemplo, vinculando una dirección de billetera a una identidad real a través de transacciones en intercambios de criptomonedas que requieren verificación de identidad, se puede potencialmente descubrir quién ha hecho un pago.

Aprovechando los nodos TOR para ocultar sus direcciones IP, los usuarios pueden acceder a sitios no listados de forma anónima y pagar las transacciones también de forma anónima. Este anonimato fomenta la utilización de la Dark Web con fines ilícitos, ya que obstruye el rastreo de los usuarios por parte de las fuerzas de seguridad, garantizando la privacidad de los usuarios en estas redes públicas.[21] Sin embargo, la privacidad por sí sola no bastaría para atraer a una masa crítica de usuarios. Por ello, estas plataformas no sólo permiten a los usuarios ofrecer bienes y servicios y realizar transacciones, sino que también les proporcionan herramientas para evitar conflictos y sistemas de resolución de litigios.

III. HERRAMIENTAS PARA EVITAR DISPUTAS EN LA DARK WEB.

Los mercados en la Dark Net necesitan ofrecer garantías a los usuarios potenciales para que éstos puedan confiar en ellos y realizar transacciones. Estas garantías se proporcionan incorporando en su diseño herramientas que reducen el riesgo de que surjan disputas en primer lugar. En consecuencia, los mercados de la Dark Web incorporan características de seguridad, advierten a los usuarios sobre la suplantación de identidad (*phishing*), los sitios espejo (*mirror sites*), vetan a sus vendedores, y proporcionan a los usuarios información sobre las transacciones anteriores de los vendedores, como el número de transacciones completadas y las opiniones de otros compradores anteriores.

1. Elementos de seguridad.

Las características de seguridad de los mercados buscan garantizar el anonimato de los usuarios y evitar interferencias de *hackers* y robots (*bots*). Además del uso del navegador TOR y la VPN, para acceder a la mayoría de los mercados se requiere que los usuarios se registren primero eligiendo un nombre de usuario y una contraseña. El inicio de sesión normalmente tiene un CAPTCHA (*Completely Automated Public Turing test to tell Computers and Humans Apart*), en el que se puede pedir al usuario que identifique los cuadrados que no pertenecen a una fotografía o que vuelva a escribir las letras o números que aparecen en una imagen.

Para completar una transacción en la que se van a entregar bienes en una dirección física, se pide al comprador que encripte su nombre y dirección utilizando la clave pública PGP del vendedor. Aunque algunos usuarios pueden utilizar una

21 Davies, 'Shining a light on policing of the Dark Web: an analysis of UK investigatory powers', cit., p. 408.

identidad falsa, la mayoría utilizan sus datos personales reales para evitar sospechas por parte del servicio de correos o del cartero.[22] Además, algunos mercados, como ASAP Market, recomiendan a los usuarios que empleen la autenticación de dos factores (2FA).

Lo más importante es que el pago de la transacción se realiza de forma anónima utilizando criptomoneda que se deposita en el *escrow*. De hecho, la mera existencia del *escrow* produce un nivel de confianza entre las partes implicadas, ya que ni el comprador ni el vendedor tienen control sobre los fondos hasta que se cumplan las condiciones contractuales, lo que reduce el riesgo de fraude.

Para reducir el riesgo de que las fuerzas de seguridad relacionen los bitcoins con la identidad de los usuarios, lo que de por sí requiere una investigación, los usuarios, y especialmente los grandes vendedores, pueden emplear un *tumbler* de criptodivisas (también conocido como servicio de mezcla), que desidentifica el origen de la criptodivisa mezclándola con otras antes de devolverla en diferentes lotes. Dado que estos servicios permiten el blanqueo de dinero, varios proveedores han sido el objetivo de las fuerzas de seguridad.[23]

2. Expulsión, veto y advertencias.

Los administradores de los mercados en la Dark Net tienen como prioridad la expulsión de los vendedores poco fiables y garantizar el anonimato de sus usuarios. Para ello, los pagos deben realizarse siempre mediante criptomoneda. Más aun, solicitar otro tipo de pago, como una transferencia de Western Union o una transferencia bancaria, conllevará una prohibición permanente en dicho mercado.[24] En una línea similar, los vendedores que tengan un alto índice de disputas serán vetados. Por ejemplo, ASAP Market prohíbe la entrada a los vendedores con más de un 30% de disputas entre sus ventas.[25]

El anonimato puede plantear riesgos a los usuarios, y no sólo frente a vendedores fraudulentos, sino también frente a las fuerzas de seguridad, ya que los usuarios no pueden estar seguros de que la persona que ofrece un producto o servicio no sea un agente encubierto o un informante de la policía.[26] Para reducir estos riesgos, se exige a los vendedores habituales que paguen una cuota de entrada

22 Afilipoaie, A., y Shortis, P.: 'From Dealer to Doorstep – How Drugs are Sold on the Dark Net' *Global Drug Policy Observatory, Situation Analysis*, 2015, p. 4.

23 US Department of Justice - Office of Public Affairs, 'Individual Arrested and Charged with Operating Notorious Darknet Cryptocurrency "Mixer"' (28 abril 2021). Véase https://www.justice.gov/opa/pr/individual-arrested-and-charged-operating-notorious-darknet-cryptocurrency-mixer.

24 Véase ASAP Market Rules. Disponible en el siguiente enlace de la Dark Web http://asap4u7rq4tyakf5gdahmj2c77blwc4noxnsppp5lzlhk7x34x2e22yd.onion.

25 Ibid.

26 Campana, P., y Varese, F.: 'Cooperation in criminal organizations: Kinship and violence as credible commitments' *Rationality and Society,* 2013, vol. 25, num 3, p. 265.

antes de permitirles operar como vendedores en el mercado. La cuota no suele ser reembolsable y pretende disuadir a los vendedores fraudulentos, que serán expulsados del mercado si no respetan las normas estafando a los compradores, o si no acatan una decisión tomada en el proceso de resolución de conflictos. El valor de la tasa varía en función del mercado, pero cuanto mayor sea éste, mayor será la tasa. Por ejemplo, Nemesis exige a los vendedores una cuota de entrada de 500 USD, mientras que Royal Market cobra 1.000 USD. Otros mercados sólo admiten a vendedores con experiencia y reputación que hayan participado en otros mercados. Por ejemplo, para ser admitido en CannaHome Market un vendedor necesita tener al menos 500 ventas en otros mercados y valoraciones de 4 estrellas o menos de un 1% de opiniones negativas de clientes anteriores. Por lo tanto, las fianzas de los vendedores contribuyen a que los mercados obtengan beneficios, al tiempo que disuaden a posibles estafadores de aprovecharse de usuarios inexpertos.[27]

Las estafas y los enlaces falsos a mercados que pretenden estafar a los compradores mediante el uso de espejos (*mirror sites*) son un riesgo habitual para los usuarios de la Dark Web. Un espejo es esencialmente una copia de un sitio (*website*) que permite a los usuarios acceder a la misma información que en el sitio original, y donde cualquier cambio en el sitio espejo se producirá automáticamente en el sitio original. Sin embargo, también existen espejos maliciosos utilizados por individuos que suplantan su identidad (*phishers*) que parecen el sitio original, pero a cuyos usuarios se les copian los datos de acceso y se les cambia la dirección de pago por la del estafador. Habitualmente, el usuario no se da cuenta de la estafa hasta que presenta una reclamación en el mercado y se da cuenta de que el vendedor o el mercado no han recibido el pago. Para advertir de estos riesgos, los administradores de los mercados de la Dark Web suelen publicar mensajes en forma de banners o anuncios en el foro del mercado advirtiendo sobre los estafadores y los enlaces falsos al mercado.

3. Sistemas de reputación.

Al igual que la reputación de los vendedores y los comentarios de los compradores son cruciales en el comercio electrónico de la Surface Web, en la Dark Web los usuarios utilizan seudónimos para comunicarse y pueden dejar comentarios después de cada transacción con una calificación numérica, así como un comentario explicando su calificación.[28] Esta información se aporta cuando termina la transacción, es decir, cuando el comprador ha recibido la mercancía y el vendedor ha recibido los fondos del proveedor de custodia (*escrow*). Una

27 Afilipoaie y Shortis: 'From Dealer to Doorstep – How Drugs are Sold on the Dark Net', cit., p. 3.

28 Cybersixgill, 'Trust on the Deep and Dark Web' (22 marzo 2022). Véase https://cybersixgill.com/news/articles/trust-on-the-deep-and-dark-web.

vez finalizado el pedido, las partes no pueden impugnar la transacción. Algunos sistemas de evaluación tienen en cuenta otros factores además de las opiniones de los compradores y permiten a los vendedores evaluar a los compradores, con lo que se pretende identificar a los compradores que hacen reclamaciones falsas con el fin de obtener un reembolso del pago.[29] No obstante, las opiniones positivas de los compradores son especialmente importantes para que los vendedores atraigan el regreso de clientes, así como de nuevos compradores.

Prestar atención a la reputación de los vendedores es vital para reducir el riesgo de litigios e identificar a los vendedores reputados, mitigando así los riesgos de fraude.[30] Los sistemas de reputación desempeñan un papel fundamental a la hora de fomentar la comunicación eficaz, la cooperación y la confianza en las transacciones, disminuyendo así la probabilidad de malentendidos y conflictos.[31] Cuando surge una disputa, las partes con buena reputación son más propensas a entablar discusiones constructivas y a trabajar para encontrar soluciones amistosas. Además, las revisiones ayudan a incentivar a los vendedores para que se adhieran a las decisiones tomadas en el proceso de resolución de disputas. De hecho, los vendedores suelen esforzarse por proteger su reputación en estos mercados, ya que perder la confianza o ser expulsados reducen su capacidad para seguir comerciando.

En el ámbito de la ciberdelincuencia, los administradores y moderadores de los mercados de la Dark Web asumen una función policial al impedir activamente que los estafadores (a menudo denominados *rippers*) participen en las actividades del mercado ilícito. Esto sirve tanto para disuadir a los defraudadores potenciales como para aumentar la confianza y la fiabilidad del mercado. En consecuencia, la forma de acción disciplinaria más frecuente en estos mercados es el ostracismo mediante la aplicación de medidas de suspensión y expulsión.[32]

Según un estudio empírico de tres mercados de la Dark Web (Wallstreet Market, Hansa Market y AlphaBay), las valoraciones positivas constituían más del 90% de todas las valoraciones de cada uno de los tres mercados.[33] También se descubrió que el mayor porcentaje de valoraciones neutras y positivas se daba en el más pequeño de los tres mercados, lo que puede deberse a que resultaba

29 Afilipoaie y Shortis: 'From Dealer to Doorstep – How Drugs are Sold on the Dark Net', cit., p. 5.

30 Kapersky, 'Business on the dark web: Deals and regulatory mechanisms', 2023 p. 14. Véase https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2023/03/10151223/Business-on-the-dark-web-deals-and-regulations.pdf?reseller=gl_regular-sm_acq_ona_oth__onl_b2b_securelist_lnk_sm-team.

31 Holt, T.: 'Exploring the social organisation and structure of stolen data markets' *Global Crime* vol. 2013, num. 14(2-3), pp. 155–174 y Yip, M. , Webber, C., Shadbolt, N.: 'Trust among cybercriminals? Carding forums, uncertainty and implications for policing' *Policing and Society*, 2013, vol. 23, num. 4, pp. 516–539.

32 Holt, T. y Lampke, E., 'Exploring stolen data markets online: Products and market forces' *Criminal Justice Studies*, 2010, vol. 23, num. 1, pp. 33–50.

33 Lummen, DLM: 'Is Telegram the new Dark Net? A comparison of traditional and emerging digital criminal marketplaces' (MSc thesis, University of Twente 2023), p. 49.

menos atractivo para los estafadores que los mercados más grandes.[34] Por tanto, los vendedores de la Dark Web dependen de la reputación para hacer negocios, y una mala reputación puede ser devastadora con respecto a las futuras transacciones y su posición competitiva con otros vendedores. Además, cuando surgen disputas, los árbitros tienen en cuenta las reseñas del vendedor y el historial del comprador, por lo que aquellos con mayores reseñas positivas e historial de transacciones tienen más probabilidades de que el proceso de solución de disputas se incline a su favor. Algunos mercados oscuros, como Archetyp, también informan a los compradores y a los árbitros el número de disputas o reclamaciones abiertas que tiene el vendedor. Este sesgo inherente en el proceso de resolución de disputas podría llevar a los vendedores experimentados a ser selectivos y aprovecharse exclusivamente de los compradores sin experiencia.

IV. PROCESOS DE RESOLUCIÓN DE DISPUTAS EN LA DARK WEB.

Cuando un comprador realiza un pedido, lo hace a través de un mensaje privado enviado al vendedor donde indica los artículos que desea comprar y la dirección para la entrega, mientras que el vendedor proporciona el enlace para realizar el cripto-pago en su monedero electrónico, o en el del servicio de custodia (*escrow*). Dado que la dirección del comprador (ya sea digital o física) es un dato personal sensible que los compradores no quieren que esté disponible en la Dark Web, se les recomienda que la cifren utilizando la clave PGP pública de los vendedores, para que éstos puedan descifrar la dirección del comprador utilizando su clave privada. Ello evita que terceros interceptores puedan leer el mensaje. Sin embargo, los compradores inexpertos que no sepan utilizar PGP pueden realizar pequeños pedidos con éxito sin cifrar los datos personales, pero la mayoría de los vendedores insisten en proporcionar el cifrado y pueden ignorar la información que no haya sido cifrada.[35] Una vez recibido el pago en la dirección del monedero electrónico facilitada por el vendedor, éste enviará los artículos comprados y borrará el texto cifrado.

Si las partes tienen problemas con su transacción, pueden discutir una solución utilizando la sala de mensajes privados abierta para la transacción. El vendedor puede presentar una reclamación si no ha recibido el pago. Sin embargo, esto no es muy habitual, ya que los vendedores normalmente cancelan una transacción que no ha sido pagada en un plazo determinado, que puede ser de unas horas o hasta unos días desde que el comprador realizó el pedido. Los compradores, no obstante, son los reclamantes paradigmáticos cuando no han recibido la mercancía en el plazo previsto, o cuando los artículos adquiridos funcionan mal, como los

34 Ibid.

35 Afilipoaie y Shortis: 'From Dealer to Doorstep – How Drugs are Sold on the Dark Net' cit., p. 2.

litigios relativos a programas maliciosos, como los de ransomware, ineficaces, o cuando la calidad de los bienes no se ajusta a su descripción, como los litigios relativos a la baja calidad de las drogas o medicamentos. Aunque el valor de la mayoría de los litigios oscila entre unos cientos y unos miles de dólares, se han registrado casos de mayor cuantía, como uno de dos millones de dólares por servicios de piratería informática.[36] De hecho, hay pruebas de que algunos consumidores compran drogas a granel en la Dark Web para venderlas después en cantidades más pequeñas,[37] por lo que estos mercados pueden funcionar tanto como mayoristas como minoristas, permitiendo transacciones de alto y bajo valor.

Cuando no existen mecanismos para resolver disputas en la Dark Web, hay un mayor riesgo de que las disputas deriven en violencia u otras actividades ilegales, como el chantaje o la extorsión, que pueden ser utilizadas por los vendedores para resolver las disputas a su favor. Así pues, los compradores estarán especialmente expuestos a estos riesgos cuando hayan facilitado a los vendedores su domicilio para la entrega de los artículos adquiridos.

Cuando surge un litigio, las partes intentan negociar una solución. Si no se puede llegar a un acuerdo, los usuarios recurrirán al servicio de custodia o al administrador del mercado, que investigará la reclamación y tomará una decisión definitiva sobre el resultado de la disputa. Cuanto mayor sea el mercado, más probable es que tenga un equipo de atención al cliente dedicado a resolver disputas. Este es el caso de Tor2door, que ofrece un servicio de resolución de disputas 24 horas al día. Ambas partes aceptan el proceso cuando realizan una transacción en el mercado, y como ambas partes quieren mantener el pago de la transacción, están incentivadas a participar en el proceso de resolución de disputas. Los principales procesos de resolución de disputas en la Dark Web son la negociación, que a veces se apoya en un proceso que trata de identificar las cuestiones en disputa, y la mediación y adjudicación proporcionadas por el servicio de custodia o el moderador del mercado. Estos procesos se examinan a continuación.

1. Negociación entre las partes.

Los mercados de la Dark Web recomiendan que los reclamantes se comuniquen primero directamente con la otra parte para aclarar cualquier malentendido y explorar una resolución rápida. Un estudio empírico a pequeña escala de 201 casos en el foro en ruso BHF.IO descubrió que los acuerdos tardaban una media

36 Vijayan, J.: 'The Dark Web has its own people's court' (7 diciembre 2021) Dark Reading. Véase https://www.darkreading.com/threat-intelligence/the-dark-web-has-its-own-people-s-courts.

37 Afilipoaie y Shortis: 'From Dealer to Doorstep – How Drugs are Sold on the Dark Net' cit., p. 4.

de 3,05 días desde la presentación de la disputa, mientras que las adjudicaciones tardaban 6,77 días. [38]

Las comunicaciones directas se producen normalmente a través del sistema de mensajería privada disponible en el mercado y busca lograr una resolución confidencial y rápida. La sala privada puede ser la misma que se abrió para completar la transacción, o puede ser una nueva sala de chat abierta por el reclamante. Además de los mensajes privados, algunos mercados que han cerrado, como AlphaBay, ofrecían a las partes un servicio automatizado de resolución de disputas llamado *Automatic Dispute Resolver.*[39] Básicamente, se trata de un sistema de resolución en el que el comprador y el vendedor pueden ampliar el tiempo de custodia, acordar reembolsos totales o parciales u opciones de sustitución. Este proceso de negociación imita los pasos que, de otro modo, habría dado un administrador del mercado durante un proceso de resolución de disputas. En los casos en que las partes no puedan llegar a un acuerdo, permite a las partes indicar sus opciones de resolución preferidas, lo que facilita el papel del administrador del mercado en la resolución de litigios. Cada parte puede aceptar o negar las resoluciones propuestas por la otra parte.

AlphaBay también ha creado un sistema llamado *Streamlined Dispute Process* para gestionar las reclamaciones a través de conversaciones por mensaje privado, que se eliminan de los pedidos una vez resueltas.[40] A través de este sistema las reclamaciones van a una sección diferente de la web. Si las partes no alcanzan un acuerdo, la disputa pasa al modo manual donde los administradores pueden ver las interacciones no cifradas, así como las propuestas de acuerdo, y resolver la disputa pendiente.

Cuando las partes no pueden llegar a un acuerdo, el reclamante suele tener la opción de hacer clic en "Disputa" en la página del pedido para remitir la reclamación al foro de resolución de disputas previsto por el mercado.[41] Algunos mercados tienen un foro público en el que se publican las disputas y se invita a la comunidad a compartir sus opiniones sobre la disputa. Las opiniones de los usuarios pueden persuadir a las partes para llegar a un acuerdo amistoso, que puede implicar que el demandado ceda en parte o en la totalidad de la reclamación. Además, los usuarios del mercado, especialmente los más novicios, pueden utilizar el foro de los mercados para pedir consejo sobre la conveniencia de iniciar disputas contra

38 Choi y Lee: 'In the Name of Dark Web Justice: A Crime Script Analysis of Hacking Services y the Underground Justice System', cit., p. 208.

39 Onion Index, 'AlphaBay' (*GitHub,* 1 diciembre 2022) https://github.com/OnionIndex/AlphaBay; y 'AlphaBay Market | Home' (*AlphaBay*) https://alphabay-url.com/ .

40 Ibid.

41 DoingFedTime, 'Dispute Resolution Buyers vs Vendors – Deep Dot Dark Net' (27 noviembre 2022). https://www.youtube.com/watch?v=qwZvflkl-9c&t=12s.

otros vendedores. Así, al facilitar las interacciones entre los usuarios del mercado, permitiéndoles expresar sus opiniones sobre el fundamento de la reclamación, el foro público anima a las partes a llegar a un acuerdo mediante esta técnica colaborativa de resolución de problemas.

La promoción de la negociación como fase inicial del servicio de resolución de litigios reconoce que muchos conflictos pueden resolverse sin la intervención de terceros. Además, la privacidad de estas negociaciones evita la escalada innecesaria de las reclamaciones y reduce el riesgo de hacer acusaciones infundadas que difamen injustificadamente a la otra parte en el foro del mercado.

2. El sistema de custodia (*escrow*): mediación y adjudicación.

Los servicios de custodia (*escrow*) son el ingrediente clave de la Dark Net para superar el riesgo de transacciones fraudulentas. El servicio de custodia lo proporciona el mercado, y suele ser la principal fuente de ingresos del mercado, ya que cobra una comisión por transacción, que puede llegar al 10% del valor de la venta, aunque lo más habitual son comisiones más bajas, entre el 5% y el 2%.[42]

Según un estudio, el 85% de los mercados de la Dark Web utilizan agentes de custodia para cada transacción,[43] que retienen los pagos del comprador y los liberan al vendedor cuando éste confirma que el producto se ha entregado, o el servicio se ha prestado adecuadamente. Los fondos también pueden ser liberados sin la confirmación del comprador después de un período previamente acordado o después del tiempo establecido por el mercado (usualmente referido como orden 'Auto Finalizada'). Por ejemplo, Tor2door Market establece catorce días para los productos físicos y dos días para los productos digitales. Las partes pueden ampliar el plazo de custodia. En el caso de Tor2door, los compradores pueden solicitar dos veces una prórroga de cinco días a partir del noveno día desde que el vendedor marca el pedido como enviado. Es importante destacar que la disputa sólo puede plantearse antes de que se finalice el pedido (y se realice automáticamente el pago al vendedor).

Los vendedores más reputados del mercado pueden vender sus productos y servicios sin depósito de garantía, operando como vendedores cuyos pagos se realizan directamente en sus monederos electrónicos. A estos vendedores se identifican como transacciones que "finalizan pronto" (*Finalize Early* o *FE*), Los requisitos para entrar en esta categoría son bastante exigentes. Por ejemplo, ASAP Market exige a los vendedores más de 10.000 ventas y más de un 99%

42 White, G., y Archampong, P.: The Dark Web, Episode 7, Cybercrime Inc, Podcast, (8 febrero 2018).

43 HP Wolf Security et al, 'The Evolution of Cybercrime: Why the Dark Web is Supercharging the Threat Landscape y How to Fight Back – An HP Wolf Security Report' (julio 2022). https://threatresearch.ext.hp.com/wp-content/uploads/2022/07/HP-Wolf-Security-Evolution-of-Cybercrime-Report.pdf p. 15.

de opiniones positivas. Aunque estos vendedores no pueden ofrecer las mismas garantías que un tercero, dada su posición establecida en el mercado, es más probable que sigan las instrucciones del administrador del mercado.

Cuando un comprador no está satisfecho con la transacción, se presenta una reclamación ante el agente de custodia (normalmente el administrador del mercado, pero también puede ser un tercero), que congelará el importe de la custodia, examinará las pruebas y determinará quién se quedará con los fondos de la transacción. Sin embargo, antes de que el agente de custodia resuelva el litigio, suele haber un debate moderado por el tercero, similar a un mediador, que trata de explorar un acuerdo.

Cuando es el agente de custodia (*escrow*) quien actúa como tercero, el nombramiento no lo hace el administrador del mercado,[44] en su lugar, las partes se ponen en contacto directamente con el proveedor de custodia y plantean la disputa. Por el contrario, la mayoría de los mercados, como ASAP Market, proporcionan y controlan el sistema de custodia. No obstante, cuando la reclamación se hace directamente al fondo de custodia, la resolución de la disputa se realiza de manera privada.

3. El administrador del mercado: mediación, crowd ODR y adjudicación.

Cuando un sistema de custodia está controlado por el mercado, o cuando el dinero ya se ha transferido al vendedor, los reclamantes pueden publicar su queja en una sección específica del mercado, donde los administradores (o sus moderadores designados por éstos) examinan las pruebas presentadas por las partes y resuelven la disputa. A diferencia de una custodia externa, los administradores del mercado tienen competencias punitivas y reparadoras exclusivas, como la de prohibir al demandado la entrada en el mercado o pedirle que indemnice al demandante.[45]

Si el pago se hubiera depositado en el sistema de custodia facilitado por el mercado, entonces el dinero podrá transferirse a la parte ganadora. Pero, como se ha señalado anteriormente, incluso cuando el dinero no haya sido depositado en el *escrow*, y en su lugar ya haya estado en posesión del vendedor, el éxito de la futura participación de los vendedores en el mercado dependerá del cumplimiento del resultado, ya que los compradores no adquirirán bienes o servicios de vendedores que no cumplan estas resoluciones.[46] Además, el incumplimiento de la resolución puede dar lugar a la expulsión de la parte perdedora del mercado.

44 Kapersky: 'Business on the dark web: Deals and regulatory mechanisms', cit., p. 7; Mirea, M., Wang, V., y Jung, J.: 'The not so dark side of the Dark Net: a qualitative study' SJ, 2019, vol. 32, p. 105.

45 Dupont y Lusthaus: Countering Distrust in Illicit Online Networks: The Dispute Resolution Strategies of Cybercriminals' cit., p. 906.

46 Ibid.

Del mismo modo, en caso de que se constate un comportamiento fraudulento, el administrador expulsará a la parte responsable. Dado que la mayoría de los demandados son vendedores que quieren seguir operando en el mercado, normalmente acatarán el resultado y reembolsarán al comprador cuando así se lo indique el administrador.[47]

El proceso de resolución de disputas comienza cuando los compradores o vendedores denuncian su disputa en la sección de resolución de disputas del mercado. Algunos mercados tienen dos secciones de resolución de disputas, una para disputas contractuales y otra para denunciar estafas y ataques virtuales.[48] Por ejemplo, Exploit, XSS, BreachForums y Verified tienen dos salas distintas para presentar reclamaciones, una de arbitraje, y otra para reclamaciones fraudulentas, que Exploit denomina "Blacklist" y XSS "Ripper List". Dentro de las salas de arbitraje, el proceso de resolución consiste en una adjudicación que no está naturalmente sujeta a la normativa de arbitraje, ya que no necesita de los tribunales para la ejecución de las decisiones. Cuando la disputa se ha realizado en un foro público, la decisión se emitirá después de que otros usuarios del mercado hayan tenido la oportunidad de compartir sus opiniones. Cuando un demandado acepta la reclamación, lo que es más probable que ocurra en transacciones de menor valor, el resultado suele ser la devolución parcial o total del criptopago realizado en la venta disputada. Más comúnmente, cuando el demandado impugna la reclamación, el administrador adjudica la reclamación a la vista de las pruebas aportadas por las partes, y cuando no hay pruebas suficientes para sostener la reclamación, entonces ésta será desestimada.

Los usuarios que deseen denunciar una estafa deben crear un nuevo hilo de conversación, identificar al usuario que supuestamente les ha estafado y proporcionar todos los detalles posibles sobre el incidente. Algunos mercados, como BreachForums, ofrecen una plantilla para denunciar las estafas.[49] A continuación, un moderador revisa la denuncia, pide más información si es necesario y etiqueta al acusado, dándole un plazo para responder, que suele ser de 24 horas, pero que puede variar en función de la gravedad del caso y del mercado. Por ejemplo, el Chinese Market establece un límite de tres días por el que, si una de las partes no contesta antes de que expire el plazo, la resolución se decidirá a favor de la otra parte. Del mismo modo, el Royal Market establece que, si una de las partes no responde en un plazo de 72 horas, el caso se decidirá probablemente a favor de la parte activa. Otros mercados tienen plazos más largos, como Nemesis, que

47 Choi y Lee: 'In the Name of Dark Web Justice: A Crime Script Analysis of Hacking Services y the Underground Justice System', cit., p. 204.

48 Wixey, M.: 'The scammers who scam scammers on cybercrime forums: Part 1' (*Sophos*, 7 diciembre 2022) https://news.sophos.com/en-us/2022/12/07/the-scammers-who-scam-scammers-on-cybercrime-forums-part-1/.

49 Ibid.

tiene un plazo de siete días. A diferencia de lo que ocurre en las salas de arbitraje, donde las discusiones son en gran medida civiles y las partes pueden incluso llegar a un acuerdo amistoso, cuando se presenta una denuncia por estafa es más habitual que las partes caigan en insultos personales. De hecho, el lenguaje soez no es inusual en la Dark Web, incluso entre los comentarios de los administradores.

En la mayoría de los casos, el proceso de adjudicación sigue un formato informal. En el mercado Dark0de, que funcionó de 2007 a 2015, y que fue reabierto semanas después tras ser incautado por el FBI,[50] no se designó a un adjudicador como tal, dejando que los administradores decidieran su propio papel, que puede ser puramente facilitador, o adoptar el papel de adjudicador.[51] Del mismo modo, en el Mercado Hydra, los miembros de la comunidad del mercado pueden aportar testimonios, aunque, a diferencia del Dark0de, en este mercado el administrador siempre dicta una resolución final cuando las partes no pueden llegar a un acuerdo.[52] Por el contrario, algunos mercados ofrecen procesos privados. Aquí es donde entra en juego el Procedimiento Privado de Reclamación (PCP) por el que, en lugar de hacer público el asunto iniciando una reclamación en el sub-foro, el reclamante puede dirigirse en privado al administrador para solicitar la resolución de la disputa a puerta cerrada.[53]

Mientras que las comunicaciones de las partes suelen cifrarse mediante PGP, una vez que se presenta una disputa, las partes no deben cifrar los mensajes para que el administrador pueda leerlos. El formulario de reclamación suele estar estandarizado, y requiere que los reclamantes incluyan información sobre los nombres de usuarios de las partes, su información de contacto (por ejemplo, dirección de correo electrónico o perfil de Telegram), la cuantía de la reclamación, una breve descripción de la disputa, la petición que se solicita en la reclamación y las pruebas que apoyan la reclamación (por ejemplo, registros de chat, capturas de pantalla, registros de transacciones de criptomoneda, etc).[54] Aunque la reclamación puede publicarse en el sub-foro, las pruebas no suelen publicarse en dicho sub-foro, sino que se envían en privado al administrador. Esto se debe

50 Europol 'Cybercriminal Darkode Forum Taken Down Through Global Action' (15 julio 2015). Véase https://www.europol.europa.eu/content/cybercriminal-darkode-forum-taken-down-through-global-action y Stevenson, A.: 'It only took 2 weeks for the world's most dangerous hacking forum to get back online after the FBI shut it down' Insider (28 July 2015). Véase https://www.businessinsider.com/darkode-admin-returns-with-new-and-improved-hacking-site-2015-7?r=US&IR=T.

51 Dupont y Lusthaus: Countering Distrust in Illicit Online Networks: The Dispute Resolution Strategies of Cybercriminals', cit., p. 905.

52 Social Links, 'Top-10 OSINT and Cyber Security Stories of 2022' (*Social Links*, 28 diciembre 2022) https://blog.sociallinks.io/top-10-osint-and-cyber-security-stories-of-2022/.

53 Dupont y Lusthaus: 'Countering Distrust in Illicit Online Networks: The Dispute Resolution Strategies of Cybercriminals', cit., p. 899.

54 Vijayan, J.: 'The Dark Web Has Its Own People's Court' (*Dark Reading*, 8 diciembre 2021) https://www.darkreading.com/threat-intelligence/the-dark-web-has-its-own-people-s-courts; y Choi y Lee, : 'In the Name of Dark Web Justice: A Crime Script Analysis of Hacking Services y the Underground Justice System', cit., p.216; y Vanian: 'Online criminals have created their pseudo court system on the dark web' cit.

a que las partes serían reacias a proporcionar información que pudiera revelar su identidad o comprometer su seguridad, como proporcionar pruebas de que los artículos comprados han sido entregados en la dirección designada. Por ello, este tipo de información suele enviarse directamente a través de mensajes privados al administrador. Como no es aconsejable descargar nada en la Dark Web, para subir imágenes los usuarios emplean un software especializado, como filehole.org, que permite acceder a documentos y archivos a través de un enlace.

Una vez presentada la reclamación en el sub-foro, normalmente en cuestión de horas, el tercero neutral se pondrá en contacto con el demandado y le pedirá pruebas sobre la transacción en litigio.[55] En algunos casos, el tercero neutral abrirá un sub-foro independiente en el que otros usuarios del mercado podrán aportar sus opiniones sobre el caso.[56] Este proceso se asemeja al sistema de resolución colectivo (también conocido como *crowd online dispute resolution*), en el que un grupo de usuarios actúan como jurados resolviendo las disputas.[57] Sin embargo, a diferencia de los jurados de los tribunales o de los procesos de *crowd-ODR*, las opiniones de los usuarios no son vinculantes, ya que sólo los administradores (o sus terceros neutrales designados) tienen plena autoridad para adjudicar el resultado de la disputa.[58] En este modelo, todos los usuarios del mercado pueden publicar sus opiniones y comentarios en el sub-foro. Aunque sus opiniones no influyan necesariamente en el resultado del litigio, su capacidad para ver y comentar el fondo de la demanda va más allá del principio de justicia abierta, ya que los usuarios no son meros observadores, sino terceros intervinientes (también conocidos como *amicus curia*e en el contexto de los litigios judiciales),[59] cuyas opiniones buscan influir en última instancia en la decisión de las partes de llegar a un acuerdo o en la decisión final del administrador.

Aunque los administradores gozan de plena discrecionalidad para adoptar sus decisiones, éstas se basan en las pruebas aportadas por las partes y se ajustan a las normas del mercado y a los términos y condiciones de la transacción. El criterio de prueba utilizado se asemeja al empleado en el derecho privado inglés

55 Vanian, ibid; CyberSec_Sai, 'Did You Know Darkweb Has Its Own Courts and Justice System?' (*Medium*, 8 marzo 2023) https://medium.com/geekculture/did-you-know-darkweb-has-its-own-courts-and-justice-system-7ecfa25c46c8; Choi y Lee: 'In the Name of Dark Web Justice: A Crime Script Analysis of Hacking Services y the Underground Justice System', cit., p. 216.

56 Kapersky, 'Business on the dark web: Deals and regulatory mechanisms', cit., p. 13.

57 Raymond, A. y Stemler, A.: 'Trusting Strangers: Dispute Resolution in the Crowd' *Cardozo Journal of Conflict Resolution,* 2014, vol. 16, p. 357.

58 Bisson, D., 'How a Cyber Criminal Justice System Resolves Disputes' (*Security Intelligence,* 26 enero 2022) https://securityintelligence.com/news/cyber-criminal-justice-system-resolves-disputes/; Analyst1, 'Dark Web – Justice League' (*Analyst1,* 2021) https://analyst1.com/dark-web-justice-league/; Mujezinovic, D.: 'How to Police Hackers: Inside the Dark Web's Justice System' (*MakeUseOf,* 31 diciembre 2021) https://www.makeuseof.com/inside-dark-webs-justice-system/; Bracken, B.: 'When Scammers Get Scammed, They Take It to Cybercrime Court' (*threat post,* 7 diciembre 2021) https://threatpost.com/scammers-cybercrime-court/176834/.

59 Krislov, S., 'The Amicus Curiae Brief: From Friendship to Advocacy' *Yale Law Journal,* 1963, vol. 72, p. 694.

del balance de probabilidades. La carga de la prueba recae en el demandante, que debe convencer al administrador del fundamento de su reclamación, pero si el demandado no responde, puede ser suspendido o expulsado permanentemente del mercado.

Tanto si las partes llegan a un acuerdo como si es un tercero el que resuelve la reclamación, la decisión final suele publicarse en el sub-foro.[60] Sin embargo, se han dado casos en los que el administrador ha accedido a la petición del demandado de borrar la reclamación para proteger la reputación del vendedor frente a futuros compradores.[61] Por lo tanto, la eliminación de la reclamación queda a discreción del administrador, pero se espera que los demandados acaten el resultado antes de que se elimine el mensaje del foro. La petición de borrar la reclamación ilustra lo importante que es la reputación para los vendedores.

Si se estima la demanda, el procedimiento suele terminar con la obligación de indemnizar al demandante por una parte o por el coste total de la transacción. Si el demandado es declarado responsable pero no devuelve el dinero en el plazo fijado por el administrador, suele ser expulsado del mercado y añadido a la lista de miembros poco fiables de la comunidad. En esencia, se trata de una "lista negra" (a veces denominada "lista de defraudadores" o simplemente "doxing") que indica no sólo el nombre de usuario, sino que también puede incluir el nombre del mercado, el motivo de la prohibición y otros datos identificativos, como las criptomonedas o monederos electrónicos utilizados, correos electrónicos y apodos empleados en otros mercados de la Dark Net.[62] Otras consecuencias menos comunes incluyen el "swatting", que consiste en hacer una llamada a la policía para que acuda al lugar donde se encuentra el objetivo.[63]

Con todo, la consecuencia más común para un demandado que no acata la decisión del adjudicador es su expulsión del mercado.[64] Los demandantes también pueden ser vetados por presentar demandas frívolas. Además, si una o ambas partes no han seguido las normas del mercado, el administrador puede enviarles advertencias, suspenderles durante un periodo de tiempo o prohibirles el acceso de forma permanente. Una suspensión temporal puede consistir en que el administrador bloquee la cuenta del demandado hasta que se emita el

60 Kapersky, 'Business on the dark web: Deals and regulatory mechanisms', cit., p.13; Choi y Lee: 'In the Name of Dark Web Justice: A Crime Script Analysis of Hacking Services y the Underground Justice System', cit., p. 206.

61 Ibid, p. 213.

62 Kapersky, 'Business on the dark web: Deals and regulatory mechanisms', cit., p.13.

63 Lusthaus, J.: *Industry of anonymity: Inside the business of cybercrime*, Harvard University Press, 2018.

64 Bisson: 'How a Cyber Criminal Justice System Resolves Disputes' cit. Mujezinovic: 'How to Police Hackers: Inside the Dark Web's Justice System' cit.; Vijayan, J.: 'The Dark Web Has Its Own People's Court' (*Dark Reading,* 8 diciembre 2021) https://www.darkreading.com/threat-intelligence/the-dark-web-has-its-own-people-s-courts; Wixey: 'The scammers who scam scammers on cybercrime forums: Part 1' cit.

reembolso.[65] Una vez publicada la decisión, si las normas del foro lo permiten, las partes pueden apelar la decisión ante otro tercero neutral o ante el administrador que presida el caso. Sin embargo, lo habitual es que la apelación solo pueda tener lugar después de que se haya ejecutado la decisión inicial.

V. EL SURGIMIENTO DE UN ECOSISTEMA DE DERECHO PRIVADO EN LA DARK WEB.

El presente estudio examina cómo la mayoría de los usuarios que participan en el comercio ilícito de la Dark Web tienen acceso a un proceso de resolución de litigios, que a menudo se apoya en un sistema de custodia y en herramientas para evitar litigios, tales como la fianza exigida a los vendedores, advertir a los usuarios de los riesgos fraudulentos e incorporar un sistema de reputación para los vendedores. Cuando las partes no pueden llegar a un acuerdo, normalmente pueden presentar una reclamación poniéndose en contacto con el agente de custodia o con el administrador del mercado (u otro árbitro designado por el administrador) para resolver el litigio en equidad de forma expeditiva basándose en las normas del mercado de la Dark Web donde haya tenido lugar la transacción y en las condiciones contractuales de la transacción. De este modo, en la Dark Net está surgiendo un ecosistema de derecho privado para resolver las disputas que surgen en los mercados ilícitos, similar a la forma en que la *lex mercatoria* y el arbitraje surgieron en Europa durante la Edad Media como una vía más adecuada para resolver las disputas entre los comerciantes internacionales que llegaban por la Ruta de la Seda y por otros itinerarios.

En esta última sección se examina, por un lado, la aparición de un ecosistema de derecho privado que busca aumentar la confianza en el usuario del mercado para fomentar el comercio (ilícito) y, por otro, se explican los rasgos definitorios de los procesos de resolución de disputas ofrecidos en la Dark Web, que se caracterizan por su eficacia (ya que son fácilmente accesibles, gratuitos y muy rápidos), informalidad (las partes se auto-representan), anonimato (ocultan los datos personales de los usuarios y de los terceros neutrales que dirimen las disputas) y porque se basan en mecanismos de auto-ejecución dada su naturaleza extralegal. Además, se argumenta que, aunque estos procesos no pueden garantizar el cumplimiento de las garantías procesales bajo supervisión judicial, los administradores de los mercados tienen incentivos económicos para operar con imparcialidad y garantizar la devolución del pago a los clientes, ya que suelen implicar a la comunidad de usuarios para recabar sus opiniones, y publican las decisiones adoptadas.

65 Choi y Lee: 'In the Name of Dark Web Justice: A Crime Script Analysis of Hacking Services y the Underground Justice System' cit., p. 209.

La aparición de un ecosistema de derecho privado en la Dark Web es inevitable en la medida en que el Estado no valida los contratos ilegales.[66] Sin embargo, estos ecosistemas paralelos de derecho privado no son exclusivos de la Dark Net, sino que también han surgido, aunque a un nivel más localizado, en diferentes contextos tanto ilícitos como legales. Por ejemplo, se han publicado investigaciones sobre el autogobierno en entornos como las prisiones,[67] los barrios bajo control del IRA en Belfast,[68] las favelas de Río de Janeiro,[69] la esfera de los ladrones profesionales[70] y en el tráfico de drogas.[71] En estos entornos, la coerción violenta desempeña un papel crucial para la gobernanza de estos sindicatos del crimen organizado, imponiendo el funcionamiento del proceso de resolución de disputas y garantizando el cumplimiento de sus resultados.[72] Así pues, una distinción importante entre los sistemas de resolución de litigios en la Dark Web y la resolución de litigios tradicional en los bajos fondos de la delincuencia reside en la ausencia de amenaza real de violencia en el espacio digital.[73] Otra distinción crucial es el anonimato de los usuarios. De hecho, el objetivo de los sistemas de resolución de litigios en la Dark Web no es otro que aumentar la confianza entre los usuarios que desean realizar transacciones ilícitas con comerciantes anónimos, incluso con hackers y estafadores profesionales.

Más allá de las actividades delictivas, diferentes tipos de comunidades que operan dentro de los límites de la ley también han creado procesos de resolución de disputas para aplicar sus propias normas al margen de la ley estatal sin necesidad de recurrir a los Tribunales. Por ejemplo, en ámbito del matrimonio la Iglesia Católica y los judíos ortodoxos han desarrollado sus propios sistemas de resolución de litigios basados en sofisticadas normas sustantivas y procesales.[74] Estas instituciones no dependen de los tribunales estatales para hacer cumplir los resultados, ya que los usuarios se someten voluntariamente a estos sistemas autónomos de resolución de litigios que suelen tener sus propios mecanismos de ejecución.[75]

66 Dixit, A.: *Lawlessness and economics: Alternative Modes of Governance*, Princeton University Press, 2004.

67 Skarbek, D.: 'Governance and Prison Gangs' *American Political Science Review* 2011, vol. 105, num. 4, pp. 702–716.

68 Hamill, H.: *The Hoods: Crime and Punishment in Belfast*, Princeton University Press, 2011.

69 Arias, E., y Rodrigues, C.: 'The Myth of Personal Security: Criminal Gangs, Dispute Resolution, And Identity in Rio de Janeiro's Favelas' *Latin American Politics and Society* 2006, vol. 48, num 4, pp. 53–81.

70 Conwell, C., y Sutherland, E.: *The Professional Thief*, University of Chicago Press, 1956.

71 Reuter, P.: 'Systemic Violence in Drug Markets' *Crime, Law and Social Change*, 2009, vol. 52, num 3, pp. 275–289.

72 Véase also, Campana, P. y Varese, F.: 'Organized crime in the United Kingdom: Illegal Governance of Markets and Communities' *British Journal of Criminology,* 2018, vol. 58, num 6, p. 1393.

73 Dupont y Lusthaus, 'Countering Distrust in Illicit Online Networks: The Dispute Resolution Strategies of Cybercriminals', cit., p. 218.

74 Broyde, M.: *Sharia Tribunals, Rabbinical Courts, and Christian Panels,* Oxford University Press, 2017, pp. 51–8, 151–3.

75 Bussani, M.: 'Strangers in the Law: Lawyers' Law and the Other Legal Dimensions' *Cardozo Law Review,* 2019, vol. 40, p. 3148.

Podría decirse que estos sistemas de resolución de litigios, especialmente los de la Dark Web, se basan en un enfoque libertario y en una teoría de la justicia que contradice los principios democráticos liberales y el Estado de Derecho. No sólo porque su uso permite la proliferación de actividades delictivas, sino también porque el proceso de resolución de disputas no ofrece garantías procesales, ni asegura una supervisión judicial sujeta a una revisión en apelación como se requiere en cualquier Estado de Derecho. En consecuencia, los sistemas de resolución de litigios en la Dark Net plantean una serie de riesgos en términos de equidad procesal y sustantiva porque no están regulados ni supervisados y, por tanto, no pueden garantizar que sean imparciales o justos. Además, un reto añadido en los sistemas de resolución de litigios que operan en la Dark Web es la falta de transparencia, que se ve aumentada por el anonimato de las partes, y la falta de claridad de las pruebas necesarias para sustentar una demanda con éxito.

Por el contrario, en este estudio se ha observado que los adjudicadores tratan de impulsar la transparencia y la legitimidad en el proceso de resolución de litigios consultando a la comunidad del mercado y, lo que es más importante, tienen incentivos económicos para actuar de forma imparcial y de acuerdo con las normas del mercado y las condiciones contractuales de la transacción, ya que, de lo contrario, los usuarios irían a otros mercados de la competencia. En consecuencia, la herramienta de resolución de litigios en la Dark Web ofrece una opción de reparación accesible e imparcial, que cumple conalgunos requisitos del Estado de Derecho, ya que los litigios se resuelven de conformidad con el contrato y las normas del mercado, y el proceso de resolución de litigios está dirigido por terceros imparciales que reflejan la diversidad de las comunidades en las que operan. [76]

En una línea similar, a medida que las normas sustantivas y procesales van surgiendo orgánicamente para abordar las características idiosincrásicas de los litigios en la Dark Web, es posible trazar una línea comparativa con la *lex mercatoria* que surgió como un importante cuerpo de derecho mercantil para los comerciantes en Europa durante la época medieval, mitigando así los retos para los comerciantes internacionales a la hora de cumplir con las costumbres locales. De forma comparable al desarrollo de la *lex mercatoria* (e incluso del *common law* inglés),[77] los procesos de resolución de litigios en la Dark Web están evolucionando como sistemas basados en costumbres y prácticas internacionalmente aceptadas, que ahora se encuentran cada vez más codificadas como parte de las normas de los mercados de la Dark Net. De ahí que el entorno en línea y su naturaleza transfronteriza hayan dado lugar al desarrollo de estas medidas de autogobierno.

76 Véase 'What Is Rule of Law?', *World Justice Project*, www.worldjusticeproject.org/about-us/overview/what-rule-law. Véase Tushnet, M., 'Critical Legal Studies and the Rule of Law', en Loughlin, M. y Meierhenrich, J. (eds.), *The Cambridge Companion to the Rule of Law*, Cambridge University Press, 2021, pp. 3-22.

77 Baker, JH: "The Law Merchant and the Common Law" *Cambridge Law Journal,* 1979, vol. 38, num 2, p. 295.

Aunque la legislación estatal se aplica para regular ciertos aspectos de Internet, como la protección de datos y las leyes de propiedad intelectual, la mayoría de las relaciones, especialmente en las redes sociales, se rigen por los términos y condiciones de estas redes y mercados. Como observa Bussani, "la legitimidad de esta gobernanza reside en el ideal de autodeterminación y autorregulación, y estos mundos virtuales crean su propia ley, que casi nunca se aplica a través de los canales legales oficiales".[78] A pesar de que estos espacios operan dentro de los límites de la legislación estatal, la aplicación de las normas y decisiones corre a cargo, en gran medida, de los administradores de estos espacios, que refuerzan sus propias concepciones contextuales del comportamiento aceptable.[79] Estas normas se denominan a veces *lex informática* para englobar la autorregulación desarrollada por la comunidad de usuarios de Internet como parte de sus normas y reglas habituales. Así pues, la *lex informática* puede considerarse parte de la regulación del ciberespacio[80] y una extensión de la *lex mercatoria*.[81]

De forma similar a cómo surgieron la lex mercatoria y la *lex informatica*, la autonomía social y económica de la Dark Web está contribuyendo a la generación de normas internas para regular sus transacciones ilícitas, que enfatizan la libertad contractual, evitan deliberadamente los tecnicismos legales y deciden los casos sin referencias a la ley, basándose en las reglas del mercado, las condiciones contractuales de la transacción y en lo que el juzgador considera justo y razonable en las circunstancias específicas del caso (es decir, basándose en el principio equitativo de *ex aequo et bono*). Así pues, este ámbito social autónomo cuenta con un ecosistema de derecho privado propio que funciona de forma paralela e independiente del Derecho estatal. Y lo hace de un modo más efectivo y accesible que el funcionamiento de los tribunales estatales a los que las partes con disputas sobre transacciones ilicitals no pueden acudir, aunque con una merma de garantías procesales.

Los procesos de resolución de disputas en la Dark Web siguen el modelo de justicia informal que ha caracterizado a los procesos extrajudiciales (*Alternative Dispute Resolution* o *ADR)*. Estos procesos se caracterizan por su estructura no burocrática basada en procesos *ad hoc* que operan en mercados virtuales relativamente pequeños.[82] Los procesos son accesibles a los usuarios del mercado sin necesidad de intermediarios legales, como abogados, que se requieren en los

78 Bussani, Strangers in the Law: Lawyers' Law and the Other Legal Dimensions' cit., p. 3156.

79 Ibid, p. 3157. Véase, Suzor, N., 'Order Supported by Law: The Enforcement of Rules in Online Communities' Mercer L. Rev., 2012, vol. 63 p. 523, 530.

80 Johnson, D. y Post D.: "Law and Borders: The Rise of Law in Cyberspace" *Stanford Law Review,* 1996, vol. 48, num. 5, p. 1367.

81 Wright, A. y De Filippi, P.: 'Decentralized Blockchain Technology and the Rise of Lex Cryptographia' (10 marzo 2015). Véase https://ssrn.com/abstract=2580664.

82 Palmer, M., y Simon, R.: *Dispute Processes - ADR and the Primary Forms of Decision-making*, 3rd ed., Cambridge University Press, 2020, p. 18.

procesos formales de resolución de disputas como el arbitraje o la via jurisdiccional. El proceso de resolución de conflictos está diseñado y dirigido por administradores del mercado con poca o ninguna formación en resolución de conflictos, y mucho menos en Derecho. Además, las normas sustantivas se elaboran a partir de los valores de la comunidad y la libertad contractual, en lugar de basarse en la legislación estatal. Del mismo modo, las normas de procedimiento son en gran medida imprecisas, no escritas y flexibles.

Los procesos de resolución de litigios en la Dark Web, al igual que los de los tribunales nacionales y en los sistemas regulados de ADR, como en el caso de los *ombudmen* y defensores del consumidor, tienen una función pública que va más allá de ofrecer reparación a los demandantes particulares. Su principal objetivo es promover la confianza dentro de la comunidad del mercado, y lo consiguen, entre otras cosas, disuadiendo comportamientos fraudulentos, evitando la aparición de nuevas disputas, buscando justicia e igualdad para la comunidad y expresando una identidad comunitaria. Estos objetivos también se encuentran en los mercados legales de Clear Web, ya que buscan igualmente aumentar la confianza de los usuarios y fomentar el comercio. Una investigación empírica en eBay descubrió que ofrecer un proceso de resolución de litigios aumenta la lealtad de los usuarios, incrementando incluso la actividad económica de quienes pueden resolver sus disputas de forma expeditiva.[83] Sin embargo, una peculiaridad de los foros de resolución de disputas de la Dark Net es que los administradores del sitio suelen leer las disputas y, al mismo tiempo que las resuelven, obtienen información sobre las causas de las mismas, de modo que pueden identificar mecanismos para evitar que surjan en el futuro, introduciendo cambios en el diseño del Mercado. Por ejemplo, un sub-foro del Archetyp Market afirma que el moderador detectó que los compradores frecuentemente no podían iniciar reclamaciones porque se les pasaba el breve plazo para hacerlas, por lo que el administrador añadió una función que advertía con antelación a los compradores del plazo límite para iniciar un litigio.

Mientras que los tribunales nacionales, e incluso los procesos ADR, no suelen proporcionar un acceso efectivo a los usuarios más pobres o marginados,[84] podría argumentarse que los procesos de resolución de litigios en la Dark Net pueden ser más eficaces y accesibles para todos los usuarios. Esto se debe a que es más probable que estos usuarios tengan mayores conocimientos informáticos que los consumidores medios, ya que necesitan estos conocimientos para procesar una

83 Rule, C.: 'Quantifying the Economic Benefits of Effective Redress: Large E-Commerce Data Sets and the Cost-Benefit Case for Investing in Dispute Resolution' *University of Arkansas Little Rock Law Review,* 2012, vol. 34, pp. 767–777.

84 Véase Galanter., M. y Krishnan, J.: 'Lok Adalats and Legal Rights in Modern India', en E. Jensen y T. Heller (eds) *Beyond Common Knowledge: Empirical Approaches to the Rule of Law,* Stanford University Press, 2003, pp. 96–127.

transacción (es decir, desde acceder a la Dark Net hasta pagar con criptomoneda y cifrar sus datos personales). Es posible que a estos usuarios no les resulte difícil participar en el proceso de resolución de litigios, que básicamente requiere que expliquen su reclamación y adjunten capturas de pantalla en un entorno más bien informal. Sin embargo, como las disputas están relacionadas con transacciones ilícitas, es posible que usuarios, a pesar de operar de manera anónima, decidan no presentar una reclamación, especialmente cuando sus reclamaciones se comparten en un sub-foro público. Así pues, las herramientas para evitar disputas también desempeñan un papel crucial como complemento de los sistemas de resolución de disputas.

Aunque los mecanismos de resolución de disputas en la Dark Web no distinguen entre casos penales y civiles, como se ha señalado en la sección anterior, varios mercados han desarrollado dos sistemas separados, uno para procesar las reclamaciones de comportamiento fraudulento, y otro para resolver disputas cuando no hay pruebas claras de fraude. Mientras que el principal remedio y objetivo de las listas de estafadores es eliminar a los vendedores deshonestos prohibiendo su participación en el mercado, el remedio más común en el proceso de resolución de disputas es la reasignación del pago de la transacción, o parte de él, a la parte ganadora. La ejecución de una decisión puede ser llevada a cabo por el administrador cuando tiene el control sobre la criptomoneda, e incentivando el cumplimiento voluntario para evitar la expulsión del mercado. Sin embargo, este tipo de sistema no es infalible, ya que las decisiones no siempre pueden autoejecutarse, especialmente cuando el demandado desaparece del mercado y las partes no han utilizado un sistema de custodia, o cuando el pago de la transacción ya se ha transferido al vendedor.

VI. CONCLUSIÓN.

La resolución de controversias contractuales, sean o no sobre transacciones ilícitas, no son monopolio del Estado. Sin embargo, el Estado no ejecutará las decisiones relativas al comercio ilegal. Como resultado, los mercados en la Dark Net han desarrollado sus propias herramientas que buscan evitar la aparición de disputas a través del uso de advertencias sobre usuarios fraudulentos, requiriendo el pago de una fianza a los vendedores y administrando un sistema de reputación para los vendedores. Cuando surgen disputas y las partes no pueden llegar a un acuerdo amistoso, generalmente confían en el servicio de custodia (*escrow*) y en el administrador del mercado para resolver las disputas. La comunidad del mercado también juega un papel importante, a menudo informando a los usuarios sobre las posibilidades de éxito de la reclamación y fomentando la resolución colaborativa de los conflictos.

Hasta la fecha la investigación de la resolución de disputas dentro de la Dark Web ha sido extremadamente escasa. Estos mecanismos, junto con sus sistemas de gobierno, han logrado aumentar la confianza de los usuarios en estos mercados ilícitos, lo que permite que miles de personas desconocidas participen en transacciones ilegales entre sí. Por lo tanto, funciona como una herramienta eficaz para generar y gestionar la confianza entre los usuarios, ayudando a expandir la actividad delictiva de estos mercados.

De manera similar a cómo surgió la *lex mercatoria* a través del establecimiento de tribunales arbitrales ubicados a lo largo de las principales rutas comerciales europeas, los procesos de resolución de disputas se están erigiendo en los mercados digitales, tanto legales como ilegales. Además, el servicio de custodia suele garantizar la ejecución de las decisiones. Como primer análisis legal académico de los métodos de resolución de disputas empleados en la Dark Web, el presente estudio ha pretendidodo mejorar nuestro conocimiento sobre un ecosistema de derecho privado que está emergiendo en la Dark Web con el objetivo de eliminar a los usuarios fraudulentos y brindar reparación a la comunidad de usuarios. Dichos procesos podrían extenderse al comercio electrónico legal en la medida en que éste empiece a aceptar pagos en criptomonedas o utilice sistemas de depósitos (*escrows*).

BIBLIOGRAFÍA

Afilipoaie, A., y Shortis, P.: 'From Dealer to Doorstep – How Drugs are Sold on the Dark Net' *Global Drug Policy Observatory, Situation Analysis*, 2015.

Aminuddi, M., Zaaba, Z., Samsudin, A., Zaki, F. y Anuar, N.: 'The rise of website fingerprinting on Tor' *Journal of Network and Computer Applications,* 2023.

Analyst1, 'Dark Web – Justice League' (*Analyst1,* 2021) https://analyst1.com/dark-web-justice-league/

Arias, E., y Rodrigues, C.: 'The Myth of Personal Security: Criminal Gangs, Dispute Resolution, And Identity in Rio de Janeiro's Favelas' *Latin American Politics and Society* 2006, vol. 48, num 4, pp. 53–81.

Baker, JH: 'The Law Merchant and the Common Law' *Cambridge Law Journal,* 1979, vol. 38, num 2, p. 295.

Bisson, D., 'How a Cyber Criminal Justice System Resolves Disputes' (*Security Intelligence,* 26 enero 2022) https://securityintelligence.com/news/cyber-criminal-justice-system-resolves-disputes/.

Bracken, B.: 'When Scammers Get Scammed, They Take It to Cybercrime Court' (*threat post,* 7 diciembre 2021) https://threatpost.com/scammers-cybercrime-court/176834/.

Broyde, M.: *Sharia Tribunals, Rabbinical Courts, and Christian Panels,* Oxford University Press, 2017, pp. 51–8, 151–3.

Bussani, M.: 'Strangers in the Law: Lawyers' Law and the Other Legal Dimensions' *Cardozo Law Review,* 2019, vol. 40, p. 3148.

Campana, P. y Varese, F.: 'Organized crime in the United Kingdom: Illegal Governance of Markets and Communities' *British Journal of Criminology,* 2018, vol. 58, num 6, p. 1393.

Campana, P., y Varese, F.: 'Cooperation in criminal organizations: Kinship and violence as credible commitments' *Rationality and Society,* 2013, vol. 25, num 3, p. 265.

Chertoff, M. y Simon, T.: 'The Impact of the Dark Web on Internet Governance and Cyber Security, Global Commission on Internet Governance', Paper Series: No. 6 febrero 2015.

Choi, K-S and Lee, CS,: 'In the Name of Dark Web Justice: A Crime Script Analysis of Hacking Services y the Underground Justice System' *Journal of Contemporary Criminal Justice* 2023, vol. 39, num. 2, p. 201.

Conwell, C., y Sutherland, E.: *The Professional Thief*, University of Chicago Press, 1956.

Croy, A.: *The Dark Web: The Covert World of Cybercrime*, Greenhaven Publishing LLC, 2018.

CyberSec_Sai, 'Did You Know Darkweb Has Its Own Courts and Justice System?' (*Medium*, 8 marzo 2023) https://medium.com/geekculture/did-you-know-darkweb-has-its-own-courts-and-justice-system-7ecfa25c46c8.

Cybersixgill, 'Trust on the Deep and Dark Web' (22 marzo 2022). Véase https://cybersixgill.com/news/articles/trust-on-the-deep-and-dark-web.

Davies, G.: 'Shining a light on policing of the Dark Web: an analysis of UK investigatory powers' *Journal of Criminal Law,* 2020, vol. 84 num 5, 408.

DeNicola, L.: 'What is the Dark Web?' *Experian - Cybersecurity* (12 mayo 2021). Véase https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/

Dixit, A.: *Lawlessness and economics: Alternative Modes of Governance*, Princeton University Press, 2004.

DoingFedTime, 'Dispute Resolution Buyers vs Vendors – Deep Dot Dark Net' (27 noviembre 2022). https://www.youtube.com/watch?v=qwZvflkl-9c&t=12s.

Doyle, E.: *The Dark Web*, Greenhaven Publishing LLC, 2019.

Dupont, B., y Lusthaus, J.: 'Countering Distrust in Illicit Online Networks: The Dispute Resolution Strategies of Cybercriminals' *Social Science Computer Review,* 2021, vol. 40 num 4, p. 892.

Electronic Frontier Foundation, 'GCHQ Leak: A Potential Technique to Deanonymise Users of the TOR Network' UK Top Secret Strap1 Comint, OPC-M/TECH.B/61 (13 June 2011). Véase https://www.eff.org/document/20141228-speigel-potential-technique-deanonymise-users-tor-network.

Europol 'Cybercriminal Darkode Forum Taken Down Through Global Action' (15 julio 2015). Véase https://www.europol.europa.eu/content/cybercriminal-darkode-forum-taken-down-through-global-action

FINKLEA, K.: 'Dark Web', Congressional Research Service, 7-5700, R44101 (10 marzo 2017) p. 2. Véase https://a51.nl/sites/default/files/pdf/R44101%20(1).pdf.

GALANTER., M. y KRISHNAN, J.: 'Lok Adalats and Legal Rights in Modern India', en E. JENSEN y T. HELLER (eds) *Beyond Common Knowledge: Empirical Approaches to the Rule of Law*, Stanford University Press, 2003, pp. 96–127.

HAMILL, H.: *The Hoods: Crime and Punishment in Belfast*, Princeton University Press, 2011.

HOFFMAN, H.: 'Facebook's Dark Web .Onion Site Reaches 1 Million Monthly Tor Users' (22 abril 2016). Véase https://www.inverse.com/article/14672-facebook-s-dark-web-onion-site-reaches-1-million-monthly-tor-users.

HOLLAND, A. et al.,: 'The Evolution of Cybercrime: Why the Dark Web is Supercharging the Threat Landscape and How to Fight Back' An HP Wolf Security Report' 2022. Véase https://threatresearch.ext.hp.com/wp-content/uploads/2022/07/HP-Wolf-Security-Evolution-of-Cybercrime-Report.pdf

HOLT, T. y LAMPKE, E., 'Exploring stolen data markets online: Products and market forces' *Criminal Justice Studies*, 2010, vol. 23, num. 1, pp. 33–50.

HOLT, T.: 'Exploring the social organisation and structure of stolen data markets' *Global Crime* vol. 2013, num. 14(2-3), pp. 155–174.

HP Wolf Security et al, 'The Evolution of Cybercrime: Why the Dark Web is Supercharging the Threat Landscape y How to Fight Back – An HP Wolf Security Report' (julio 2022). https://threatresearch.ext.hp.com/wp-content/uploads/2022/07/HP-Wolf-Security-Evolution-of-Cybercrime-Report.pdf p. 15.

JARDINE, E.: 'The Dark Web Dilemma: Tor, Anonymity and Online Policing' *Global Commission on Internet Governance Paper Series,* 2015, vol. 21. Véase https://ssrn.com/abstract=2667711.

JOHNSON, D. y POST D.: "Law and Borders: The Rise of Law in Cyberspace" *Stanford Law Review,* 1996, vol. 48, num. 5, p. 1367.

KAPERSKY, 'Business on the dark web: Deals and regulatory mechanisms', 2023. Véase https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2023/03/10151223/Business-on-the-dark-web-deals-and-regulations.pdf?reseller=gl_regular-sm_acq_ona_oth__onl_b2b_securelist_lnk_sm-team.

KRISLOV, S., 'The Amicus Curiae Brief: From Friendship to Advocacy' *Yale Law Journal,* 1963, vol. 72, p. 694.

LUMMEN, DLM: 'Is Telegram the new Dark Net? A comparison of traditional and emerging digital criminal marketplaces' (MSc thesis, University of Twente 2023), p. 49.

LUSTHAUS, J.: *Industry of anonymity: Inside the business of cybercrime*, Harvard University Press, 2018.

MIREA, M., WANG, V., y JUNG, J.: 'The not so dark side of the Dark Net: a qualitative study' SJ, 2019, vol. 32, p. 105.

MUJEZINOVIC, D.: 'How to Police Hackers: Inside the Dark Web's Justice System' (*MakeUseOf,* 31 diciembre 2021) https://www.makeuseof.com/inside-dark-webs-justice-system/.

ORTOLANI, P.: 'Self-enforcing online dispute resolution: lessons from Bitcoin' Oxf. J. Legal Stud., 2016, vol 36, pp. 595–629.

PALMER, M., y SIMON, R.: *Dispute Processes - ADR and the Primary Forms of Decision-making*, 3rd ed., Cambridge University Press, 2020.

RAYMOND, A. y STEMLER, A.: 'Trusting Strangers: Dispute Resolution in the Crowd' *Cardozo Journal of Conflict Resolution,* 2014, vol. 16, p. 357.

REUTER, P.: 'Systemic Violence in Drug Markets' *Crime, Law and Social Change,* 2009, vol. 52, num 3, pp. 275–289.

RULE, C.: 'Quantifying the Economic Benefits of Effective Redress: Large E-Commerce Data Sets and the Cost-Benefit Case for Investing in Dispute Resolution' *University of Arkansas Little Rock Law Review,* 2012, vol. 34, pp. 767–777.

SKARBEK, D.: 'Governance and Prison Gangs' *American Political Science Review* 2011, vol. 105, num. 4, pp. 702–716.

Social Links, 'Top-10 OSINT and Cyber Security Stories of 2022' (*Social Links*, 28 diciembre 2022) https://blog.sociallinks.io/top-10-osint-and-cyber-security-stories-of-2022/.

STEVENSON, A.: 'It only took 2 weeks for the world's most dangerous hacking forum to get back online after the FBI shut it down' Insider (28 July 2015). Véase https://www.businessinsider.com/darkode-admin-returns-with-new-and-improved-hacking-site-2015-7?r=US&IR=T.

SUZOR, N., 'Order Supported by Law: The Enforcement of Rules in Online Communities' Mercer L. Rev., 2012, vol. 63 p. 523.

The Onion Router Project. Véase https://www.torproject.org/projects/torbrowser.html.en.

Tushnet, M., 'Critical Legal Studies and the Rule of Law', en Loughlin, M. y Meierhenrich, J. (eds.), *The Cambridge Companion to the Rule of Law*, Cambridge University Press, 2021.

United Nations Office on Drugs and Crime, Global Overview – Drug Demand Drug Supply, Global Drug Report 2022. Véase https://www.unodc.org/res/wdr2022/MS/WDR22_Booklet_2.pdf.

US Department of Justice - Office of Public Affairs, 'Individual Arrested and Charged with Operating Notorious Darknet Cryptocurrency "Mixer"' (28 abril 2021). Véase https://www.justice.gov/opa/pr/individual-arrested-and-charged-operating-notorious-darknet-cryptocurrency-mixer.

Vanian, J.: 'Online criminals have created their pseudo court system on the dark web' *Fortune* (7 diciembre 2021). Véase https://fortune.com/2021/12/07/online-criminals-court-system-dark-web-russian-hackers-ransomware/

Vijayan, J.: 'The Dark Web Has Its Own People's Court' (*Dark Reading,* 8 diciembre 2021) https://www.darkreading.com/threat-intelligence/the-dark-web-has-its-own-people-s-courts;

White, G., y Archampong, P.: The Dark Web, Episode 7, Cybercrime Inc, Podcast, (8 febrero 2018).

Wixey, M.: 'The scammers who scam scammers on cybercrime forums: Part 1' (*Sophos*, 7 diciembre 2022) https://news.sophos.com/en-us/2022/12/07/the-scammers-who-scam-scammers-on-cybercrime-forums-part-1/.

Wright, A. y De Filippi, P.: 'Decentralized Blockchain Technology and the Rise of Lex Cryptographia' (10 marzo 2015). Véase https://ssrn.com/abstract=2580664.

Yip, M. , Webber, C., Shadbolt, N.: 'Trust among cybercriminals? Carding forums, uncertainty and implications for policing' *Policing and Society*, 2013, vol. 23, num. 4, pp. 516–539.

LA LUCHA CONTRA EL ABUSO SEXUAL DE MENORES EN INTERNET: REFLEXIONES A LA LUZ DE LA PROPUESTA DE REGLAMENTO*

COMBATING CHILD SEXUAL ABUSE ON THE INTERNET: CONSIDERATIONS IN THE LIGHT OF THE PROPOSAL FOR A REGULATION

Actualidad Jurídica Iberoamericana Nº 21, agosto 2024, ISSN: 2386-4567, pp. 104-129

* Estudio redactado en el marco del Proyecto "Claves para una justicia digital y algorítmica con perspectiva de género", PID2021-123170OB-I00 financiado por MCIN/ AEI/10.13039/501100011033.

Elena DE LUIS GARCÍA

ARTÍCULO RECIBIDO: 29 de mayo de 2023
ARTÍCULO APROBADO: 1 de julio de 2024

RESUMEN: Los avances en la sociedad de la información y las nuevas tecnologías de la comunicación han traído consigo un incremento alarmante de los delitos de abuso sexual de menores a través de internet. Las herramientas disponibles hasta la fecha para la lucha contra esta clase de criminalidad han resultado insuficientes, por lo que se ha puesto de manifiesto la necesidad de reforzar la regulación y desarrollar nuevos mecanismos que permitan prevenir y combatir eficazmente estas conductas. Con dicho fin se presentó en el año 2022 la Propuesta de Reglamento de la Unión Europea para prevenir y combatir el abuso sexual de los menores.

PALABRAS CLAVE: Abuso sexual; menores; nuevas tecnologías; internet; Unión Europea.

ABSTRACT: *Advances in the Information Society and new communication technologies have brought with them an alarming increase in the sexual abuse of minors via the Internet. The tools available so far to tackle this form of criminality have proved insufficient, which has highlighted the need to strengthen regulation and develop new mechanisms to effectively prevent and combat this type of conduct. To this end, the Proposal for a European Union Regulation to prevent and combat child sexual abuse was presented in 2022.*

KEY WORDS: *Sexual abuse; minors; new technologies; internet: European Union.*

I. APROXIMACIÓN A LA PROBLEMÁTICA.

La sociedad de la información y el desarrollo de nuevas tecnologías de la comunicación han traído con sí indudables ventajas derivadas de la interacción en tiempo real en cualquier parte del mundo y traducidas en una mejora de la eficiencia a nivel público y privado. Sin embargo, no todo son éxitos, sino que también este desarrollo ha propiciado que se produzca un alarmante incremento en la criminalidad a través de internet y, por lo que aquí respecta, en el abuso sexual de menores a través de dicha vía. Es evidente que la clandestinidad e impunidad que caracterizan a los delitos cometidos a través de internet suponen factores que agravan la situación y que propician su comisión. A ello se suma que los mecanismos de intervención son, en la mayoría de las ocasiones, ineficaces.

Como ilustración de lo antedicho podemos citar el informe "Evaluación de la amenaza global de 2023", presentado en octubre de 2023 por la entidad "Weprotect Global Alliance", una alianza de expertos gubernamentales y de la sociedad civil cuyo objeto es la lucha contra la explotación y abuso de menores en internet[1]. En particular, según se señala en dicho documento, en Estados Unidos se han incrementado un 87% las denuncias relativas a material de abuso sexual infantil en internet desde el año 2019. Además, en términos globales han aumentado un 360% las imágenes sexuales de menores de 7 a 10 años autogeneradas, esto es, las que han sido generadas por la propia víctima bajo engaño, coacción o intimidación. También a nivel mundial, un 54% de personas encuestadas con edades comprendidas entre los 18 y los 20 años, manifestaron haber sufrido algún tipo de daño sexual a través de internet antes de cumplir los 18 años. En consecuencia, se recoge en el informe que la mitad de los menores de edad se encuentran en riesgo de sufrir alguna clase de abuso sexual a través de internet.

1 WE PROTECT GLOBAL ALLIANCE, Evaluación de la amenaza global de 2023, 2023. Disponible en: https://www.weprotect.org/wp-content/uploads/Global-Threat-Assessment-2023-ES.pdf

• Elena de Luis García
Profesora Permanente Laboral de Derecho Procesal, Universitat de València. Correo electrónico: elena.deluis@uv.es

En definitiva, lo que dicho informe revela es que, lejos de haber mejorado la prevención y lucha contra esta clase de conductas, año tras año se agrava la situación. Esto demuestra que las herramientas actuales son claramente insuficientes para luchar contra dicha criminalidad y, por lo tanto, pone de manifiesto la necesidad de articular nuevos sistemas que permitan actuar más eficazmente. Así pues, es evidente que estamos ante un problema global, un problema que sigue creciendo exponencialmente y que requiere de todas las medidas legislativas y ejecutivas que puedan adoptarse para combatirlo.

A las dificultades inherentes al medio de comisión de estos delitos, existe una complejidad añadida y es que no estamos ante una única clase de conducta, lo que podría facilitar su prevención y erradicación, sino que el abuso sexual de menores en internet se materializa de distintas maneras. Por un lado, a través de la creación y difusión de material de abuso sexual de menores y, por otro lado, a través del llamado embaucamiento de menores o "online child grooming".

En primer lugar, respecto de la creación y difusión de material de abuso sexual menores, se refiere a la tradicionalmente denominada "pornografía infantil". Sin embargo, evitaremos tal denominación y en su lugar nos referiremos a lo largo de este trabajo a "material de abuso sexual de menores", siguiendo la recomendación contenida en las Orientaciones de Luxemburgo[2]. Conforme señala el documento, el término "pornografía" se emplea principalmente en relación con adultos que participan en actos sexuales consensuados que son distribuidos legal o ilegalmente al público para su satisfacción sexual. Por ello, el empleo del término "pornografía" en relación con menores podría llevar a una normalización voluntaria o involuntaria de una conducta constitutiva de delito grave, en la medida en que el material sexual que involucra a menores nunca puede considerarse producido con consentimiento y, en consecuencia, nunca podrá ser material sexual legal.

En segundo lugar, el embaucamiento de menores o "online child grooming", consiste en el acercamiento de un adulto a un menor a través de internet con fines sexuales, que puede producirse a través de redes sociales, foros, sistemas de mensajería en juegos online, etc. En cualquier caso, la denominación "online child grooming" no encubre un concepto cerrado, sino que vendrá definida por la existencia de un "proceso de seducción y acercamiento a menores que permite la manipulación emocional de éstos con un propósito o fin deliberado, esto es, lograr un posterior contacto sexual"[3]. En un sentido más amplio, se podría identificar con

2 Grupo de trabajo interinstitucional sobre explotación sexual de niñas, niños y adolescentes, Orientaciones terminológicas para la protección de niñas, niños y adolescentes contra la explotación y el abuso sexuales, 2016. Documento disponible en: https://www.interpol.int/es/Delitos/Delitos-contra-menores/Terminologia-apropiada

3 Górriz Royo, E.: "On-line child grooming en Derecho penal español", *Indret: Revista para el Análisis del Derecho*, 2016, núm. 3, p. 7.

la conducta consistente en que un adulto trate de entablar una conversación con un menor aún cuando éste no quiera, que le solicite hablar de sexo, o le solicite que le dé información sexual o que realice alguna conducta sexual no voluntaria[4].

Estamos, en consecuencia, ante una gran variedad de conductas atentatorias contra la libertad e indemnidad sexual de los menores de edad, contra las cuales existe un deber de protección y actuación de los poderes públicos.

Precisamente con dicha finalidad, la Unión Europea ha desplegado una importante actividad legislativa en las últimas décadas, encaminada tanto a mejorar la protección desde el punto de vista del derecho penal sustantivo, como desde la perspectiva de la investigación y enjuiciamiento de tales delitos. Aun cuando actualmente se encuentran en tramitación distintas normas en este ámbito, sus borradores y propuestas permiten aventurar cuál va a ser el futuro en materia de prevención y lucha contra el abuso sexual de menores cometido a través de las nuevas tecnologías. A todo ello, dedicaremos precisamente los siguientes apartados del presente trabajo.

II. EL PAPEL DE UNIÓN EUROPEA EN LA LUCHA CONTRA EL ABUSO SEXUAL DE MENORES EN INTERNET.

1. Antecedentes y evolución legislativa.

En las últimas dos décadas hemos asistido a un importante desarrollo legislativo en el ámbito comunitario en materia de lucha contra el abuso sexual de menores, en general y, por lo que aquí respecta, contra el abuso sexual cometido a través de internet. Así pues, destacaremos a continuación algunos de los principales hitos que han contribuido al fortalecimiento de las medidas y a la armonización de la legislación en los distintos Estados Miembros.

El punto de partida lo encontramos en la Decisión marco 2004/68/JAI relativa a la lucha contra la explotación sexual de los niños y la pornografía infantil[5]. Dicha norma tenía por objeto establecer unos mínimos para la tipificación de las conductas constitutivas de abuso sexual de menores en el territorio de la Unión, para lo cual se definían las conductas que debían ser sancionadas, junto con las posibles circunstancias modificativas de la responsabilidad penal, y también otras cuestiones relativas a la responsabilidad de las personas jurídicas y la competencia para el enjuiciamiento de tales delitos.

4 Villacampa Estiarte, C.: "Predadores sexuales online y menores: grooming y sexting en adolescentes", *Revista electrónica de Ciencias Criminológicas*, 2017, núm. 2, p. 2.

5 Decisión marco 2004/68/JAI del Consejo, de 22 de diciembre de 2003, relativa a la lucha contra la explotación sexual de los niños y la pornografía infantil.

Esta norma fue sustituida por la Directiva 2011/93/UE[6] de lucha contra el abuso sexual de menores, que modifica y amplía considerablemente las disposiciones de la Decisión marco. Uno de los aspectos más relevantes de la Directiva es la definición de qué conductas son constitutivas de delitos de abuso sexual de menores, a las que luego nos referiremos, pues es dicha conceptualización la que siguen las restantes normas en materia de lucha contra el abuso sexual de menores que han sido aprobadas en el seno de la UE. Además, no se limita únicamente a la descripción de las conductas delictivas, sino que va un paso más allá y establece las penas privativas de libertad que deberán imponerse como mínimo para cada una de las conductas. Junto con las disposiciones de carácter sustantivo, incorpora también disposiciones de naturaleza procesal, relativas a la competencia judicial, el apoyo y protección de las víctimas menores en los procesos penal y la investigación y enjuiciamiento, entre otras cuestiones.

Por todo ello, la Directiva constituye la principal norma de derecho comunitario en la materia, pues ha traído como consecuencia la armonización de los Códigos Penales de los Estados Miembros en materia de abuso sexual de menores. Es evidente que en una materia como la que estamos tratando en la cual el carácter transfronterizo es frecuente, es esencial contar con una legislación penal unificada que facilite la investigación y enjuiciamiento.

En el año 2020 se aprobó la Estrategia de la UE para una lucha más eficaz contra el abuso sexual de menores[7]. En ella se incide en que la lucha contra esta clase de delitos es prioritaria para la Unión, así como en el hecho de que "el mundo en conjunto está perdiendo la batalla contra estos delitos y no protege de manera efectiva el derecho de cada niño de vivir a salvo de la violencia". La Estrategia se basa en una serie de iniciativas para luchar contra el abuso sexual, que se concretan en las siguientes: garantizar la plena aplicación de la Directiva 2011/93/UE; garantizar que la legislación de la UE permita una respuesta eficaz; identificar lagunas jurídicas, mejores prácticas y acciones prioritarias; fortalecer los esfuerzos de las fuerzas y cuerpos de seguridad a escala nacional y de la UE; capacitar a los Estados miembros para proteger mejor a los menores a través de la prevención; crear un centro europeo de prevención y lucha contra el abuso sexual de menores; estimular los esfuerzos de las empresas del sector para garantizar la protección de los niños en sus productos; y, por último, mejorar la protección de los menores en el mundo mediante la cooperación multilateral. En definitiva, constituye un plan de acción para combatir la criminalidad sexual que involucra a menores de edad.

6 Directiva 2011/93/UE del Parlamento Europeo y del Consejo, de 13 de diciembre de 2011, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil y por la que se sustituye la Decisión marco 2004/68/JAI del Consejo.

7 Estrategia de la UE para una lucha más eficaz contra el abuso sexual de menores [COM(2020) 607 final], de 24 de julio de 2020.

Apenas un año después se aprobó la Estrategia de la UE sobre los Derechos de los Niños[8]. En el tercer pilar, centrado en "Combatir la violencia contra los niños y garantizar la protección de la infancia: una UE que ayude a los niños a crecer sin violencia", se incide sobre la violencia sexual, señalando que se complementarán y reforzarán las acciones previstas en la Estrategia de la UE para una lucha más eficaz contra el abuso sexual de menores.

En la misma línea, este mes de abril de 2024 se ha publicado la Recomendación de la Comisión Europea sobre el desarrollo y el refuerzo de los sistemas integrados de protección de la infancia que redunden en el interés superior del niño[9], en la cual se vuelve a poner de relieve la acción prioritaria de la UE en la lucha contra el abuso sexual de menores, tanto en línea como fuera de ella. En concreto, señala la necesidad de establecer medidas que permitan denunciar situaciones de inseguridad, recibir apoyo (psicológico y de otra clase) y recibir información sobre los riesgos relacionados con cualquier forma de violencia, incluida la violencia sexual.

Finalmente, como continuación de la labor legislativa en materia de lucha contra el abuso sexual de menores iniciada hace dos décadas, este mismo año 2024 se ha presentado una Propuesta de Directiva sobre la lucha contra los abusos sexuales y la explotación sexual de los menores y el material de abuso sexual de menores[10]. Como señala en su Exposición de Motivos, el texto nace con el objetivo de dar respuesta a las nuevas formas de criminalidad y de cubrir las lagunas detectadas en la Directiva del año 2011.

En este sentido, se señala la necesidad de garantizar que se tipifiquen como delito todas las formas de abuso y explotación de menores "incluidas aquellas que son posibles o se ven facilitadas por los avances tecnológicos" y, de igual forma, mejorar las normas de investigación y enjuiciamiento "teniendo en cuenta los últimos avances tecnológicos". Excedería el objeto del presente el análisis de las novedades que incorpora, pero sí que consideramos necesario destacar que, por primera vez, se quiere incluir en las conductas tipificadas la creación de material de abuso sexual de menores a través de las denominadas "ultrafalsificaciones" o "deep fakes"[11] e incluso la realidad virtual[12], así como el embaucamiento de menores

8 Estrategia de la UE sobre los Derechos de los Niños, COM(2021) 142 final, de 24 de marzo de 2021.

9 Recomendación de la Comisión de 23 de abril de 2024 sobre el desarrollo y el refuerzo de los sistemas integrados de protección de la infancia que redunden en el interés superior del niño, C(2024) 2680 final.

10 Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y el material de abuso sexual de menores y por la que se sustituye la Decisión marco 2004/68/JAI del Consejo (versión refundida) [COM(2024) 60 final].

11 Sobre esta nueva forma de criminalidad puede verse más: Simó Soler, E.: "Retos jurídicos derivados de la Inteligencia Artificial Generativa. Deepfakes y violencia contra las mujeres como supuesto de hecho", *Indret: Revista para el Análisis del Derecho*, 2024, núm. 2, pp. 493-515.

12 Señala el texto, en relación la modificación del artículo 2 de la Directiva 2011/93/UE que "El desarrollo de entornos de realidad aumentada, ampliada y virtual y la posibilidad de hacer un uso indebido de la

mediante "chatbots" desarrollados para tal fin. Por lo tanto, consideramos que se trata de una actualización necesaria, dado el vertiginoso desarrollo en materia de inteligencia artificial y otras herramientas tecnológicas desde la aprobación de la primera Directiva en el año 2011, que han dado lugar a nuevas formas de criminalidad que deben ser afrontadas adecuadamente.

A las normas antedichas debemos sumar las relativas específicamente a la detección de abusos sexuales de menores en línea, a las que nos referiremos en los apartados siguientes, en particular el Reglamento provisional y la propuesta de Reglamento que vendrá a sustituirlo en un futuro.

2. El Reglamento provisional (UE) 2021/1232.

Como se ha puesto de manifiesto, el abuso sexual de menores a través de internet no solo no se ha reducido, sino que año tras año los informes que publican distintas organizaciones revelan que estamos ante un fenómeno criminológico creciente. Las primeras actuaciones para tratar de detener la comisión de estos delitos fueron llevadas a cabo voluntariamente por los proveedores de servicios de internet, a través de sus propios mecanismos de control. El amparo legal lo encontraban en el Reglamento General de Protección de Datos[13], concretamente en su artículo 6, cuando dispone que el tratamiento será lícito si: "es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño".

Sin embargo, a partir del 21 de diciembre de 2020 dejaban de poder acogerse a dicho precepto para ser incluidos en el ámbito de aplicación de la Directiva 2002/58/CE sobre privacidad y comunicaciones electrónicas[14], en virtud del Código Europeo de las Comunicaciones Electrónicas, aprobado mediante la Directiva (UE) 2018/1972[15]. Por lo tanto, surgió la necesidad de establecer un marco jurídico para amparar dichas actuaciones que ya estaban llevando a cabo

inteligencia artificial para crear 'ultrafalsificaciones', es decir, material de abuso sexual de menores creado de forma sintética, ya han ampliado la definición de 'imagen', ya que dichos materiales pueden hacer uso de avatares, incluida la retroalimentación sensorial, por ejemplo, a través de dispositivos que proporcionan una percepción del tacto."

13 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

14 Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas).

15 Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2018, por la que se establece el Código Europeo de las Comunicaciones Electrónicas.

los proveedores de servicios de internet para luchar contra el abuso de menores. Para ello, el Parlamento Europeo aprobó el Reglamento (UE) 2021/1232 del Parlamento Europeo y del Consejo de 14 de julio de 2021[16] por el que se establece una excepción temporal a determinadas disposiciones de la Directiva 2002/58/CE y permite a los proveedores de servicios seguir aplicando la excepción del artículo 6 del Reglamento General de Protección de Datos y llevando a cabo actuaciones voluntarias para luchar contra el abuso de menores. Así pues, nació con vocación de provisionalidad, hasta en tanto se apruebe una norma definitiva.

La Directiva 2002/58/CE, cuyas disposiciones exceptúa la norma provisional, tiene por objeto velar por el adecuado tratamiento de los datos personales y el respeto de la intimidad de las personas en el ámbito concreto de las comunicaciones electrónicas. Para ello, se prevén en la misma una serie de garantías, traducidas en deberes para los prestadores de servicios y derechos para los individuales que, en síntesis, conllevan la prohibición de escucha, grabación, almacenamiento u otros tipos de intervención o vigilancia de las comunicaciones y los datos de tráfico asociados a ellas, conforme dispone su artículo 5. De igual forma, la norma prevé en su artículo 6 que los datos de tráfico vinculados a un usuario que sean tratados y almacenados deberán eliminarse o hacerse anónimos cuando ya no sea necesario a los efectos de la transmisión de una comunicación.

Sin embargo, dada la impunidad y clandestinidad que caracterizan a los delitos de abuso sexual de menores, y ante el vacío legal al que nos hemos referido, era necesario regular una serie de excepciones a esta garantía de intimidad cuando se basen en la lucha contra esta clase de criminalidad.

Para ello el Reglamento (UE) 2021/1232 exceptúa las garantías previstas en los citados artículos 5 y 6 de la Directiva 2002/58/CE, a las que nos hemos referido antes, y permite a los proveedores de servicios la utilización de "tecnologías específicas para el tratamiento de datos personales y de otro tipo en la medida estrictamente necesaria para detectar abusos sexuales de menores en línea cometidos en sus servicios y denunciarlos y para retirar el material de abuso sexual de menores en línea de sus servicios", conforme dispone en su artículo 1.

Ahora bien, la excepción solamente se aplicará bajo las siguientes circunstancias, conforme recoge su artículo 3:

- Respecto del tratamiento de los datos, debe ser necesario para detectar, retirar y denunciar el material de abuso de menores, así como el embaucamiento.

16 Reglamento (UE) 2021/1232 del Parlamento Europeo y del Consejo de 14 de julio de 2021 por el que se establece una excepción temporal a determinadas disposiciones de la Directiva 2002/58/CE en lo que respecta al uso de tecnologías por proveedores de servicios de comunicaciones interpersonales independientes de la numeración para el tratamiento de datos personales y de otro tipo con fines de lucha contra los abusos sexuales de menores en línea.

Además, debe ser proporcionado y limitado estrictamente a los datos de contenido y datos de tráfico conexos que sea necesario.

- En cuanto a las tecnologías empleadas, deben ser las menos intrusivas para la intimidad y limitarse a detectar patrones de comportamiento, pero no a deducir el contenido de las comunicaciones. Además, deben ser lo suficientemente fiables para reducir la tasa de errores en la detección de contenidos y rectificar las consecuencias de estos cuando se produzcan. Por último, deben limitarse al uso de indicadores fundamentales y factores objetivos de riesgo para detectar los patrones de abuso.

- Finalmente, los proveedores deben establecer mecanismos internos para prevenir cualquier acceso o transferencia no autorizado de datos personales, así como para supervisar el tratamiento de la información. Asimismo, deben poner a disposición de los usuarios mecanismos de reclamación adecuados para ser oídos ante actuaciones de los proveedores que afecten a su derecho a la privacidad.

Esta norma provisional entró en vigor en julio de 2021 y su vigencia finalizaba el 3 de agosto de 2024. Sin embargo, el pasado 29 de abril de 2024, el Parlamento Europeo aprobó su prórroga hasta el 3 de agosto de 2026[17], mientras sigan las negociaciones para la aprobación de un nuevo Reglamento que con carácter definitivo regule las medidas a adoptar en la lucha contra el abuso de menores en internet.

En particular, se trata de la Propuesta de Reglamento para prevenir y combatir el abuso sexual de los menores[18], presentada el 22 de mayo de 2022 y a la que nos referiremos seguidamente.

III. PROPUESTA DE REGLAMENTO PARA PREVENIR Y COMBATIR EL ABUSO SEXUAL DE LOS MENORES.

Como se ha adelantado, el Reglamento para prevenir y combatir el abuso sexual de menores en internet, sustituirá al Reglamento provisional cuando sea definitivamente aprobado. Sin embargo, la aprobación del texto definitivo no está siendo tan sencilla como sería lo deseable, dada la finalidad con la que nace el texto, sino que el borrador presentado ha suscitado controversia desde el principio por su injerencia en la intimidad de los usuarios de internet. Ello le ha valido

17 Reglamento (UE) 2024/1307 del Parlamento Europeo y del Consejo, de 29 de abril de 2024, por el que se modifica el Reglamento (UE) 2021/1232 por el que se establece una excepción temporal a determinadas disposiciones de la Directiva 2002/58/CE en lo que respecta al uso de tecnologías por proveedores de servicios de comunicaciones interpersonales independientes de la numeración para el tratamiento de datos personales y de otro tipo con fines de lucha contra los abusos sexuales de menores en línea.

18 Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas para prevenir y combatir el abuso sexual de los menores COM/2022/209 final.

el sobrenombre de "chat control", pues, como posteriormente expondremos, desde algunos sectores se ha criticado que las medidas que establece podrían estar menoscabando la intimidad de las personas y dando lugar a un escaneo generalizado de las conversaciones de todos los usuarios de la Unión Europea.

Pasaremos a continuación a examinar algunas de sus principales características y medidas que impone.

1. Ámbito de aplicación de la norma.

El objeto de la Propuesta de Reglamento es, como hemos adelantado, luchar contra el abuso sexual de menores en internet, pero conviene precisar qué conductas se entienden incluidas dentro de dicho concepto. Para ello, debemos acudir al artículo 2 de definiciones en el cual se incluye dentro del concepto de "abuso sexual de menores en línea", tanto la difusión de material de abuso sexual, como el embaucamiento de menores. Para una definición más amplia de tales conceptos el texto remite a la Directiva 2011/93/UE, a la que antes nos hemos referido, y que contiene una detallada definición de tales conductas. Todo ello sin perjuicio de la conceptualización que se ha ofrecido en el apartado primero del presente trabajo.

Así pues, siguiendo lo dispuesto en el artículo 2 de la citada Directiva, apartados c) y e), se entiende incluido en el concepto "material de abuso sexual", cualquier representación visual de un menor participando en una conducta sexual (sea real o simulada), así como de sus órganos sexuales, incluso cuando la persona involucrada en la conducta no sea menor de edad, pero parezca serlo. Y ello con independencia de que sea material creado y difundido posteriormente o se trate de una exhibición en directo, a través de las tecnologías de la comunicación y de la información.

Respecto de lo antedicho, destaca el hecho de que la conducta también se califique como material de abuso sexual de menores cuando represente a "una persona que parezca ser un menor". Es decir, con esta disposición no se está protegiendo la libertad e indemnidad sexuales de un menor de edad que haya sido obligado de cualquier modo a participar en la actividad sexual, sino que se castiga la mera representación de un menor de edad. En este sentido, podría decirse que se sanciona el deseo de obtener satisfacción sexual con la idealización de menores de edad[19], aun cuando ningún menor haya participado realmente.

19 Fernández Teruelo, J.G.: "Concepto de pornografía infantil y modalidades típicas comisivas tras la reforma del Código Penal operada por la Ley Orgánica 1/2015 de 30 de marzo: la pornografía infantil y la que no lo es (aunque se tipifique como tal)", en AA.VV.: *Menores y redes sociales. Ciberbullying, ciberstalking, cibergrooming, pornografía, sexting, radicalización y otras formas de violencia* (dir. por M.L. Cuerda Arnau y coord. por A. Fernández Hernández), Tirant lo Blanch, Valencia, 2016, p. 177.

Por lo que respecta a la conducta de embaucamiento de menores o "child grooming", el artículo 6 de la Directiva lo define como "La propuesta por parte de un adulto, por medio de las tecnologías de la información y la comunicación, de encontrarse con un menor que no ha alcanzado la edad de consentimiento sexual, con el fin de cometer una infracción contemplada en el artículo 3, apartado 4, y en el artículo 5, apartado 6, cuando tal propuesta haya ido acompañada de actos materiales encaminados al encuentro". En particular, el objetivo debe ser llevar a cabo un acto sexual o producir material de abuso sexual de menores, por remisión del artículo 6 a los artículos 3 y 5 de la misma norma.

Como característica común a la regulación europea, debe indicarse que no se exige en ningún caso la presencia de violencia o intimidación, sino que el abuso sexual de menores (en este caso a través de internet) se entenderá cometido siempre que afecte a un menor que no haya alcanzado la edad de consentimiento sexual[20].

Por lo tanto, estas dos formas delictivas, la creación de material y la captación de menores, con sus múltiples variantes, son contra las que se quiere reforzar la protección y para cuya investigación se regulan las medidas que posteriormente se expondrán.

2. Centro de la Unión Europea sobre Abuso Sexual de Menores y autoridades nacionales de coordinación.

La Propuesta de Reglamento contiene una importante novedad y es la creación del Centro de la Unión Europea para prevenir y combatir el abuso sexual de menores (en adelante, Centro de la UE), creado con el encargo de velar por la aplicación de las disposiciones de la norma relativas a la detección, denuncia, eliminación del contenido de abuso sexual y recopilación de información, entre otras. Ello en consonancia con lo manifestado en la Estrategia de la UE para una lucha más eficaz contra el abuso sexual de menores. Su creación se prevé en el artículo 40 de la Propuesta, con la finalidad de contribuir a la consecución del objetivo de la norma. Por lo que respecta a la naturaleza jurídica del Centro de la UE, se constituye como un organismo de la Unión Europea con personalidad jurídica y se prevé que su sede se establecerá en La Haya.

Por lo que respecta a sus funciones, pueden concretarse en las siguientes, desarrolladas ampliamente en el artículo 43 de la Propuesta:

- Apoyar y facilitar la aplicación de sus disposiciones relativas a la detección, la denuncia, la eliminación del contenido de abuso sexual de menores en línea, la inhabilitación del acceso a él y su bloqueo.

20 Tapia Ballesteros, P.: "Estrategia de la UE para una lucha más eficaz contra el abuso sexual de menores", *Revista de Estudios Europeos*, 2013, núm. 1, p. 437.

- Recopilar y compartir información y conocimientos especializados.

- Facilitar la cooperación entre las partes públicas y privadas.

Además de las funciones antedichas, el Centro de la UE será el encargado de crear, mantener y gestionar una base de datos de indicadores y otra de denuncias. La primera de ellas, prevista en el artículo 44, tiene por objeto la recogida de identificadores digitales que permitan detectar la difusión de material de abuso sexual infantil nuevo o ya conocido, así como detectar conductas de embaucamiento de menores. La segunda de las bases, como su nombre sugiere, se destinará a la recogida de todas las denuncias que se reciban de los prestadores de servicios, así como de ciertos datos relacionados relativos a su tramitación anterior y posterior, e información sobre la actuación del prestador de servicios en cuanto a la eliminación y bloqueo de la información. Finalmente, incluirá también los indicadores y etiquetas que estén asociadas al material detectado.

Además, debe destacarse que el Centro de la UE colaborará directamente con Europol en la persecución de esta clase de criminalidad. En particular, dicha colaboración lo será mediante la recepción de las denuncias de los proveedores de servicios, su verificación para evitar denuncias improcedentes y se remisión a Europol y a las autoridades nacionales competentes para la investigación.

Junto al Centro de la UE, otro de los actores principales en materia de lucha contra el abuso de menores en internet, lo serán las autoridades nacionales de coordinación. Conforme dispone el artículo 25 de la Propuesta se designará en cada Estado Miembro una autoridad nacional de coordinación en materia de abuso sexual de menores (en adelante, autoridad de coordinación). Esta autoridad es competente sobre todas las materias relacionadas con la aplicación y ejecución del Reglamento.

Por lo que respecta a los requisitos para su designación, el artículo 26 de la Propuesta indica que debe tratarse de entidades públicas jurídica y funcionalmente independientes, deben gozar de un estatuto propio que les permita actuar con objetividad e imparcialidad, deben estar libres de cualquier influencia externa -directa o indirecta-, no deben solicitar ni aceptar instrucciones de otras autoridades públicas o privadas y no deben encargarse de otras tareas en el ámbito de la lucha contra el abuso sexual de menores distintas de las encomendadas en virtud del Reglamento.

Finalmente, en cuanto a las competencias que tienen atribuidas, se pueden clasificar en investigación, ejecución, verificación del cumplimiento de las obligaciones impuestas por el Reglamento por los prestadores de servicios y notificación de material conocido de abuso sexual de menores. En particular,

respecto de la investigación, se les atribuye la competencia para exigir a los prestadores de servicios y cualquier otra persona relacionada que les preste información en relación con presuntas infracciones, así como para inspeccionar sobre el terreno cualquier instalación que se utilice para la prestación del servicio o solicitar a otras autoridades que lleven a cabo tal inspección e incluso la obtención de información. Cabe suponer que siempre que las actuaciones de investigación puedan conllevar alguna clase de injerencia en los derechos de las partes afectadas, podrán solicitar a la autoridad judicial competente una orden pertinente para su ejecución. Es también destacable que se les atribuye competencia para la imposición de sanciones administrativas ante el incumplimiento por parte de los prestadores de las obligaciones adquiridas en virtud de la norma.

A tenor de lo expuesto, queda patente que las autoridades de coordinación gozan de un papel esencial en la aplicación y ejecución de las disposiciones del Reglamento, tanto en lo que respecta a las propias funciones que tienen atribuidas, como en la medida en que actuarán como interlocutoras entre las autoridades nacionales judiciales o administrativas que tengan competencias para emitir las órdenes de eliminación, bloqueo o detección, así como con el Centro de la UE y las fuerzas y cuerpos de seguridad del Estado Miembro competente para la investigación.

3. Obligaciones para los proveedores de servicios.

La esencia de la Propuesta de Reglamento reside en el establecimiento de una serie de deberes para los proveedores de servicios de datos y comunicaciones, que se clasifican en obligaciones de evaluación de riesgos, detección, información y eliminación y bloqueo. Dentro de estas, las de detección son las que mayores dudas han planteado desde el punto de vista de los derechos y que han convertido a este texto en una de las normas más polémicas de los últimos años. Por dicho motivo, las desarrollaremos posteriormente.

En primer lugar, conforme dispone el artículo 3 de la Propuesta, los prestadores de servicios deberán determinar, analizar y evaluar para cada servicio que ofrezcan, el riesgo que existe de que el mismo sea utilizado con fines de abuso sexual de menores. En concreto, se establecen como criterios para la evaluación del riesgo los siguientes: casos previos detectados, la política ya establecida por el prestador y su aplicación, la forma en que los usuarios utilizan el servicio, así como el diseño y forma de explotación del mismo. Respecto del embaucamiento de menores, se tendrá en cuenta la edad de los usuarios y si existen funcionalidades que pueden reforzar el riesgo (entre otras: que se permita buscar a otros usuarios, que se permita el contacto a través de comunicaciones directas privadas y que se permita compartir imágenes y vídeos de forma privada).

Además, en función del riesgo que se haya determinado, los prestadores de servicios deberán adoptar las medidas pertinentes para reducirlo. En particular, dispone el artículo 4 de la Propuesta que deberán incluir, al menos, una de las acciones siguientes: adaptar los sistemas de moderación de contenidos o de recomendación, sus funcionalidades o la aplicación de sus condiciones, entre otras; reforzar los procesos y la supervisión interna; y, finalmente, cooperar con otros prestadores de servicios, así como con otras instituciones públicas y privadas.

Estas medidas de mitigación del riesgo deberán ser eficaces, específicas, proporcionadas y no discriminatorias. Además, serán susceptibles de introducirse, revisarse, suspenderse o ampliarse, según proceda, cada vez que se lleve a cabo una nueva evaluación de riesgos.

En segundo lugar, los artículos 7 a 11 de la Propuesta se refieren las obligaciones de detección. A grandes rasgos, estas imponen sobre los prestadores de servicios el deber de ejecutar las actuaciones necesarias para detectar las conductas de abuso sexual de menores, tanto de material de abuso como de embaucamiento, bajo determinadas circunstancias, con la finalidad de su denuncia, eliminación y bloqueo. Como ya hemos adelantado, nos limitaremos aquí a mencionar las obligaciones de detección, en tanto que serán objeto del siguiente apartado, dada su relevancia.

En tercer lugar, las obligaciones relativas a la información se concretan en los artículos 12 y 13 de la Propuestas y consisten en el deber de denunciar que pesa sobre los prestadores de servicios siempre que tengan conocimiento de cualquier indicio que indique un posible abuso sexual de menores a través de sus servicios. La denuncia se presentará ante el Centro de la UE y deberán contener cuantos datos sean necesarios para identificar al usuario o usuarios implicados, su ubicación geográfica, la dirección IP, así como acompañarla de todos los datos de contenido de los que se disponga. Cabe señalar que el usuario afectado será informado sobre la presentación de la denuncia, el contenido principal, el modo en que se ha obtenido y las posibilidades de alegación que tiene frente a la denuncia presentada en su contra.

Finalmente, dentro de las obligaciones de información, cabe destacar la creación y gestión de un mecanismo accesible y de fácil uso que permita a los usuarios informar al prestador de posibles abusos sexuales de menores.

En cuarto y último lugar, la Propuesta contempla la obligación de eliminar y bloquear los contenidos de abuso sexual de menores.

Por un lado, en cuanto a la eliminación de contenidos (artículos 14 y 15), la Propuesta regula las denominadas "órdenes de eliminación", que deberá ejecutar el

prestador de servicios cuando se haya identificado y confirmado que determinado contenido constituye material de abuso sexual de menores. Las órdenes serán emitidas por una autoridad judicial a petición de la autoridad de coordinación y contendrán un requerimiento a un prestador de servicios de alojamiento de datos para que elimine el material ilícito. Lo más destacable es que la eliminación se llevará a cabo en todos los Estados miembros de la UE y deberá ser ejecutada por el prestador de servicios en el plazo máximo de 24 horas desde la recepción de la orden.

Cabe señalar que el artículo 15 prevé la necesidad de informar al usuario afectado de la eliminación del contenido y garantizar que tenga acceso a un recurso efectivo para impugnar la orden de eliminación ante las autoridades judiciales o administrativas que sean competentes para conocer de la impugnación, según el órgano que haya dictado la orden. Transcurrido el plazo para presentar recurso (de conformidad con el derecho nacional) o una vez confirmada una orden de eliminación tras un recurso, se procederá a la eliminación definitiva de los contenidos afectados por la orden.

Por otro lado, se regulan las "órdenes de bloqueo". Sobre este respecto, dispone el artículo 16 de la Propuesta que tendrán por objeto exigir a un prestador de servicios la adopción de medidas para impedir el acceso a material conocido de abuso sexual de menores. Igual que en el caso de la eliminación, la orden deberá ser solicitada por la autoridad nacional de coordinación a la autoridad nacional judicial o administrativa competente para la emisión de la orden.

Una vez hechas las comprobaciones oportunas por parte de la autoridad de coordinación y solicitada la emisión de la misma a la autoridad competente, se acordará siempre que concurran las siguientes condiciones: a) haya pruebas de que el servicio se ha utilizado en los últimos 12 meses para acceder o intentar acceder a material conocido de abuso de menores; b) la orden sea necesaria para impedir la difusión de material ilícito a los usuarios de la UE, considerando la cantidad y calidad de dicho material; c) los indicadores señalen de manera suficientemente fiable que se trata de material de abuso sexual de menores; d) los motivos para emitir la orden compensen las consecuencias negativas en los derechos e intereses de las partes.

Finalmente, como garantía ante el bloqueo de contenidos, la autoridad que las emita deberá especificar los límites y salvaguardias efectivos y proporcionados para minimizar las consecuencias negativas en los derechos e intereses, así como asegurar que el periodo de aplicación se limite al necesario. El periodo de vigencia se establecerá por la autoridad de coordinación y no podrá exceder de cinco años.

4. La polémica en torno a las medidas de detección.

Tras exponer sucintamente en qué consisten las obligaciones de evaluación y mitigación de riesgos, información y eliminación y bloqueo de contenidos, pasaremos a continuación a abordar en mayor profundidad las obligaciones de detección, en la medida en que constituyen uno de los pilares esenciales en la lucha contra el abuso de menores en la Propuesta. Sin embargo, como ya hemos adelantado, el deber de detección ha suscitado dudas desde la publicación del primer texto de la Propuesta y desde organismos públicos y privados se ha puesto de manifiesto la necesidad de retirar o, al menos, modificar, la forma en que se había configurado inicialmente.

Analizaremos a continuación sus elementos y los aspectos más controvertidos de la regulación que se propone.

A) Solicitud de la orden de detección.

El procedimiento de detección comienza con la emisión de una orden de detección por la autoridad judicial o administrativa nacional competente, a solicitud de la autoridad nacional de coordinación, como en el caso de las órdenes de eliminación y bloqueo.

Como dispone el artículo 7 de la Propuesta, con carácter preliminar, la autoridad de coordinación deberá elaborar el proyecto de solicitud de emisión de la orden con el contenido de la misma y los motivos que la fundamentan, que deberá presentar al prestador de servicios, así como al Centro de la UE. A la vista del proyecto, el prestador de servicios podrá presentar observaciones y el Centro de la UE emitirá un dictamen sobre el mismo. Una vez recibidas las observaciones y el dictamen, del prestador y del Centro de la UE, respectivamente, la autoridad de coordinación presentará un nuevo proyecto modificado. Finalmente, considerando el segundo proyecto de la autoridad de coordinación, el prestador de servicios presentará su plan de ejecución de la orden. Una vez recibido el plan de ejecución, procederá la autoridad de coordinación a solicitar la emisión de la orden, acompañando, en su caso, el dictamen del Centro de la UE y el plan de ejecución.

B) Requisitos para su adopción.

Según regula el artículo 7 de la Propuesta, los requisitos para la solicitud y emisión de la orden son, en primer lugar, que exista un riesgo significativo de que el servicio se está utilizando para abuso sexual de menores y, en segundo lugar, que la medida de detección sea proporcionada, en el sentido de que los motivos para emitir la orden compensen los efectos negativos sobre los derechos de las

partes implicadas. Estos elementos serán los que la autoridad de coordinación deberá tener en cuenta para decidir solicitar la orden y, asimismo, son los que valorará la autoridad judicial o administrativa competente para su emisión.

Respecto de las situaciones en que habrá riesgo significativo, quedan definidas en el mismo artículo, en los apartados 5, 6 y 7 del mismo artículo, en función de si se trata de difusión de material ya conocido o de nuevo material, o, en el tercer caso, de embaucamiento de menores. En concreto, señala el precepto lo siguiente:

- Primero, en cuanto a la difusión de material conocido de abuso sexual de menores, habrá riesgo significativo cuando sea probable que el servicio se utilice con dicho fin, a pesar de las medidas de mitigación del riesgo y, además, haya pruebas de que se haya utilizado con dicha finalidad en los últimos doce meses y en una medida apreciable.

- Segundo, respecto de la difusión de nuevo material de abuso sexual de menores, se valorarán las mismas circunstancias que en el caso anterior, con la circunstancia añadida de que el prestador haya presentado un número significativo de denuncias relativas a dicho material ilícito.

- Tercero, en cuanto al embaucamiento de menores, las circunstancias de las que se desprenderá la existencia de riesgo significativo son que se trate de un servicio de comunicaciones interpersonales y, además, igual que en los casos anteriores, que sea probable que el servicio se utilice con dicho fin y así haya sido en los últimos doce meses. En todo caso, las órdenes de detección relativas al embaucamiento de menores solamente se podrán aplicar cuando uno de los usuarios implicados sea un menor.

A la vista de lo antedicho, consideramos que el concepto de "riesgo significativo" no está adecuadamente definido, pues se utilizan en el texto expresiones como "que sea probable" que el servicio se utilice con fines ilícitos o que se haya utilizado "en una medida apreciable". Por ello, entendemos que esto podría conducir a una situación de inseguridad jurídica y a una posible aplicación diferenciada y arbitraria según cada autoridad nacional de coordinación e incluso cada juzgado dentro del mismo Estado Miembro. Máxime si consideramos que dichos elementos serán valorados, en primer lugar, por la autoridad de coordinación, y, en segundo lugar, por la autoridad judicial o administrativa competente a la hora de decidir sobre la emisión de la orden. Por ello, entendemos que podría ponerse en riesgo el derecho de defensa y el derecho a una resolución judicial motivada, al no poder conocer exactamente a qué hacen referencia dichos términos que sirven de parámetros para decidir o no la interceptación de las comunicaciones.

Cabe señalar que la Propuesta contempla en su artículo 9 que la orden debe poder ser recurrida ante la autoridad judicial o administrativa competente, tanto por el proveedor de servicios como por el usuario afectado. Sin embargo, respecto de este último, como es lógico, también se prevé que no se le notifique la orden cuando pueda frustrar su finalidad.

En concreto, el artículo 10 prevé dicha excepción de información en dos situaciones. Primero, respecto de la información general ofrecida a los usuarios del servicio de que se están empleando tecnologías para ejecutar una orden de detección, de que debe denunciar cualquier posible abuso sexual de menores y del derecho al recurso de los usuarios afectados. Y, segundo, en relación con los usuarios directamente afectados. En particular, señala el texto que se informará a los usuarios tras formular denuncia ante Europol o las autoridades nacionales y recibir la confirmación de que la información no interferirá en las actividades de "prevención, detección, investigación y enjuiciamiento de delitos de abuso sexual de menores". Por ello, debemos entender que lo habitual será que la notificación no se produzca con carácter previo, sino, en todo caso, una vez ejecutada la orden y asegurado el buen fin de la investigación.

C) Procedimiento de detección.

Respecto a la forma de ejecutar la detección de conductas ilícitas, el artículo 10 de la Propuesta regula una serie de garantías que deben regir respecto de las tecnologías a emplear.

En primer lugar, en relación con las herramientas que se utilizarán, se prevé que el Centro de la UE ponga a disposición de los prestadores de servicios tecnologías específicas que podrán adquirir, instalar y explotar gratuitamente (artículo 50). No obstante, los prestadores no están en ningún caso obligados a utilizar dichas tecnologías, sino que podrán emplear cualesquiera otras, siempre que cumplan los requisitos previstos en dicho artículo.

Por lo que respecta a las condiciones que las tecnologías deben cumplir, señala el artículo 10, apartado 3, de la Propuesta que las tecnologías deben ser: eficaces para detectar la difusión de material ilícito o el embaucamiento de menores, lo suficientemente fiables para reducir los errores en la detección, que no puedan extraer de las comunicaciones ninguna otra información que no sea la estrictamente necesaria para detectar la conducta de abuso sexual y, finalmente, que sean lo menos intrusivas posibles en términos de derechos a la vida privada, el secreto de las comunicaciones y los datos personales.

En relación con esto último, debe señalarse que la proporcionalidad de la medida de detección podría verse en riesgo, tanto por el componente tecnológico

inherente a la misma, como por la precisión de los indicadores que se emplearán para la detección de las conductas de embaucamiento de menores[21]. Asimismo, es criticable que no se establezcan mayores garantías o requisitos en cuanto a la fiabilidad, lo que podría hacerse estableciendo en la norma un grado de éxito cuantificable necesario, así como regulando la necesidad de que exista una evaluación independiente de un tercero o del propio Centro de la UE[22].

Además de lo antedicho, el texto prevé una serie de actuaciones adicionales que deberá llevar a cabo el prestador del servicio. En particular, debe adoptar todas las medidas posibles para garantizar que las tecnologías empleadas y el tratamiento de datos lo sean con el único fin de detectar las conductas de abusos sexual de menores. Además, debe establecer procedimientos internos para prevenir y remediar cualquier uso indebido de las herramientas y de los datos personales obtenidos a través de las mismas, así como implantar mecanismos de supervisión humana para detectar posibles errores. De igual forma, deberá establecer mecanismos accesibles de reclamaciones para los usuarios. Y, en último lugar, debe informar a la autoridad nacional de coordinación de la aplicación de las medidas de la orden de detección. Como garantía adicional a todo ello, deberá periódicamente revisar el funcionamiento de las medidas anteriores y revisarlas cuando sea necesario.

En cualquier caso, el proceso de detección será más intrusivo cuando se trate de captación de menores porque lo que se analiza es directamente el contenido de las comunicaciones personales, aun cuando según el texto, solo se deben escanear aquellas en las que haya un menor implicado.

Sobre el análisis de las comunicaciones, fue muy crítico el informe conjunto sobre la Propuesta de Reglamento elaborado por el Comité Europeo de Protección de Datos y el Supervisor Europeo de Protección de Datos en el año 2022[23]. En dicho documento se afirma que las tecnologías actualmente disponibles se basan en el tratamiento automatizado de datos de contenido de todos los usuarios. A ello su suma que la Propuesta permite aplicar la medida a todo un servicio (no a una comunicación concreta) y por plazos de hasta 24 meses en el caso de material de abuso sexual y 12 meses en el caso de embaucamiento. Por estos motivos, el informe referido pone de relieve que la medida detección podría convertirse

21 Fiodorova, A.: "La lucha contra abusos de menores en línea: hacía una nueva regulación", *Revista de Estudios Europeos*, 2023, núm. 1, p. 469.

22 Montoro Sánchez, J.A.: "Análisis crítico de la Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas para prevenir y combatir el abuso sexual de los menores", *Revista de la Asociación de Profesores de Derecho Procesal de las universidades españolas*, 2023, núm. 8, p. 94.

23 Comité Europeo de Protección de Datos y Supervisor Europeo de Protección de Datos, Dictamen conjunto 4/2022 sobre la Propuesta de Reglamento del Parlamento Europeo y el Consejo por el que se establecen normas para prevenir y combatir el abuso sexual de los menores, adoptado el 28 de julio de 2022. Documento disponible en: https://www.edpb.europa.eu/system/files/2023-02/edpb_edps_jointopinion_202204_csam_es.pdf

en "un escaneo generalizado e indiscriminado del contenido de prácticamente cualquier comunicación electrónica de todos los usuarios de la Unión". Por ello, concluyen las autoridades europeas en materia de protección de datos que el sistema de detección plantea serias dudas desde el punto de vista de la protección de datos, la vida privada, la necesidad y proporcionalidad de las medidas.

Asimismo, se critica también que las garantías a adoptar desde el punto de vista del procedimiento para la ejecución de la orden de detección residen principalmente en la actuación del prestador de servicios y no en las autoridades. Y es que, conforme hemos expuesto, estos tendrán libertad para elegir qué tecnologías emplean. Además, es en ellos donde recae la adopción de las medidas de garantía, aun cuando el texto de la Propuesta establezca qué condiciones deben cumplir y se prevea asimismo la presentación de un plan de ejecución, tal y como hemos referido anteriormente. En todo caso, dadas las circunstancias y, especialmente, la injerencia en los derechos de las personas, consideramos que sería deseable que la redacción definitiva otorgase mayores facultades de control efectivo a la hora de la ejecución de las órdenes de detección.

En el mismo sentido crítico, en julio de 2023 se presentó una carta firmada por más de 300 académicos de todo el mundo solicitando al Parlamento y al Consejo que diesen marcha atrás en la Propuesta del Reglamento conforme estaba planteado, pues reiteran que la tecnología actual o de previsible desarrollo a medio plazo no permite una detección con garantías[24]. Lo que señala este documento es que las herramientas de inteligencia artificial con la que contamos en la actualidad, aun cuando pueden ser entrenadas para detectar patrones, cometen errores continuamente, máxime cuando se trata de detectar delitos como el "child grooming", pues, dice el documento, "carecen del contexto y el sentido común de los seres humanos". Por ello, proponen que los recursos que se necesitarían para revisar todos los falsos positivos se empleen en desarrollar otras estrategias para proteger a los menores.

Junto a estas no han sido pocas las voces que se han alzado en contra de la Propuesta de Reglamento con base en argumentos similares a los que se acaban de exponer, lo que revela, como decíamos al inicio, que ha causado una enorme controversia desde su presentación y cabe esperar que las negociaciones no sean pacíficas. No obstante, a la vista de su desarrollo legislativo, parece que algunas de las objeciones planteadas al texto desde distintos sectores podrían ser acogidas. En este sentido, el Parlamento Europeo dio el primer paso al rechazar, en su informe de noviembre de 2023 sobre la Propuesta, que se pueda producir un escaneo generalizado y propone que las órdenes de detección tengan un

24 Joint statement of scientists and researchers on EU's proposed Child Sexual Abuse Regulation: 4 July 2023. Disponible en: https://edri.org/wp-content/uploads/2023/07/Open-Letter-CSA-Scientific-community.pdf

carácter fundamentalmente subsidiario, cuando todos los demás mecanismos de prevención hayan fallado[25]. En consecuencia, deberemos estar atentos a la tramitación en el Parlamento Europeo y a las negociaciones sobre la norma definitiva que presumiblemente se vayan a producir en los próximos meses.

IV. CONCLUSIONES.

Haciendo nuestras las palabras contenidas en la Estrategia de la UE para una lucha más eficaz contra el abuso sexual de menores, se puede afirmar rotundamente que estamos perdiendo la batalla contra el abuso sexual de menores y no estamos protegiendo de manera efectiva el derecho de los menores a vivir libres de violencia. Por ello, como afirmábamos al inicio del presente, deben necesariamente buscarse nuevas formas de prevención y lucha contra esta clase de conductas, pues lejos de ver reducidos sus números, aumentan alarmantemente año tras año.

En la Unión Europea ha habido en las últimas décadas un importante desarrollo legislativo para luchar contra el abuso sexual de menores, en general, y contra el abuso cometido a través de internet y las nuevas tecnologías, en especial. Tanto es así que actualmente existen dos importantes normas en tramitación: la Propuesta de Directiva sobre la lucha contra los abusos sexuales y la explotación sexual de los menores y el material de abuso sexual de menores del año 2024 y la Propuesta de Reglamento para prevenir y combatir el abuso sexual de menores del año 2022. Ambos textos tienen el mismo objetivo: fortalecer y actualizar las medidas para luchar contra dichas conductas, especialmente teniendo en cuenta el desarrollo tecnológico y las nuevas formas de criminalidad que ha propiciado.

Sin embargo, no está siendo cuestión pacífica, pues cuando se trata de investigar estos delitos cometidos a través de internet, bien sea mediante foros, herramientas de mensajería, redes sociales o en cualquier otro sistema, entran en juego derechos fundamentales tan esenciales como la privacidad, la protección de datos personales y la intimidad personal y familiar. Son precisamente estos riesgos los que han convertido a la Propuesta de Reglamento en uno de los textos más polémicos y criticados de los últimos años.

Es evidente que no estamos ante un asunto sencillo, pues se trata de poner en una balanza el derecho de los usuarios a la privacidad de sus comunicaciones electrónicas frente a la lucha contra una de las formas de criminalidad más reprochables que existen, el abuso sexual de menores. No obstante, sí que entendemos que la regulación propuesta presenta algunas áreas de mejora, fundamentalmente en lo relativo a las medidas de detección que tan censuradas han sido desde distintos

25 Report on the proposal for a regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, 16.11.2023 - (COM(2022)0209).

sectores. Para ello sería conveniente, entre otras cuestiones, que se definiese con mayor claridad en qué supuestos podrá acordarse la orden de detección y, asimismo, se concrete qué tecnologías se usarán y cómo se podrá garantizar por las autoridades (y no por los prestadores de servicios) que se respetan los derechos fundamentales de las personas. Además, como el Parlamento Europeo ha puesto de manifiesto, la detección debe ser absolutamente residual cuando todo lo demás haya fallado. En definitiva, el principio de proporcionalidad exigible a cualquier injerencia en los derechos fundamentales debe ser rigurosamente respetado.

Por todo ello, el próximo paso en las negociaciones de la norma residirá en hallar el necesario equilibrio entre la protección del interés superior del menor y el respeto de los derechos de las personas, pues si en algo existe consenso mundial es en la necesidad de mejorar la protección ofrecida a los menores y luchar eficazmente contra tan reprensibles conductas.

BIBLIOGRAFÍA

FERNÁNDEZ TERUELO, J.G.: "Concepto de pornografía infantil y modalidades típicas comisivas tras la reforma del Código Penal operada por la Ley Orgánica 1/2015 de 30 de marzo: la pornografía infantil y la que no lo es (aunque se tipifique como tal)", en AA.VV.: *Menores y redes sociales. Ciberbullying, ciberstalking, cibergrooming, pornografía, sexting, radicalización y otras formas de violencia* (dir. por M.L. CUERDA ARNAU y coord. por A. FERNÁNDEZ HERNÁNDEZ), Tirant lo Blanch, Valencia, 2016.

FIODOROVA, A.: "La lucha contra abusos de menores en línea: hacía una nueva regulación", *Revista de Estudios Europeos*, 2023, núm. 1.

GÓRRIZ ROYO, E.: "On-line child grooming en Derecho penal español", *Indret: Revista para el Análisis del Derecho*, 2016, núm. 3.

MONTORO SÁNCHEZ, J.A.: "Análisis crítico de la Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas para prevenir y combatir el abuso sexual de los menores", *Revista de la Asociación de Profesores de Derecho Procesal de las universidades españolas*, 2023, núm. 8.

SIMÓ SOLER, E.: "Retos jurídicos derivados de la Inteligencia Artificial Generativa. Deepfakes y violencia contra las mujeres como supuesto de hecho", *Indret: Revista para el Análisis del Derecho*, 2024, núm. 2.

TAPIA BALLESTEROS, P.: "Estrategia de la UE para una lucha más eficaz contra el abuso sexual de menores", *Revista de Estudios Europeos*, 2013, núm. 1.

VILLACAMPA ESTIARTE, C.: "Predadores sexuales online y menores: grooming y sexting en adolescentes", *Revista electrónica de Ciencias Criminológicas*, 2017, núm. 2.

LEGISLACIÓN

Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas).

Decisión marco 2004/68/JAI del Consejo, de 22 de diciembre de 2003, relativa a la lucha contra la explotación sexual de los niños y la pornografía infantil.

Directiva 2011/93/UE del Parlamento Europeo y del Consejo, de 13 de diciembre de 2011, relativa a la lucha contra los abusos sexuales y la explotación

sexual de los menores y la pornografía infantil y por la que se sustituye la Decisión marco 2004/68/JAI del Consejo.

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2018, por la que se establece el Código Europeo de las Comunicaciones Electrónicas.

Reglamento (UE) 2021/1232 del Parlamento Europeo y del Consejo de 14 de julio de 2021 por el que se establece una excepción temporal a determinadas disposiciones de la Directiva 2002/58/CE en lo que respecta al uso de tecnologías por proveedores de servicios de comunicaciones interpersonales independientes de la numeración para el tratamiento de datos personales y de otro tipo con fines de lucha contra los abusos sexuales de menores en línea.

Reglamento (UE) 2024/1307 del Parlamento Europeo y del Consejo, de 29 de abril de 2024, por el que se modifica el Reglamento (UE) 2021/1232 por el que se establece una excepción temporal a determinadas disposiciones de la Directiva 2002/58/CE en lo que respecta al uso de tecnologías por proveedores de servicios de comunicaciones interpersonales independientes de la numeración para el tratamiento de datos personales y de otro tipo con fines de lucha contra los abusos sexuales de menores en línea.

Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas para prevenir y combatir el abuso sexual de los menores COM/2022/209 final.

Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y el material de abuso sexual de menores y por la que se sustituye la Decisión marco 2004/68/JAI del Consejo (versión refundida) [COM(2024) 60 final].

LA RESPUESTA JAPONESA A LA DIGITALIZACIÓN DE LA JUSTICIA - ENMIENDA DE LA LEY DE ENJUICIAMIENTO CIVIL EN MAYO DE 2022*

THE JAPANESE RESPONSE TO DIGITALIZATION OF JUSTICE - AMENDMENT OF CIVIL PROCEDURE CODE IN MAY 2022

Actualidad Jurídica Iberoamericana Nº 21, agosto 2024, ISSN: 2386-4567, pp. 130-147

* Estudio redactado en el marco del Proyecto "Claves para una justicia digital y algorítmica con perspectiva de género", PID2021-123170OB-I00 financiado por MCIN/ AEI/10.13039/501100011033.

Takuya HATTA

ARTÍCULO RECIBIDO: 29 de mayo de 2023
ARTÍCULO APROBADO: 1 de julio de 2024

RESUMEN: Durante mucho tiempo, Japón ha sido un país atrasado en la digitalización de su sistema judicial. Pero finalmente dio un paso importante hacia la digitalización de la justicia mediante la modificación de la Ley de Enjuiciamiento Civil en mayo de 2022. La aplicación completa de la enmienda aún está por llegar, pero es seguro que llegará en un futuro cercano. Este artículo tiene como objetivo trazar la historia de la enmienda, explicar el contenido general de la misma y hacer algunos análisis.

PALABRAS CLAVE: Digitalización de la justicia; proceso civil; anonimidad de las partes; enjuiciamiento acelerado; enjuiciamiento civil japonés.

ABSTRACT: *For a long time, Japan has been a laggard in the digitization of its judiciary. But finally, it took a very important step towards the digitalization of justice through the modification of the Code of Civil Procedure in May 2022. This article aims at tracing the history of the amendment, explaining the overall content of it and giving some analysis.*

KEY WORDS: *Digitalization of justice; Civil procedure; anonymity of the parties; accelerated procedure; Japanese Civil procedure.*

I. INTRODUCCIÓN.

Japón lleva mucho tiempo a la zaga de los rankings mundiales de digitalización de la justicia. Para situarse en el estándar mundial de este campo, Japón decidió introducir la tecnología de la información en el procedimiento civil. Esto se ha logrado a través de dos etapas, una primera etapa de digitalización del enjuiciamiento civil, y una segunda etapa de digitalización de otros procedimientos civiles, como el procedimiento de ejecución o el procedimiento de insolvencia. La primera etapa se logró mediante la modificación de la Ley de Enjuiciamiento Civil japonesa (en adelante LECJ) en mayo de 2022. La segunda etapa se logró a través de la Ley sobre el desarrollo de las leyes pertinentes para promover el uso de las tecnologías de la información y la comunicación en los procedimientos relacionados con los casos civiles, que se aprobó por el legislativo japonés el 6 de julio de 2023.

Este artículo se centra en la primera etapa, es decir, la digitalización del enjuiciamiento civil y ver la historia de la legislación (apartado II) y el contenido de la digitalización (apartado III). En la ley de modificación de la LECJ para la digitalización del enjuiciamiento civil, se introdujeron dos nuevas instituciones, que son, por un lado, una institución para hacer posible que las partes puedan participar en el enjuiciamiento civil ocultando su nombre y/o su dirección, y por otro lado un enjuiciamiento civil especial para finalizar el procedimiento en la primera instancia en un plazo máximo de 7 meses desde la presentación de la demanda al tribunal. Estas instituciones se resumen brevemente también en los apartados IV y V. Y finalmente se dan algunos comentarios en el apartado VI.

El autor de este artículo entiende que España introdujo la digitalización en el enjuiciamiento civil mucho antes que Japón. Por ello, no se sabe hasta qué punto será útil una introducción a la situación en Japón, un país retrasado en este ámbito,

• Takuya Hatta
Catedrático de Derecho Procesal Civil, Universidad de Kobe, Japón.
Correo electrónico: hatta@dragon.kobe-u.ac.jp

pero espera que la comparación de las distintas legislaciones sea útil en algún sentido[1].

II. LA HISTORIA DE LA LEGISLACIÓN.

1. La historia[2].

En el año 2004, Japón trató de introducir un sistema que permite presentar en línea diversas peticiones en procedimientos civiles. Sin embargo, este intento fracasó. En la LECJ se introdujo una disposición que permite realizar diversos trámites judiciales como peticiones al tribunal o actos de comunicación de las causas civiles en línea (art. 132-10.1 LECJ). Pero esta disposición necesita un reglamento especial del Tribunal Supremo para comenzar su funcionamiento y dicho reglamento del Tribunal Supremo no se estableció[3]. Japón tuvo la oportunidad de ser una pionera en este ámbito de la justicia en línea, pero la perdió[4].

Después de mucho tiempo, más de una década, en el año 2017 el Banco Mundial publicó "Doing Business 2017", en la que se valoró a los tribunales japoneses con una muy baja puntuación en cuanto a la introducción de TI (Tecnología de la Información)[5].

En junio de 2017 el Gabinete Japonés tomó una decisión llamada "Estrategias de inversión para el futuro 2017", en la que se determinó empezar los estudios para introducir las TI en los tribunales de Japón. Siguiendo esta decisión, en octubre de 2023, se estableció el Comité para Estudiar la Introducción de IT en Tribunales de Japón bajo la Secretaría del Gabinete[6].

1 Se puede encontrar la explicación en inglés de la enmienda 2022 de la LECJ en Nohara, M.: "Digital Reformation of Japanese Civil Procedures and its Future Prospects" (https://law.stanford.edu/wp-content/uploads/2023/08/Monami-Nohara_digital-reformation-of-Japanese-civil-procedures1.pdf, la última fecha de visita: 15.2.2024). La explicación general en japonés se puede encontrar en Wakimura, S., Hatano, N., Fujita, N., Nishi R. y Oniwa Y.: "'Minjisoshohotou no Ichibu wo Kaisei suru Horitsu' no Gaiyo", *Houritsu no Hiroba*, 2022, vol. 75°, núm. 9°, pp. 4-12.

2 La explicación detallada en japonés de la historia de la enmienda se puede en encontrar en Yamamoto, K.: *Minjisaibantetsuzuki no ITka*, Kobundo, Tokyo, 2023, pp. 1-28.

3 Con una excepción de un reglamento para el procedimiento de reclamación. El procedimiento de reclamación es un procedimiento en lo que el demandante interpone una reclamación de pago de determinadas sumas de dinero al tribunal, que se procesa por el secretario judicial, quien entrega la reclamación al demandante sin examinar el fondo, y si el demandante no se opone, la reclamación se puede ejecutar. Para este procedimiento se estableció un reglamento que permite el tratamiento en línea. Ver https://www.toku-on.courts.go.jp/GA0101.html (Sólo en japonés. La última fecha de visita: 15.2.2024).

4 Yamamoto, K.: *Minjisaibantetsuzuki no*, cit. p. 9-10.

5 Yamamoto, K.: *Minjisaibantetsuzuki no*, cit. p. 11.

6 Yamamoto, K.: *Minjisaibantetsuzuki no*, cit. p. 11.

En marzo de 2018, este comité publicó un informe escrito. El informe propuso la implantación de la digitalización completa en el proceso civil japonés. De modo que, se dividió la digitalización en 3 secciones de digitalización:[7]

Una primera sección que permite la presentación a través de medios electrónicos. Y no solo la presentación, sino también la notificación de la demanda en línea y el intercambio de los documentos dentro del procedimiento en línea.

Una segunda sección para la gestión de los casos a través de medios electrónicos, principalmente para la digitalización del archivo de los casos.

Y una tercera sección que prevé una sala de vistas a través de medios electrónicos, de modo que sea posible celebrar las vistas (incluyendo la prueba testifical) por reuniones en línea.

En este informe se propuso también el calendario para realizar la digitalización, dividiendo las fases en tres[8].

Una primera fase, cuyo objetivo era el aprovechamiento de la TI existente y permitida dentro del marco de la legislación vigente (la delimitación de los hechos controvertidos (que necesitan ser probados) por reunión en línea con capacidad limitada.) y que dio comienzo en 2019.

Una segunda fase de introducción de las medidas que necesitan nueva legislación, pero no nuevos equipamientos (intercambio de las alegaciones por las partes, delimitación de los hechos controvertidos a través de reunión en línea con capacidad completa.). Para ello se comenzaron los estudios para la legislación en 2019 y se introdujeron las propias medidas en 2022.

Y una tercera fase de introducción de las medidas que necesitan nueva legislación y también nuevos equipamientos (presentación de documentos por las partes al tribunal en línea, etc.). Se empezaron los estudios para la legislación en 2019 y por otro lado, los estudios de equipamientos necesarios también en 2019.

En julio de 2018 se creó la Asociación de Investigación para la Digitalización del Derecho Procesal Civil. Esta realizó una Ronda preliminar para preparar la legislación[9]. La asociación publicó un informe escrito en diciembre de 2019. Siguiendo este informe empezó la deliberación para la legislación en el Consejo Legislativo del Ministerio de Justicia en febrero de 2020[10]. En febrero de 2022 el

7 Yamamoto, K.: *Minjisaibantetsuzuki no*, cit. p. 11-12.

8 Yamamoto, K.: *Minjisaibantetsuzuki no*, cit. pp. 16-18.

9 Yamamoto, K.: *Minjisaibantetsuzuki no*, cit. pp. 22-23.

10 Yamamoto, K.: *Minjisaibantetsuzuki no*, cit. p. 23.

Consejo terminó la deliberación y presentó el borrador del Proyecto de la Ley de Modificación de la LECJ[11]. En el mismo mes, el Gabinete japonés presentó al Parlamento el Proyecto de la Ley de Modificación de la LECJ. En mayo del mismo año la Dieta[12] aprobó la Ley de Modificación de la LECJ. La entrada en vigor de esta Ley se realizará gradualmente y su finalización está prevista para marzo de 2026[13].

2. Tres pilares de modificación.

La Ley de Modificación de la LECJ aprobado en mayo de 2022 tiene 3 pilares, que son:

1. Digitalización del Enjuiciamiento Civil.

2. Posibilitar que las partes participen en el procedimiento sin que la otra parte conozca su nombre y/o dirección bajo una determinada condición.

3. Introducción de un enjuiciamiento acelerado[14].

Veremos estos 3 pilares uno por uno.

III. DIGITALIZACIÓN DEL ENJUICIAMIENTO CIVIL.

El primer pilar de la digitalización del procedimiento civil consiste en los siguientes puntos.

1. Presentar una demanda y otros documentos al tribunal en línea (art. 132-10.1, 132-11.1 nueva LECJ)[15].

En la nueva ley, es posible presentar una demanda y otros documentos (documentos de preparación[16], por ejemplo) en línea. En el curso del proceso legislativo, había discusión sobre si se debía hacer obligatoria la presentación en línea. La solución que da la nueva ley es que presentar una demanda y los documentos que deban acompañarla en línea es obligatorio solo para los abogados cuando

11 Yamamoto, K.: *Minjisaibantetsuzuki no*, cit. p. 23-24.

12 Que la conforman las Cámaras legislativas japonesas.

13 Texto legislativo disponible en: https://elaws.e-gov.go.jp/document?lawid=408AC0000000109_20260524_504AC0000000048, última visita 15.2. 2024 (sólo en japonés).

14 Yamamoto, K.: *Minjisaibantetuduki no*, cit. pp. 29-30.

15 Entrada en vigor prevista para marzo de 2026. La explicación detallada de este sistema en japonés se encuentra en Kakiuchi, S.: "Minjisaibantetsuzuki no ITka – 1. Online Moushitate, Soshokiroku no Denshika", *Houritsu no Hiroba*, 2022, vol. 75°, núm. 9°, pp. 13-15; Yamamoto, K.: *Minjisaibantetsuzuki no*, cit. pp. 31-41.

16 Es obligatorio para las partes presentar al tribunal y a la otra parte un documento que indique qué alegaciones van a hacer o qué pruebas van a presentar en la próxima audiencia previa o en el próximo juicio (art. 161 LECJ). Este documento es llamado "documento de preparación".

representan a las partes, pero no cuando las partes litigan en representación y defensa propia[17].

2. Gestión de expedientes de litigios[18].

Como hemos visto arriba (III. -1.), los documentos que las partes presentan al tribunal en un enjuiciamiento pueden presentarse en línea y es obligatorio en principio solo cuando la parte está representada por un abogado.

Por ello, las partes pueden presentar los documentos físicamente cuando no están representadas por un abogado. Incluso en estos casos, la gestión de los documentos que las partes presentan se hace digitalmente. El secretario del tribunal encargado del caso debe escanear los documentos y convertirlos a PDF, a menos que sea difícil hacerlo o exista una gran necesidad de confidencialidad de la información contenida en ellos (art. 132-12.1, 132-13.1 nueva LECJ).

El secretario del tribunal es el encargado de formar los expedientes de las audiencias previa y los juicios. Estos deben ser creados como un documento digital (art. 160.1 nueva LECJ). Y las sentencias también deben ser redactadas como un documento digital (art. 252.1 nueva LECJ).

El acceso de las partes y los terceros a los expedientes del proceso es reglado como detallamos a continuación.

Las partes y sus representantes tienen acceso a los expedientes desde los ordenadores externos a los tribunales (en casa o en su despacho, por ejemplo) siempre, incluso cuando los tribunales están cerrados (los 365 días del año, las 24 horas del día) (art. 91-2.1, 2 nueva LECJ. Los detalles se estipularán en el próximo nuevo Reglamento del Tribunal Supremo). Está permitida la visualización y la descarga de los expedientes.

Los Terceros que tienen un interés legítimo en el caso tienen acceso a los expedientes desde los ordenadores dentro y fuera de los tribunales, pero solo durante el horario en que el tribunal está abierto (art. 91-2.1,2,4, 91.5 nueva LECJ. Los detalles se estipularán en el próximo nuevo Reglamento del Tribunal Supremo). A ellos se les permite ver y descargar los expedientes igual que a las partes.

17 Para ser más precisos, presentación de los documentos en línea es obligatorio en 3 casos siguientes: a) cuando los abogados representan las partes, b) cuando una persona litiga en representación del estado Japón, c) cuando un personal de un organismo público litiga en representación del organismo. Art. 132-11.1 LECJ.

18 Entrada en vigor prevista para marzo de 2026. La explicación detallada de este sistema en japonés se encuentra en Kakiuchi, S.: "Minjisaibantetsuzuki no", cit., p. 15; Yamamoto, K.: *Minjisaibantetsuzuki no*, cit. pp. 80-95.

El resto de personas también tienen acceso a todos los expedientes[19], salvo que el tribunal ordene la prohibición de la publicación de la audiencia, pero sólo desde los ordenadores en los tribunales. (art. 91-2.1,4, 91.2,5 nueva LECJ. Los detalles se estipularán en el próximo nuevo Reglamento del Tribunal Supremo). Sin embargo, a estos sólo les está permitido ver los expedientes, pero no descargarlos.

3. Entrega de los documentos (demanda para la iniciación del proceso, sentencia, etc.)[20].

El tratamiento es distinto para los que han aceptado "la notificación sistemática" o electrónica y para los que no la han aceptado.

Para los que la han aceptado, la entrega de los documentos procesales en línea se realiza por "la notificación sistemática". En la "notificación sistemática", el tribunal carga los documentos en el sitio web e informa al destinatario de que los documentos están listos para descargar (art. 109-2.1 nueva LECJ). Los abogados que representan las partes están obligados a aceptarla (art. 109-2.2 nueva LECJ).

A los ciudadanos que no han aceptado "notificación sistemática", la entrega se realiza enviando los documentos impresos. (art. 109 nueva LECJ). Los ciudadanos normalmente no la aceptarán. Así que se prevé que la notificación de una demanda se haga mediante entrega de documentos impresos, porque normalmente el demandado no está representado por un abogado al principio del procedimiento.

4. Celebración de fechas de audiencias y vistas a través de internet[21].

En Japón, el enjuiciamiento estándar se desarrolla en tres etapas: En la primera, las partes hacen sus alegaciones del caso; en la segunda se delimitan los hechos controvertidos y las evidencias aparte de las documentales (las evidencias documentales se examinan en esta etapa) y en la tercera se examinan las evidencias no documentales (las pruebas testificales, los interrogatorios de las partes, las pruebas periciales, etc.). En principio, todas las etapas se celebran a través de audiencias. Las audiencias para la primera y la tercera etapa necesitan ser públicas.

19 En Japón, la Constitución estipula que los juicios deben celebrarse en audiencia pública (art. 82.1 de la Constitución de Japón). Por eso, incluso ahora, cualquier ciudadano tiene acceso y puede leer a todos los expedientes de cualquier caso en principio. Pero está prohibido hacer una copia. Art. 91.1 LECJ vigente. Según la Constitución japonesa, el tribunal puede prohibir la publicación de la audiencia cuando decida que la publicación vulneraría el orden público o la moralidad (art. 82.2 de la Constitución japonesa), en su caso, los terceros que no tienen un interés legítimo al caso no tienen acceso a los expedientes. Art. 91.2 de LECJ vigente y art. 91.2 y 91-2.4 nueva LECJ.

20 Entrada en vigor prevista para marzo de 2026. La explicación detallada de este sistema en japonés se encuentra en Kakiuchi, S.: "Minjisaibantetsuzuki no", cit., pp. 15-16; Yamamoto, K.: Minjisaibantetsuzuki no, cit. pp. 42-51.

21 La explicación detallada de este sistema en japonés se encuentra en Ata, H.: "Minjisaibantetsuzuki no Digitalka (ITka) – 2. Web Kaigitou", *Houritsu no Hiroba*, 2022, vol. 75°, núm. 9°, pp. 18-23; Yamamoto, K.: *Minjisaibantetsuzuki no*, cit. pp. 56-80.

Las audiencias para la segunda etapa no necesitan ser públicas. Y hay también audiencias para la transacción entre las partes, que no necesitan ser públicas. [22]

En virtud de la LECJ, antes de la modificación en el año 2022, ya era posible celebrar las audiencias en línea. Pero según la nueva ley, la celebración de las audiencias en línea está permitida bajo una condición más relajada.

Las audiencias con el objetivo de que las partes hagan las alegaciones del caso pueden celebrarse en línea cuando el tribunal lo considere oportuno, tras oír la opinión de las partes (art. 87-2.1 LECJ).[23] Las audiencias para la delimitación de los hechos controvertidos también pueden celebrarse en línea cuando el tribunal lo considere oportuno, tras oír la opinión de las partes (art. 170.3 nueva LECJ).[24] En estos casos el tribunal no necesita obtener los consentimientos de las partes. Este reglamento se aplica también a las audiencias para la transacción, es decir, para llegar a un acuerdo entre las partes (art. 89.2,3 nueva LECJ).[25]

Las audiencias para las pruebas testificales y para los interrogatorios de las partes pueden celebrarse en línea cuando el tribunal lo considere oportuno y además se cumpla uno de los siguientes requisitos:

1. Que sea difícil que el testigo (en caso de la prueba testifical) o la parte (en caso del interrogatorio de las partes) se presente ante el tribunal;

2. que sea posible que el testigo o la parte se sienta amenazada si acude a dar testimonio ante los jueces y las partes o

3. que ninguna de las partes se oponga. (art. 204, 210 nueva LECJ)[26].

En la prueba pericial, el tribunal decidirá si se hará oralmente o documentalmente (art. 215.1 LECJ). Si el tribunal decide que se haga oralmente, el tribunal puede decidir que se haga en línea cuando lo considere oportuno (art. 215-3 nueva LECJ)[27]. En este caso tampoco necesita oír la opinión de las partes. Si el tribunal

22 Para una explicación del procedimiento civil ordinario de Japón, véanse Yasunaga, Y.: "La prueba pericial civil en Japón", en AA.VV.: *La Prueba Pericial a Examen – Propuestas de lege ferenda* (dir. por J. Picó i Junoy, coord. por J. A. Andino López y E. Cerrato Guri), J. M. Bosh Editor, Barcelona, 2020, pp. 196-199. La explicación en inglés puede obtenerse en Supreme Court of Japan: *Outline of Civil Procedure in JAPAN* 2022 (https://www.courts.go.jp/english/vc-files/courts-en/Material/Outline_of_Civil_Procedure_in_JAPAN_2022.pdf, última visita 29.3.2024).

23 Entrada en vigor prevista para marzo de 2024.

24 Ya ha entrado el vigor en 3. 3. 2023.

25 Ya ha entrado el vigor en 3. 3. 2023.

26 Entrada en vigor prevista para marzo de 2026.

27 Entrada en vigor prevista para marzo de 2026.

decide que se haga documentalmente, el perito puede presentar su opinión por un archivo digital (art 215.2 nueva LECJ)[28].

La práctica de las pruebas en lugares distintos de la sede del tribunal puede celebrarse en línea cuando el tribunal lo considere oportuno, tras oír la opinión de las partes. (art. 185.3 nueva LECJ).[29]

La antigua ley no tenía un reglamento especial para la prueba de las informaciones que existen digitalmente y la prueba se debía hacer a través de un documento impreso. La nueva ley si lo contempla en el art. 231-2 nueva LECJ, según la cual se puede hacer a través de la presentación (cuando el proponente de la prueba tiene los datos) o a través de un mandato del tribunal en el que se ordene la presentación (cuando el proponente no tiene los datos) del archivo digital[30].

IV. LA INSTITUCIÓN QUE PERMITE QUE LAS PARTES PARTICIPEN EN EL PROCEDIMIENTO DE MANERA ANÓNIMA[31].

Bajo la nueva LECJ, las partes (demandante y demandado) o el representante legal de una parte pueden participar en el procedimiento sin que la otra parte conozca parte o la totalidad de su nombre y/o dirección, si se demuestra que con ello se causarían dificultades significativas para llevar una vida social normalizada (art. 133 nueva LECJ). Por ejemplo, una víctima de violencia doméstica puede presentar una demanda por daños y perjuicios contra su exesposo ocultando parte o la totalidad de su nueva dirección a él. Especialmente cuando el esposo presenta una demanda contra su esposa por divorcio, cuando ya están viviendo separados y este no conoce su dirección actual. En estos casos la demandada puede seguir con el procedimiento (sin que el demandante conozca su dirección), si ella fue una víctima de violencia doméstica y se confirma que el esposo era violento con ella[32]. Así mismo, una víctima de delito sexual puede presentar una

28 Entrada en vigor prevista para marzo de 2026.

29 Entrada en vigor prevista para marzo de 2026.

30 Yamamoto, K.: *Minjisaibantetsuzuki no*, cit. pp. 51-55.

31 Ya ha entrado en vigor el 20. 2. 2023. La explicación detallada de este sistema en japonés se encuentra en Aoki, S.: "Jusho, Shimeitou no Hitokuseido", *Houritsu no Hiroba*, 2022, vol. 75°, núm. 9°, pp. 47-50; Yamamoto, K.: *Minjisaibantetsuzuki no*, cit. pp. 111-133.

32 Cuando la esposa cambia su domicilio, su residencia se registra en el municipio que tiene jurisdicción sobre su nueva dirección. Normalmente el esposo puede obtener el traslado del certificado de residencia de la esposa en el municipio que tiene jurisdicción sobre la residencia donde vivián los dos juntos. El traslado tiene información sobre la nueva dirección de la esposa. De este modo, el esposo puede conocer su nueva dirección. Pero si la esposa fue una víctima de violencia y existe el riesgo de que su vida o su cuerpo corran peligro por la violencia, ella puede hacer una petición para que su esposo no pueda obtener el traslado del certificado de su residencia. Se llama medidas de protección. Si se aplican medidas de protección, el esposo no puede conocer la dirección actual de su esposa. Por eso el esposo presenta una demanda indicando que se desconoce el domicilio de la demandada, su esposa. En este caso, el tribunal encarga al municipio la investigación de la dirección de la demandada. Bajo la nueva ley, cuando el tribunal obtenga el documento con la información sobre la dirección actual de la demandada, emite una orden en

demanda por daños y perjuicios ocultando su dirección y nombre al demandado, si el demandado no los conoce.

La parte o el representante de una parte que quiere ocultar dicha información debe presentar una solicitud de secreto y mostrar la causa (explicando que se causaría dificultades significativas para llevar una vida social, si la otra parte la conoce). Cuando el tribunal acepta la causa de anonimización, emite una decisión de secreto, en la que especifica la alternativa para la información oculta (nombre y/o dirección). Se considera que la parte ha escrito su nombre y/o dirección (la información oculta) cuando escribe la alternativa especificada por el tribunal (art. 133 nueva LECJ).

Dentro de los expedientes, las partes de los documentos que contienen información oculta no pueden ser leídas ni consultadas por la otra parte, si se dicta la decisión de secreto de alguna parte de los expedientes (art. 133-2 nueva LECJ).

La otra parte tiene derecho a presentar una moción para anular la decisión de secreto con la razón por la que no se cumple o ha desaparecido el requisito (art. 133-4.1 nueva LECJ). También se le permite leer o consultar la información oculta cuando demuestre que se ve amenazado con la posibilidad de que su derecho a la defensa sufra un perjuicio importante (art. 133-4.2 nueva LECJ). Cuando el tribunal permite a la otra parte leer o consultar la información oculta, la otra parte no está autorizada a utilizar la información para fines distintos de la continuación del procedimiento o para mostrar la información a otras personas (art. 133-4.7 nueva LECJ).

V. INTRODUCCIÓN DE UN ENJUICIAMIENTO ACELERADO[33].

El enjuiciamiento acelerado que la nueva ley introdujo se llama "el enjuiciamiento con plazo de juicio estatutario". En este enjuiciamiento especial la delimitación de los hechos controvertidos (que necesitan ser probados) debe ser finalizado en 5 meses. La celebración de las pruebas debe terminarse en 6 meses desde el inicio de la demanda. Y el tribunal debe dictar la sentencia en 7 meses desde el inicio del proceso (art. 381-3 nueva LECJ). Este nuevo procedimiento no tiene una

la que prohíbe al demandante leer el documento de oficio, cuando es evidente que se puede causar un impedimento grave a la vida social de la demandada, si el demandante lea el documento (art. 133-2.1 nueva LECJ). Con este orden, la entrega de la demanda se celebra sin que el demandante conozca la dirección de la demandada. Cuando la demandada recibe la demanda, ella puede hacer una petición por la decisión de secreto. Véanse Koshiyama, K.: "Higaisha no Shimeitou wo Aitegata ni Hitoku suru Seido", Jurist, 2022, núm. 1577°, pp. 61-62. (escrito en japonés) ; Yamamoto, K.: *Minjisaibantetsuzuki no*, cit. pp. 122-124.

33 Entrada en vigor prevista para marzo de 2026. La explicación detallada de este sistema en japonés se encuentra en Kasai, M.: "Houteishinrikikan Soshoutetsuzuki", *Houritsu no Hiroba*, 2022, vol. 75°, núm. 9°, pp. 43-46; Yamamoto, K.: *Minjisaibantetsuzuki no*, cit. pp. 100-111.

relación directa con la digitalización de la justicia, pero la eficacia realizada por la digitalización facilita que el procedimiento termine tan pronto.

Los litigios en materia de consumo y los litigios laborales individuales son excluidos de este enjuiciamiento (art. 381-2.1 nueva LECJ). En estos casos no se puede elegir este enjuiciamiento especial. Pero no hay ninguna otra limitación de los casos en que se puede utilizar este procedimiento. Si bien, ambas partes deben estar de acuerdo para usar este procedimiento (art. 381-2.2 nueva LECJ).

No se puede usar este procedimiento cuando el tribunal considere que el uso de este procedimiento perjudicaría la equidad entre ambas partes o impediría la realización de una investigación adecuada del caso. (art. 381-2.2 nueva LECJ). Además, cualquiera de las partes puede solicitar en cualquier momento que el asunto se juzgue por un procedimiento ordinario. (art. 381-4.1 nueva LECJ).

Contra la sentencia dada como el resultado de este procedimiento, las partes pueden presentar una objeción. (art. 381-7.1 nueva LECJ). Esta objeción hace que el caso sea juzgado otra vez por el mismo tribunal en un procedimiento ordinario. (art. 381-8.1 nueva LECJ).

VI. ALGUNOS COMENTARIOS.

1. Sobre la digitalización.

A) En cuanto al presentar una demanda y otros documentos en línea como obligación parcial.

Como hemos visto antes (en IV. -1.), presentar una demanda y otros documentos en línea es obligatorio para los abogados, pero no para los procesos que realizan ciudadanos sin representación.

Poder gestionar los expedientes en línea facilita compartir información entre las partes y el tribunal, y a través de eso promueve la eficacia y la eficiencia del proceso. Si la demanda y otros documentos son presentada con los documentos físicos, estos se escanearán a datos digitales, pero sólo como PDF y no se realiza digitalización completa. Por ello, es deseable que las demandas y otros documentos se presenten en línea.

Por otra parte, uno de los objetivos de la digitalización del proceso es aumentar y mejorar el acceso a la justicia. Debido al alto porcentaje de la población con carencias digitales, es imposible obligar a toda la nación presentar una demanda y otros documentos en línea y por ello obligar solo a los abogados es una solución sensata.

En Japón un buen porcentaje de las partes litigan pro se, es decir, autodefendiéndose[34]. Si se busca que las demandas y otros documentos sean presentadas en línea para promover la eficacia del proceso, es imprescindible enriquecer el apoyo que se les presta a los ciudadanos y hay un problema de cómo hacerlo. También existen los abogados con debilidad digital, y en este sentido hay un problema de cómo ayudarlos para solventar esta brecha digital.

B) En cuanto la celebración las audiencias y los juicios en línea.

Así las cosas, queda como un problema por resolver cómo asegurar que las acciones de las partes no sean afectadas por un tercero. Si resulta prácticamente imposible prevenir la intervención de un tercero, pero podrían surgir dudas sobre la racionalidad de limitar la representación de las partes a los abogados, porque la limitación de la representación de las partes a los abogados no tendría ningún efecto para impedir la intervención e influencia del tercero sobre las partes.

El riesgo de la influencia de un tercero es especialmente alto en la prueba testifical. Se dice también que la impresión que los jueces obtienen del testimonio es mucho más vívida cuando se hace cara a cara que cuando se hace en línea. Realizar la prueba testifical en línea podría resultar desventajoso para las partes.

En la nueva ley, la prueba testifical puede celebrarse en línea sólo cuando ambas partes están de acuerdo con ella, si no existen circunstancias objetivas que justifiquen celebrar prueba testifical en línea, como la dificultad del testigo para presentarse ante el tribunal debido a su edad, etc. (art. 204 nueva LECJ. Véanse también III. 4. supra). Esto significa que está en manos de las partes decidir si la audiencia de testigos se llevará a cabo en línea o no en tal situación. Las partes deben de ser cautelosas en dar luz verde a la prueba testifical en línea.

El tribunal puede decidir llevar a cabo el examen de las pruebas fuera del tribunal cuando lo considere oportuno (art. 185.1 LECJ). Esto debe incluir la audiencia de testigos. Y cuando el tribunal lleve a cabo el examen de las pruebas fuera del tribunal, puede decidir hacerlo en línea sin el consentimiento de las partes si oye su opinión (art. 185.3 nueva LECJ. Véanse también III. 4. anterior). Este reglamento podría dejar un resquicio para que el tribunal lleve a cabo el examen de testigos sin el consentimiento de las partes, incluso en situaciones en

34 Según Nihon Bengoshi Rengokai (Colegio de Abogados de Japón): *Bengoshi Hakusho 2023 (Libro Blanco de la Abogacía 2023)*, Nihon Bengoshi Rengokai, Tokyo, 2024, en los tribunales de distrito, 10.4 % de los demandantes y 49.1% de los demandados litigaron pro se, y en los tribunales sumarios, 84.5 % de los demandantes y 86.8% de los demandados litigaban pro se en el año 2023.
En Japón, existen 2 tipos de tribunales que conocen de los asuntos en primera instancia. Uno es el tribunal de distrito, de que hay 50 en todo Japón; el otro es el tribunal sumario, de que hay 438 en todo Japón. Los tribunales de distrito aceptan demandas cuyo valor supere los 140 yenes y demandas sobre bienes inmuebles. Los tribunales sumarios aceptan demandas cuyo valor no supere los 140 yenes. Supreme Court of Japan: *Outline of*, cit., p. 6.

las que las circunstancias objetivas no lo justifiquen. Podría ser tarea del mundo académico impedir tal interpretación o manipulación de la ley.

C) En cuanto a si se retransmiten en abierto al público las audiencias y los juicios en línea.

La nueva ley decidió que no, porque los legisladores estaban preocupados por los riesgos de ciberseguridad. También se señaló el problema de que la gente podría dudar a la hora de presentar una demanda o actuar en defensa por miedo a que su caso fuera ampliamente conocido por el público.

Pero la retransmisión de la vista por Internet tiene el efecto de reforzar la vigilancia del procedimiento por parte del público y hay opiniones a favor de introducir este sistema en el futuro[35]. Queda como un problema por resolver si debemos introducirlo[36].

En cuanto a la vigilancia del procedimiento por parte del público, el fácil acceso a los expedientes por parte de terceros (véanse III. 2. supra) también puede tener este efecto. Desde este punto de vista, la creación de una base de datos de todas las sentencias judiciales es muy deseable. Esto también facilitaría la investigación de las sentencias judiciales por parte de los académicos. No se trata de una cuestión regulada por la Ley de Enjuiciamiento Civil, sino de una decisión del Tribunal, pero esperamos que se cree dicha base de datos.

D) Uso de los IA (inteligencia artificial) o justicia predictiva.

Todavía no estamos preparados para examinar como debemos utilizar y regular inteligencia artificial o como debemos enfrentarnos a la justicia predictiva. Es una próxima etapa tras la digitalización del procedimiento que hicimos con la ley de 2022 y de 2023. Pero con el rápido desarrollo de la tecnología, no tenemos tiempo que perder para decidir nuestra postura sobre cómo hacer frente a la IA en el ámbito de la justicia.

2. Sobre la anonimización de las partes.

Es importante comentar la situación por la que la nueva ley introdujo un sistema en que las partes o su representante pueden participar en el proceso ocultando incluso su nombre. El sistema está estructurado para permitir el anonimato siempre que no se vulnere el derecho a la defensa de la otra parte.

35 Honma, M.: "Digital Jidai niokeru Minjisosho no Kokai to Sono Kadai", *Minjisosho Zasshi*, 2023, núm. 69°, pp. 148-155 (escrito en japonés).

36 Yamamoto, K.: *Minjisaibantetsuzuki no*, cit. p. 64.

Pero aquí se requiere un equilibrio muy sutil en la gestión del sistema. Proceder con la demanda ocultando el propio nombre tiene el riesgo de perjudicar considerablemente el derecho a la defensa de la otra parte. Por eso, por un lado, el tribunal debe gestionar el sistema para permitir la anonimidad sólo cuando no infrinja el derecho de defensa de la otra parte. Por otro lado, aunque el tribunal autorice la anonimidad en un primer momento, ésta puede anularse a petición de la otra parte. Pero no hay ninguna estipulación en la ley que permita a la parte que ha estado ocultando su nombre (o dirección) impedir que su nombre (o dirección) sea conocido por la otra parte incluso renunciando a la demanda, una vez cancelado el anonimato.

Esto podría traicionar la expectativa de la parte que solicitó la anonimidad, que pretendía continuar con el pleito ocultando su nombre y/o dirección a la otra parte. El tribunal también está obligado a gestionar el sistema para no provocar este tipo de consecuencias. Sin embargo, es cuestionable que sea posible una gestión tan cuidadosa. Por ello, deberemos observar atentamente cómo gestionará el tribunal este nuevo sistema.

3. Sobre el enjuiciamiento acelerado.

Se produjeron fuertes discusiones en el curso del procedimiento legislativo de esta institución, pero la nueva ley adoptó un diseño liviano, ya que este procedimiento especial se puede poner en marcha sólo cuando ambas partes lo deseen y es muy fácil para ambas partes salirse de él (cada parte puede decidir cambiar el procedimiento al ordinario en cualquier momento del procedimiento e incluso después de la sentencia).

Por eso, cabe dudar de la frecuencia con que se utilizará este procedimiento finalmente, pero quizás se usará con más frecuencia en demandas por conflictos entre empresas, debido a la rapidez que precisan en sus transacciones comerciales.

V. CONCLUSIONES.

El propósito de la digitalización de la justicia a través de la enmienda 2022 de la LECJ era hacer más eficiente a la judicatura y conseguir que el procedimiento civil fuera más eficaz, rápido y fructífero. Eficaz en el sentido de que se puede reducir la carga del tribunal (porque ya no necesita imprimir todos los documentos, etc.) [37] y también de las partes (porque ya no necesita ir al tribunal para asistir a la audiencia, porque tienen acceso al expediente del caso desde sus casas u oficinas en cualquier momento, etc.)[38] y de terceros (porque es posible que no necesita

37 Yamamoto, K.: *Minjisaibantetsuzuki no*, cit. pp. 1-2.

38 Yamamoto, K.: *Minjisaibantetsuzuki no*, cit. pp. 2-3.

ir al tribunal para dar testimonios, etc.)[39]. Rápido porque podemos suprimir el desfase temporal causado por la entrega de documentos por correo, porque resulta más fácil para el tribunal fijar una fecha de audiencia, etc.[40]. Fructífero en el sentido de que el tribunal y las partes pueden utilizar el tiempo ahorrado para examinar el caso más en detalle y aumentar la productividad[41].

Este objetivo no puede alcanzarse únicamente mediante la presentación de documentos, la gestión de expedientes, la celebración de vistas, etc. a través de Internet. Además de ser necesaria la introducción de la IA, el manejo de la nueva ley debe hacerse teniendo en cuenta el propósito antes mencionado. Por ello, tenemos que vigilar de cerca para que el desarrollo de la digitalización de la justicia no se desvíe del propósito original.

39 Yamamoto, K.: *Minjisaibantetsuzuki no*, cit. p. 2.

40 Yamamoto, K.: *Minjisaibantetsuzuki no*, cit. pp. 2-3.

41 Yamamoto, K.: *Minjisaibantetsuzuki no*, cit. p. 3.

BIBLIOGRAFÍA

Aoki, S.: "Jusho, Shimeitou no Hitokuseido", *Houritsu no Hiroba*, 2022, vol. 75º, núm. 9º, pp. 47-50 (escrito en japonés).

Ata, H.: "Minjisaibantetsuzuki no Digitalka (ITka) – 2. Web Kaigitou", *Houritsu no Hiroba*, 2022, vol. 75º, núm. 9º, pp. 18-23 (escrito en japonés).

Honma, M.: "Digital Jidai niokeru Minjisosho no Kokai to Sono Kadai", *Minjisosho Zasshi*, 2023, núm. 69º, pp.148-155 (escrito en japonés).

Kakiuchi, S.: "Minjisaibantetsuzuki no ITka – 1. Online Moushitate, Soshokiroku no Denshika", *Houritsu no Hiroba*, 2022, vol. 75º, núm. 9º, pp. 13-15 (escrito en japonés).

Kasai, M.: "Houteishinrikikan Soshoutetsuzuki", *Houritsu no Hiroba*, 2022, vol. 75º, núm. 9º, pp. 43-46 (escrito en japonés).

Koshiyama, K.: "Higaisha no Shimeitou wo Aitegata ni Hitoku suru Seido", *Jurist*, 2022, núm. 1577º, pp. 61-62. (escrito en japonés).

Nihon Bengoshi Rengokai (Colegio de Abogados de Japón): *Bengoshi Hakusho 2023 (Libro Blanco de la Abogacía 2023)*, Nihon Bengoshi Rengokai, Tokyo, 2024

Nohara, M.: "Digital Reformation of Japanese Civil Procedures and its Future Prospects" (https://law.stanford.edu/wp-content/uploads/2023/08/Monami-Nohara_digital-reformation-of-Japanese-civil-procedures1.pdf, la última fecha de visita: 15.2.2024) (escrito en inglés)

Supreme Court of Japan: *Outline of Civil Procedure in JAPAN* 2022 (https://www.courts.go.jp/english/vc-files/courts-en/Material/Outline_of_Civil_Procedure_in_JAPAN_2022.pdf, última visita 29.3.2024) (escrito en inglés).

Wakimura, S., Hatano, N., Fujita, N., Nishi R. Y Oniwa Y.: "'Minjisoshohotou no Ichibu wo Kaisei suru Horitsu' no Gaiyo", *Houritsu no Hiroba*, 2022, vol. 75º, núm. 9º, pp. 4-12 (escrito en japonés).

Yamamoto, K.: *Minjisaibantetsuzuki no ITka*, Kobundo, Tokyo, 2023.

Yasunaga, Y.: "La prueba pericial civil en Japón", en AA.VV.: *La Prueba Pericial a Examen – Propuestas de lege ferenda* (dir. por J. Picó i Junoy, coord. por J. A. Andino López y E. Cerrato Guri), J. M. Bosh Editor, Barcelona, 2020, pp. 196-199 (escrito en castellano).

EL CARÁCTER ELECTRÓNICO DEL PRIMER EMPLAZAMIENTO O CITACIÓN DEL DEMANDADO: ¿EFICIENCIA VERSUS GARANTÍAS? EL ANTES Y EL DESPUÉS DEL REAL DECRETO-LEY 6/2023*

THE ELECTRONIC CHARACTER OF THE FIRST DOCUMENT INSTITUTING THE PROCEEDINGS OR SUMMONS OF THE DEFENDANT: EFFICIENCY VERSUS GUARANTEES? BEFORE AND AFTER ROYAL DECREE-LAW 6/2023

Actualidad Jurídica Iberoamericana Nº 21, agosto 2024, ISSN: 2386-4567, pp. 148-189

* Este trabajo ha sido redactado en el marco del Proyecto de investigación "Claves para una justicia digital y algorítmica con perspectiva de género" (expediente: PID2021-123170OB-I00) financiado por MCIN/AEI/10.13039/501100011033 y toma como base la ponencia "La comunicación electrónica: ¿eficiencia *versus* garantías procesales?" impartida en el "Congreso Internacional Digitalización y algoritmización de la justicia: nuevos retos, desafíos y oportunidades", celebrado los días 26 y 27 de octubre de 2023 en la Universidad Católica de Valencia San Vicente Mártir.

Diana MARCOS FRANCISCO

ARTÍCULO RECIBIDO: 29 de mayo de 2023
ARTÍCULO APROBADO: 1 de julio de 2024

RESUMEN: Sorpresivamente, y con una gran premura, acaba de aprobarse el Real Decreto-ley 6/2023, de 19 de diciembre, por el que se aprueban medidas urgentes para la ejecución del Plan de Recuperación, Transformación y Resiliencia en materia de servicio público de justicia, función pública, régimen local y mecenazgo, que introduce -por lo que ahora interesa destacar- trascendentales medidas de fomento y uso de las tecnologías de la información y comunicación (TIC) en el ámbito de la Administración de Justicia. Dicha aprobación invita a valorar los cambios introducidos al respecto, de entre los que el presente estudio se centra en analizar críticamente la regulación atinente a una cuestión procesal esencial al relacionarse con el derecho fundamental a obtener una tutela judicial efectiva (art. 24.1 CE), como es la forma en que se debe practicar el primer emplazamiento o citación del demandado cuando éste sea un sujeto obligado a relacionarse electrónicamente con la aludida Administración. Tal examen se efectúa considerando la jurisprudencia española existente, incluyendo la más reciente.

PALABRAS CLAVE: Notificaciones electrónicas; primer emplazamiento o citación; garantías procesales; derecho a la tutela judicial efectiva.

ABSTRACT: *Surprisingly, and with great haste, Royal Decree-Law 6/2023, of December 19, has just been approved, which approves urgent measures for the execution of the Recovery, Transformation and Resilience Plan in matters of public justice service , public service, local government and patronaje, which introduces - for what is now interesting to highlight - transcendental measures to promote and use information and communication technologies (ICT) in the subject of the Administration of Justice. This approval invites us to evaluate the changes introduced in this regard, among which the present study focuses on critically analyzing the regulation related to an essential procedural issue like the right to effective legal protection (art. 24.1 CE), as is the way in which the first document instituting the proceedings or summons of the defendant should be carried out when the latter is a subject obliged to relate electronically with the aforementioned Administration. Such examination is carried out considering the Spanish jurisprudence, including the most recent.*

KEY WORDS: *Electronic notifications; first document instituting the proceedings or summons; procedural guarantees; right to effective legal protection.*

SUMARIO.- I. SUJETOS OBLIGADOS Y NO OBLIGADOS A RELACIONARSE ELECTRÓNICAMENTE CON LA ADMINISTRACIÓN DE JUSTICIA.- 1. Introducción.- 2. Lo que no cambia con el Real Decreto-ley 6/20232.- 3. ¿Qué cambia con el Real Decreto-ley 6/2023? II. EL PRIMER EMPLAZAMIENTO O CITACIÓN DEL DEMANDADO: ¿EN PAPEL O DE FORMA ELECTRÓNICA?- 1. Antes del Real Decreto-ley 6/2023.- 2. En la normativa proyectada y en el Real Decreto-ley 6/2023.- A) Del papel al formato electrónico.- B) Hablemos de garantías: garantías de lege ferenda.- 3. En la jurisprudencia.- III. CONCLUSIONES.

I. SUJETOS OBLIGADOS Y NO OBLIGADOS A RELACIONARSE ELECTRÓNICAMENTE CON LA ADMINISTRACIÓN DE JUSTICIA.

1. Introducción.

La pandemia del COVID-19 ha demostrado que los medios electrónicos son muy eficaces y eficientes y muy especialmente en lo que a actos de comunicación se refiere. Incluso antes de la pandemia se utilizaban los medios electrónicos para determinados actos de comunicación en los procesos judiciales[1].

En este sentido basta recordar que el art. 152 de la vigente Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil (en adelante, LEC), sobre la "forma de los actos de comunicación", en su apartado 2 ya establecía antes de la pandemia desde la Ley 42/2015, de 5 de octubre, de reforma de la LEC[2], que "los actos de comunicación se practicarán por medios electrónicos cuando los sujetos intervinientes en un proceso estén obligados al empleo de los sistemas telemáticos o electrónicos existentes en la Administración de Justicia conforme al artículo 273, o cuando aquéllos, sin estar obligados, opten por el uso de esos medios, con sujeción, en todo caso, a las disposiciones contenidas en la normativa reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia" (previsión plenamente aplicable desde el 1 de enero de 2017, conforme a su Disposición final duodécima, apartado 2, 2º), como ha venido siendo la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de información y la comunicación en la Administración de Justicia[3] (TIC), derogada por el reciente

1 Recordemos que las clases de actos de comunicación se regulan en el art. 149 LEC, precepto que recoge las notificaciones, emplazamientos, citaciones, requerimientos, mandamientos y oficios. A estos tipos hay que añadir otro, aunque el legislador no lo haya incluido en dicho precepto: los exhortos, a que se refieren los arts. 171 y ss. LEC, mediante los cuales un órgano jurisdiccional solicita auxilio judicial a otro órgano jurisdiccional.

2 Esta Ley pretendió "generalizar y dar mayor relevancia al uso de los medios telemáticos o electrónicos, otorgando carácter subsidiario al soporte papel", con la finalidad de conseguir "una mayor eficacia y eficiencia en la tramitación de los procedimientos" y un "ahorro de costes al Estado y a los ciudadanos" (párrafo 3º del apartado I de su Preámbulo).

3 Este mismo apartado 2 del art. 152 LEC excepcionaba y matizaba en su párrafo 2º: "No obstante, los actos de comunicación no se practicarán por medios electrónicos cuando el acto vaya acompañado de elementos

• Diana Marcos Francisco
Profesora Titular de Derecho procesal, Universidad Católica de Valencia San Vicente Mártir.
Correo electrónico: diana.marcos@ucv.es

Real Decreto-ley 6/2023, de 19 de diciembre, por el que se aprueban medidas urgentes para la ejecución del Plan de Recuperación, Transformación y Resiliencia en materia de servicio público de justicia, función pública, régimen local y mecenazgo (*vid.* su Disposición derogatoria única)[4]. Y no olvidemos que la LEC tiene carácter supletorio y se aplica en defecto de regulación en las leyes reguladores de los demás órdenes jurisdiccionales, es decir, de los procesos penales, contencioso-administrativos, laborales y militares (art. 4 LEC).

En la misma línea el párrafo 1º del art. 271 de la vigente Ley Orgánica 6/1985, del 1 de julio, del Poder Judicial[5] (sucesivamente, LOPJ), desde la reforma operada por la LO 4/2018, de 28 de diciembre, postula:

"Los actos de comunicación se practicarán por medios electrónicos cuando los sujetos intervinientes en un proceso estén obligados al empleo de los sistemas telemáticos o electrónicos existentes en la Administración de Justicia conforme a lo establecido en las leyes procesales y en la forma que estas determinen.

Cuando los sujetos intervinientes en un proceso no se hallen obligados al empleo de medios electrónicos, o cuando la utilización de los mismos no fuese posible, los actos de comunicación podrán practicarse por cualquier otro medio que permita la constancia de su práctica y de las circunstancias esenciales de la misma según determinen las leyes procesales".

2. Lo que no cambia con el Real Decreto-ley 6/2023.

¿Y quiénes son los sujetos obligados y no obligados a usar medios electrónicos de acuerdo con el art. 273 LEC? Según éste, están obligados los profesionales de la justicia (apartado 1) y, en todo caso, los siguientes sujetos (apartado 3)[6]:

que no sean susceptibles de conversión en formato electrónico o así lo disponga la ley". Y en su párrafo 3º rezaba: "El destinatario podrá identificar un dispositivo electrónico, servicio de mensajería simple o una dirección de correo electrónico que servirán para informarle de la puesta a su disposición de un acto de comunicación, pero no para la práctica de notificaciones. En tal caso, con independencia de la forma en que se realice el acto de comunicación, la oficina judicial enviará el referido aviso. La falta de práctica de este aviso no impedirá que la notificación sea considerada plenamente válida". El art. 152.2 ha sido modificado por el Real Decreto-ley 6/2023, de 19 de diciembre, por el que se aprueban medidas urgentes para la ejecución del Plan de Recuperación, Transformación y Resiliencia en materia de servicio público de justicia, función pública, régimen local y mecenazgo (*vid.* su artículo 103, punto veintitrés) en los términos que infra se indicarán.

4 Dicho Real Decreto-ley ha sido convalidado por el Pleno del Congreso de los Diputados el 10 de enero del presente año, que ha acordado por mayoría tramitarlo como proyecto de ley por el procedimiento de urgencia.

5 Repárese en que fue la LOPJ (art. 230) la que antes de la LEC, tras la reforma operada por la LO 16/1994, de 8 de noviembre, hacía referencia al posible uso de TIC por juzgados y tribunales en el desarrollo de sus funciones.

6 Los apartados 1 a 3 del art. 273 LEC no han sido modificados por el RD-ley 6/2023, pero sí lo ha sido el apartado 4. Los cambios consisten en: 1) Precisar en el párrafo 1º que "el escrito principal deberá incorporar firma electrónica"; 2) Eliminar del 2º párrafo -ésta es la modificación más relevante- la exigencia de presentar en soporte papel en los tres días siguientes a la presentación de los documentos por vía telemática o electrónica, copias de los documentos que dan lugar al primer emplazamiento, citación o

"a) Las personas jurídicas.

b) Las entidades sin personalidad jurídica[7].

c) Quienes ejerzan una actividad profesional para la que se requiera colegiación obligatoria para los trámites y actuaciones que realicen con la Administración de Justicia en ejercicio de dicha actividad profesional.

d) Los notarios y registradores.

e) Quienes representen a un interesado que esté obligado a relacionarse electrónicamente con la Administración de Justicia.

f) Los funcionarios de las Administraciones Públicas para los trámites y actuaciones que realicen por razón de su cargo"[8].

Sin embargo, "en principio" no son sujetos obligados las personas físicas que en el proceso judicial no actúen representadas por procurador (así se desprende del art. 273.2 LEC en relación con el citado art. 273.3 LEC), porque así lo han decidido

requerimiento del demandado o ejecutado (antes había que presentar tantas copias literales como partes, evitando así el coste de dichas copias a cargo de la Administración de Justicia); 3) y en recoger en el nuevo párrafo 2º la siguiente previsión: "Si se considera de interés, el escrito principal podrá hacer referencia a los documentos adicionales, siempre y cuando exista una clave que relacione esa referencia de manera unívoca por cada uno de los documentos, y, a su vez, asegure de manera efectiva su integridad".

7 La Ley 42/2015 también modificó la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de información y la comunicación en la Administración de Justicia, indicando en su art. 33.1, 2º la posibilidad de "establecer legal o reglamentariamente la obligatoriedad de comunicarse con ella utilizando solo medios electrónicos cuando se trate de personas jurídicas o colectivos de personas físicas que por razón de su capacidad económica o técnica, dedicación profesional u otros motivos acreditados tengan garantizado el acceso y disponibilidad de los medios tecnológicos precisos". Con independencia de que llamaba la atención que esta regulación no fuera coincidente con la introducida por igual Ley 42/2015 en el art. 273.3 LEC (al establecer, sin excepción alguna, la obligatoriedad para personas jurídicas y entes sin personalidad), poco después se aprobó el Real Decreto 1065/2015, de 27 de noviembre, sobre comunicaciones electrónicas en la Administración de Justicia en el ámbito territorial del Ministerio de Justicia y por el que se regula el sistema LexNET, cuyo art. 4 también introducía la obligatoriedad de las personas jurídicas y entidades sin personalidad de relacionarse por canales electrónicos con la Administración (el art. 4, en cuanto a los sujetos obligados, es una fiel reproducción del art. 273.3).

8 La regulación en este punto es igual a la propia del procedimiento administrativo recogida en el art. 14.2 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, que establece como sujetos obligados a relacionarse telemáticamente con las Administraciones Públicas a:
"a) Las personas jurídicas.
b) Las entidades sin personalidad jurídica.
c) Quienes ejerzan una actividad profesional para la que se requiera colegiación obligatoria, para los trámites y actuaciones que realicen con las Administraciones Públicas en ejercicio de dicha actividad profesional. En todo caso, dentro de este colectivo se entenderán incluidos los notarios y registradores de la propiedad y mercantiles.
d) Quienes representen a un interesado que esté obligado a relacionarse electrónicamente con la Administración.
e) Los empleados de las Administraciones Públicas para los trámites y actuaciones que realicen con ellas por razón de su condición de empleado público, en la forma en que se determine reglamentariamente por cada Administración".

en procesos en que la intervención de dicho profesional no es obligatoria[9], se sobreentiende (*vid.* art. 23.2 LEC, sobre los casos en que no es obligatoria la intervención del procurador en los procesos civiles). Esto mismo se desprendía de los arts. 33.1[10] y 36.1[11] de la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia y se desprende ahora de los arts. 32.1[12] y 33.1[13] del Real Decreto-ley 6/2023.

Y digo "en principio" porque ex art. 32.1 in fine del Real Decreto-ley 6/2023 (antes, del art. 33.1, 2º párrafo de la Ley 18/2011) se infiere la posibilidad de que excepcionalmente se establezca la obligación de comunicarse electrónicamente con la Administración de Justicia a ciertos colectivos de personas físicas que "tengan garantizado el acceso y disponibilidad de los medios tecnológicos precisos"[14] (aunque el Real Decreto-ley 6/2023 haya omitido la referencia expresa

9 Convenimos con Cotino Hueso y Montesinos García en que, si el ciudadano decide valerse de postulación procesal pese a no ser obligatoria, la relación de los profesionales con la Administración deberá ser electrónica (*vid.* "Derechos de los ciudadanos y los profesionales en las relaciones electrónicas con la Administración de Justicia", en AA.VV.: *Las Tecnologías de la Información y la Comunicación en la Administración de Justicia. Análisis sistemático de la Ley 18/2011, de 5 de julio*, (coord. por E. Gamero Casado y J. Valero Torrijos), Thomson Reuters Aranzadi, Cizur Menor (Navarra), 2012, p. 195).

10 El tenor literal era el siguiente:
"Los ciudadanos podrán elegir en todo momento la manera de comunicarse con la Administración de Justicia, sea o no por medios electrónicos.
Asimismo, se podrá establecer legal o reglamentariamente la obligatoriedad de comunicarse con ella utilizando solo medios electrónicos cuando se trate de personas jurídicas o colectivos de personas físicas que por razón de su capacidad económica o técnica, dedicación profesional u otros motivos acreditados tengan garantizado el acceso y disponibilidad de los medios tecnológicos precisos".

11 Según este precepto, "la iniciación de un procedimiento judicial por medios electrónicos por los ciudadanos, «en aquellos juicios en los que pueden comparecer de forma personal y directa por no ser preceptiva la asistencia letrada ni la representación por procurador conforme a lo establecido en las normas de procedimiento», requerirá la puesta a disposición de los interesados de los correspondientes modelos o impresos normalizados en la sede judicial electrónica, que deberán ser accesibles sin otras restricciones tecnológicas que las estrictamente derivadas de la utilización de estándares y criterios de comunicación y seguridad aplicables de acuerdo con las normas y protocolos nacionales e internacionales" (el entrecomillado es mío).

12 Reza esta norma lo siguiente: "La presentación de escritos y documentos, los actos de comunicación, la consulta de expedientes judiciales o de su estado de tramitación, cualesquiera otras actuaciones y todos los servicios prestados por la Administración de Justicia se llevarán a cabo por medios electrónicos. Se exceptúa de lo anterior a las personas físicas que, conforme a las leyes procesales, no actúen representadas por Procurador. En estos casos, las personas físicas podrán elegir, en todo momento, si se comunican con la Administración de Justicia a través de medios electrónicos o no, salvo en aquellos supuestos en los que expresamente estén obligadas a relacionarse a través de tales medios".

13 Conforme a este precepto, "el inicio por los ciudadanos y ciudadanas de un «procedimiento judicial por medios electrónicos en aquellos asuntos en los que no sea precisa la representación procesal ni la asistencia letrada», requerirá la puesta a disposición de los interesados, en la sede judicial electrónica, de los correspondientes modelos o impresos normalizados, que deberán ser accesibles sin otras restricciones tecnológicas que las estrictamente derivadas de la utilización de estándares y criterios de comunicación y seguridad aplicables de acuerdo con las normas y protocolos nacionales e internacionales" (el entrecomillado es mío).

14 Lo mismo sucede en el ámbito del procedimiento administrativo, en el que en principio las personas físicas pueden decidir cómo comunicarse con la Administración Pública (si por los medios tradicionales -papel- o electrónicos), salvo que estén obligadas a relacionarse por medios electrónicos (art. 14.1 de la citada Ley 39/2015, de 1 de octubre) porque así se establezca reglamentariamente "para determinados procedimientos y para ciertos colectivos de personas físicas que por razón de su capacidad económica, técnica, dedicación profesional u otros motivos quede acreditado que tienen acceso y disponibilidad de los medios electrónicos necesarios" (art. 14.3 de igual Ley). De ahí, a modo de ejemplo, los Reglamentos de colegios profesionales que contemplan las comunicaciones telemáticas con los colegiados (como es el Reglamento 1/2016 del Sistema Colegial de Comunicación Telemática, del Ilustre Colegio de Procuradores

a tal garantía a la que sí aludía la Ley 18/2011, deben igualmente observarse para que pueda regir la obligatoriedad, so pena de afectar a derechos fundamentales como la igualdad y la tutela judicial efectiva en sus distintas vertientes, tales como el acceso a la justicia o la prohibición de indefensión). De la misma forma, del citado art. 273.2 LEC también se desprende la posibilidad de que haya personas físicas obligadas a relacionarse con la Administración de Justicia por medios electrónicos.

Pues bien, de las reformas legales llevadas a cabo por la Ley 42/2015 en materia de sujetos obligados a relacionarse electrónicamente con la Administración de Justicia, la más controvertida y discutible fue la atinente a su imposición a las personas jurídicas, entes sin personalidad y ciertos colectivos de personas físicas[15].

Y ello por supuesto sin perjuicio de que las personas físicas que no actúen representadas por procurador ostentan el derecho a actuar ante la Administración de Justicia por medios electrónicos, por lo que podrán relacionarse con ella por estos medios si así lo desean (*vid.* los citados art. 32.1 del Real Decreto-ley 6/2023 y art. 273.2 LEC). En este sentido el art. 5.2 del repetido Real Decreto-ley 6/2023 reconoce a los "ciudadanos y ciudadanas"[16], como manifestaciones concretas del derecho a emplear los medios electrónicos (reconocido expresamente en el apartado 1 del mencionado art. 5), los derechos -entre otros- a elegir el canal o vía electrónica (internet, videoconferencia, servicios de telefonía fija o móvil, etc.), de entre todas las disponibles, mediante el que relacionarse con la Administración de Justicia (letra e[17]) y a elegir los programas o sistemas de información con los que relacionarse con la Administración, que empleen estándares abiertos[18] o sean de uso generalizado "y, en todo caso, siempre que sean compatibles con los que

de Madrid) o, inclusive, el uso de medios telemáticos en la tramitación de solicitudes de incorporación a tales colegios (como sucede en el Ilustre Colegio de Abogados de Sevilla).
No obstante, la influencia de la STS 6 mayo 2021 (Roj: STS 1587/2021) se está empezando a notar y, en ese sentido, se están anulando distintas normas reglamentarias que imponen la obligación de relacionarse electrónicamente con las Administraciones Públicas al no constatar suficientemente "la razón que le lleva a considerar que las personas a las que se impone la obligación tienen capacidad económica, técnica, dedicación profesional u otro motivo que determinan que tienen acceso y disponibilidad de los medios electrónicos necesarios" (*vid.* Sánchez Lamelas, A.: "La reciente jurisprudencia sobre la obligación de utilizar medios electrónicos en las relaciones administrativas", *Revista de Administración Pública*, 2023, núm. 220, pp. 215 y 216, donde cabe encontrar varios ejemplos de normas anuladas).

15 Un interesante estudio crítico al respecto, aunque con respecto al procedimiento administrativo, puede verse en Gamero Casado, E.: "Panorámica de la Administración electrónica en la nueva legislación administrativa básica", *Revista Española de Derecho Administrativo,* 2016, núm. 175, pp. 1-6 (edición electrónica).

16 En la línea de las últimas tendencias legislativas las reformas operadas por el Real Decreto-ley 6/2023 emplean un lenguaje inclusivo (que, por cierto, yo no empleo en el presente trabajo para evitar una mayor extensión). Aunque llama la atención que algunos preceptos, supongo que por descuido, únicamente hagan referencia al género masculino.

17 El tenor literal de la letra e) es coincidente con el del art. 4.2.a) de la derogada Ley 18/2011, de 5 de julio, que a su vez reproducía, en el concreto ámbito de la Administración de Justicia, los términos del art. 6.2.a) de la derogada Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

18 El Anexo de Definiciones del Real Decreto-ley 6/2023 define el "estándar abierto" como "aquel que reúna las siguientes condiciones: que sea público y su utilización sea disponible de manera gratuita o a un coste que no suponga una dificultad de acceso y cuyos uso y aplicación no estén condicionados al pago de un derecho de propiedad intelectual o industrial".

dispongan los órganos judiciales y se respeten las garantías y requisitos previstos en el procedimiento de que se trate" (letra k[19]). Tales derechos presentan una dicción inconcreta para dar cabida a posibles evoluciones de las TIC y la existencia de nuevos canales de comunicación o programas informáticos[20].

Lo anteriormente indicado resultaba -y resulta- plenamente aplicable en el ámbito de la jurisdicción social. Y ello, ya no por el mencionado carácter supletorio de la LEC, sino por la remisión expresa que la Ley 36/2011, de 10 de octubre, reguladora de la Jurisdicción Social (en lo sucesivo, LJS), hacía a dicha LEC en su art. 53.1 -y sigue haciendo tras el Real Decreto-ley 6/2023- sobre la forma de efectuar los actos de comunicación "con las especialidades previstas en esta Ley (…)"; remisión que también existía -y sigue existiendo, si bien con algún cambio en el tenor literal, señalado infra- con respecto a las comunicaciones electrónicas (art. 56.5 LJS).

3. ¿Qué cambia con el Real Decreto-ley 6/2023?

Como he adelantado en la nota 3 a pie de página, el Real Decreto-ley 6/2023 ha modificado el art. 152 LEC, dentro de toda una serie de modificaciones que forman parte de un conjunto de medidas de eficiencia digital y procesal del servicio público de justicia[21] (recogidas en su Libro Primero). Por lo que respecta a la entrada en vigor de dichas medidas (*vid.* su Disposición final novena), las medidas de eficiencia digital lo hicieron a los veinte días de su publicación en el BOE (20 de diciembre de 2023), esto es, el 9 de enero de 2024. Ello sin perjuicio de que aún no sean plenamente aplicables en las Comunidades Autónomas que no dispongan de los servicios y sistemas tecnológicos oportunos o, disponiendo de ellos, no hayan llevado a cabo la correspondiente integración con los estatales del Ministerio de la Presidencia, Justicia y Relaciones con las Cortes, lo que en todo caso deberá haberse realizado a más tardar el 30 de noviembre del próximo año 2025[22]. Y, por lo que respecta a las medidas de eficiencia procesal, recogidas en el

19 Salvo el nuevo lenguaje inclusivo, el tenor literal de la letra k) es coincidente con el del art. 4.2.i) de la derogada Ley 18/2011, de 5 de julio, que a su vez acogía la primera parte de la regulación del art. 6.2.k) de la derogada Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

20 A la luz de lo previsto en el art. 6.2.k) de la Ley 11/2007 y art. 4.2.i) de la Ley 18/2011 autores como González De la Garza, L. M.: *Justicia electrónica y garantías constitucionales. Comentario a la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia*, La Ley, Las Rozas (Madrid), 2012, pp. 83 y 84, hablaban de errores injustificables y de una posible regulación discriminatoria para los ciudadanos, dada la diferente regulación aplicable en función de la Administración con la que se relacionasen. Tras la derogación de la Ley 11/2007, de 22 de junio, por la Ley 39/2015, de 1 de octubre, esta Ley introdujo la comunicación con las Administraciones Públicas "a través de un Punto de Acceso General electrónico de la Administración" (*vid* su art. 13, letra a), mientras que el Real Decreto-ley 6/2023 mantiene los términos de la Ley 18/2011.

21 Las mismas tienen su origen en los decaídos Proyectos de Ley de eficiencia procesal y digital del servicio público de justicia, aprobados en Consejo de Ministros el 12 de abril de 2022 y el 19 de julio de 2022, respectivamente. Dichos Proyectos decayeron tras la disolución de las Cortes decretada por el Consejo de Ministros Extraordinario en mayo de 2023.

22 Esperemos que el problema de la falta de interoperabilidad, que ya estaba presenta bajo la vigencia de la Ley 18/2011, de 5 de julio (Ley que en su Disposición adicional tercera otorgaba un plazo de cuatro años

Título VIII del Libro Primero, entrarán en vigor a los tres meses de su publicación en el BOE, es decir, el 20 de marzo de 2024[23].

Con la aludida modificación del art. 152.2 LEC[24], que acoge literalmente -salvo un par de palabras, que no cambian su sentido- los términos propuestos por el Proyecto de Ley de medidas de eficiencia procesal del servicio público de justicia, los actos procesales se deberán comunicar electrónicamente por la Administración de Justicia, no sólo cuando los sujetos que intervengan estén obligados a relacionarse con ella por tales medios y cuando, sin estar obligados, opten por su uso, sino también cuando, no siendo sujetos legalmente obligados, "los intervinientes se hayan obligado contractualmente a hacer uso de los medios electrónicos existentes en la Administración de Justicia para resolver los litigios que se deriven de esa relación jurídica concreta que les vincula, debiendo indicar los medios de los que pretenden valerse. En los contratos de adhesión en los que intervengan consumidores y usuarios, el acto de comunicación se practicará conforme a lo dispuesto para aquellos supuestos en los que los intervinientes no estén obligados a relacionarse electrónicamente con la Administración de Justicia, siendo esta última forma la que tendrá validez a efectos de cómputo de plazos".

Esta es una de las tres novedades fundamentales introducidas en el art. 152.2 LEC, que atañe al ámbito subjetivo de los actos de comunicación electrónicos: la obligatoriedad de relacionarse electrónicamente con la Administración puede tener un origen legal o convencional, esto es, derivar tanto de la ley como de un contrato. Estamos ante una previsión legal -la del posible origen convencional- de dudosa practicidad: me resulta difícil creer que las personas físicas que firmen un contrato vayan a pensar en incluir una cláusula en el mismo (o en acordarlo como documento independiente) sobre la forma de relacionarse con la Administración de Justicia en caso de surgir un conflicto entre ellas que se lleve a los tribunales. Pese a ello, la nueva norma piensa también en el hipotético caso de que dicha cláusula se incluya en contratos de adhesión celebrados con consumidores, en

para que los diferentes sistemas de gestión procesal de las distintas CCAA fueran interoperables y que fue incumplido), esta vez se solucione. A este y otros problemas técnicos y económicos existentes para conseguir un "papel cero" aluden Cerdá Meseguer, J. I.: "Hacia una administración de justicia plenamente electrónica: disfunciones normativas y jurisprudenciales", AA.VV.: *Modernización digital e innovación en la Administración de Justicia* (coord. por M. F. Gómez Manresa y M. Fernández Salmerón), Thomson Reuters Aranzadi, Cizur Menor (Navarra), 2019, pp. 378-381, y Cernada Badía, R.: "«LexNET» o la selección natural en el foro del siglo XXI", AA.VV.: *Modernización digital e innovación en la Administración de Justicia* (coord. por M. F. Gómez Manresa y M. Fernández Salmerón), Thomson Reuters Aranzadi, Cizur Menor (Navarra), 2019, pp. 418-425.

23 Nótese que el presente trabajo ha sido finalizado en febrero de 2024, lo que justifica la utilización del tiempo verbal futuro.

24 El Real Decreto-ley 6/2023, acogiendo los cambios que planteaba el Proyecto de Ley de medidas de eficiencia procesal, además de modificar el art. 152.2 LEC añade un apartado 6 en este precepto con el siguiente tenor: "Si se practicase un mismo acto de comunicación dos o más veces, tendrá eficacia a efectos procesales la primera fecha en que se hubiese verificado, con independencia del medio que se hubiere empleado, a salvo los casos en los que las leyes procesales prevean expresamente la posibilidad de que una resolución se comunique más de una vez, en cuyo caso tendrá los efectos que dichas leyes determinen".

cuyo caso contempla como solución pro consumatore tener dicha cláusula por no puesta y, por ende, permitiendo a dichos consumidores decidir si desean o no relacionarse electrónicamente.

Si nos centramos en el ámbito laboral, al respecto hay que traer a colación la reforma que el Real Decreto-ley 6/2023 hace del art. 56.5[25] LJS. Aunque en lo esencial el contenido de dicho precepto se mantiene (la remisión a la LEC), el cambio consiste en prohibir la aludida obligación de origen convencional en contratos de trabajo.

En definitiva, como adelantaba el apartado X de la Exposición de Motivos del Proyecto de Ley de medidas de eficiencia procesal del servicio público de justicia, "con dichas modificaciones, los únicos que no están obligados a comunicarse electrónicamente con la Administración de Justicia son las personas físicas que no se hayan obligado previa y contractualmente a hacerlo o que no hayan optado voluntariamente por comunicarse en dicha forma, exceptuándose la obligación contractual en determinados supuestos" (dichos casos son los contratos de adhesión con consumidores, por no ser sus condiciones o clausulado negociado, sino impuesto por las empresas; así como los contratos con trabajadores, en los que sabemos que el trabajador poco puede negociar en la práctica en la mayoría de los casos, dada la situación de superioridad de la empresa y la necesidad de trabajar).

La segunda novedad fundamental introducida en el art. 152.2 LEC atañe al alcance o ámbito objetivo de los actos de comunicación[26], estableciéndose la obligatoriedad de practicar electrónicamente todos los actos de comunicación, aunque vayan acompañados de elementos no susceptibles de conversión en medios electrónicos (antes de la reforma, en estos últimos casos o cuando lo dispusiera la ley, la comunicación de los actos procesales debía hacerse de forma tradicional en papel). Ahora bien, será necesario indicar cómo se entregarán dichos elementos, matizándose que "si este acto de comunicación diese lugar a la apertura de un plazo procesal, este comenzará a computar desde el momento en que consten recibidos por el destinatario todos los elementos que componen el acto".

25 Su tenor ha pasado a ser el siguiente: "Cuando se trate de personas que estén legalmente obligadas a relacionarse electrónicamente con la Administración de Justicia o que hayan optado por la utilización de estos medios, la comunicación se realizará conforme a lo establecido en el artículo 162 de la Ley 1/2000, de 7 de enero, sin que quepa en el orden jurisdiccional social la posibilidad de obligar contractualmente al trabajador a dicha relación electrónica".

26 A la tercera me referiré infra en el epígrafe II, 2., B).

II. EL PRIMER EMPLAZAMIENTO O CITACIÓN DEL DEMANDADO: ¿EN PAPEL O DE FORMA ELECTRÓNICA?

Pues bien, tras efectuar la anterior introducción acerca de los sujetos que deben y los que pueden relacionarse electrónicamente con la Administración de Justicia, lo que me planteé cuando impartí la ponencia en que trae base el presente trabajo[27], partiendo de la enorme efectividad y eficiencia de los medios electrónicos, es hasta qué punto sería posible y conveniente ampliar o extender el uso obligatorio de estos medios virtuales a los primeros emplazamientos de los aludidos sujetos obligados a usar dichos medios virtuales[28] (en concreto, a las personas jurídicas y entes sin personalidad), para personarse y actuar dentro de un plazo en un proceso judicial (pensemos en la notificación de una demanda civil de juicio verbal o juicio ordinario al demandado, emplazándole para contestar a la misma en el plazo de diez o veinte días, respectivamente) y a las primeras citaciones de los repetidos sujetos obligados a usar dichos medios virtuales, para comparecer y actuar en determinado lugar, fecha y hora en un proceso judicial (pensemos en la citación para los actos de conciliación y juicio en un proceso laboral)[29].

Sabemos que hoy en día en el ámbito administrativo son muchas, y cada vez más, las personas (incluyendo las personas físicas), que se comunican con las Administraciones Públicas por medios electrónicos (pensemos p. ej. en el proceso de solicitud de admisión del alumnado en los centros públicos y en las enseñanzas

27 *Vid.* supra, nota a pie *.

28 Tras la reforma operada por el Real Decreto-ley 6/2023, dicha cuestión habría que circunscribirla a los sujetos obligados legalmente, no a los que hayan decidido obligarse convencionalmente.

29 Nótese que, aunque el presente trabajo se circunscribe a los aludidos actos de comunicación (primer emplazamiento o citación del demandado), las consideraciones que se efectúan son igualmente predicables con respecto a todo primer acto de comunicación con el demandado o, inclusive, con el ejecutado cuando el proceso ejecutivo no vaya precedido de un proceso declarativo previo. Así, pensemos en el primer requerimiento de este conforme al art. 581 LEC, que decreta el Letrado de la Administración de Justicia y que se notifica junto con el auto despachando ejecución. Y es que, tras la reforma operada por el Real Decreto 6/2023, el nuevo art. 582 LEC permite efectuar el requerimiento de pago "[a] través de la sede judicial electrónica en el caso de que el ejecutado esté obligado a intervenir con la Administración de Justicia a través de medios electrónicos". O pensemos en los no pocos procedimientos de ejecución hipotecaria contra personas jurídicas, dado que el 2º párrafo del art. 682.2, 2º LEC, tras la modificación realizada por el Real Decreto-ley 6/2023, dispone que "los actos de comunicación se practicarán siempre por medios electrónicos cuando sus destinatarios tengan obligación, legal o contractual, de relacionarse con la Administración de Justicia por dichos medios".
Las cosas no están tan claras con respecto al requerimiento de pago en un juicio monitorio porque, pese a que el art. 815 LEC ha sido modificado por el Real Decreto-ley 6/2023, sigue indicando que se notificará de acuerdo con lo previsto en el art. 161 LEC. En la medida en que el art. 815.1, 2º no se ha remitido al art. 162 (que es el que regula los actos de comunicación electrónicos) sino al 161, podría entenderse que estamos ante una excepción en la forma de practicar la primera comunicación al demandado (frente a la regla del carácter electrónico). Pero, como el art. 161.1 LEC, tras la reforma operada por el Real Decreto-ley 6/2023, habla de la posible entrega de la copia de la resolución o cédula "en la sede judicial electrónica" (además de la entrega en la sede del tribunal o en el domicilio personal), también podría entenderse que no estamos ante ningún supuesto excepcional. De lege ferenda convendría, pues, su aclaración.
Por lo que atañe al proceso cambiario, no ha sido modificada su normativa reguladora. Aunque hubiera sido deseable modificar el art. 821 y clarificar la posibilidad u obligatoriedad, según los casos, de requerir de pago por medios telemáticos, no parecen existir razones para pensar que este requerimiento en todo caso se va a seguir haciendo de forma tradicional (en papel).

concertadas de los centros privados de la Comunidad Valenciana que impartan enseñanzas de educación infantil, educación primaria, educación secundaria obligatoria y bachillerato[30]), siendo también lo normal en este ámbito que las Administraciones comuniquen electrónicamente a los interesados obligados a usar estos medios el inicio de un determinado procedimiento. Y también sabemos que en el ámbito procesal, sobre todo en el laboral, algunos juzgados, en virtud de lo contemplado en el art. 8.2 del Real Decreto 1065/2015, de 27 de noviembre, sobre comunicaciones electrónicas en la Administración de Justicia en el ámbito territorial del Ministerio de Justicia y por el que se regula el sistema LexNET, y del Acuerdo entre el Ministerio de Hacienda y Justicia, han hecho uso de la Dirección Electrónica Habilitada (DEH)[31] creada y empleada en el ámbito tributario, para efectuar allí el primer acto de comunicación con el demandado o ejecutado (fundamentalmente, en la citación para los actos de conciliación y juicio con ocasión de demandas interpuestas por trabajadores contra sus empresas).

Desde luego, no hay que perder de vista que, mientras los actos de comunicación electrónicos con los sujetos obligados al uso de estos medios telemáticos vienen siendo satisfactorios, no podemos decir lo mismo con respecto al "primer acto de comunicación al interesado por correo certificado o de forma personal (160 y 161 LEC), es decir, en las comunicaciones en papel, así como en la citación a testigos y requerimiento a terceros ajenos al proceso, sumado a aquellos procedimientos sin asistencia profesional preceptiva ni obligatoriedad de medios electrónicos, que exigen repetir constantemente la comunicación con el destinatario en soporte papel o su averiguación domiciliaria"[32]. Por ello en la praxis judicial hay Juzgados que

30 Si estamos al vigente Decreto 40/2016, de 15 de abril, del Consell, por el que se regula la admisión en los centros docentes públicos y privados concertados que imparten enseñanzas de Educación Infantil, Educación Primaria, Educación Secundaria Obligatoria y Bachillerato, su art. 26.1 contempla, tras la reforma operada por el Decreto 21/2022, de 4 de marzo, del Consell, la obligatoriedad de formular la solicitud de plaza de forma telemática mediante "la aplicación informática que establezca la Conselleria competente en materia de educación", aunque -eso sí- siempre garantizando "el acceso al procedimiento para aquellas personas que no dispongan de medios electrónicos o conocimientos suficientes para poder trabajar con la administración electrónica", esto es, permitiéndoles ser atendidos presencialmente en los centros escolares.
Un ejemplo en el ámbito de la Administración General del Estado es el de la obligatoriedad de presentar electrónicamente las solicitudes de evaluación de la actividad investigadora (para el reconocimiento de los conocidos sexenios de investigación) del profesorado universitario y personal investigador. *Vid.* el punto 5.2 de las Bases específicas del Anexo de la Resolución de 19 de diciembre de 2023, de la Secretaría General de Universidades, por la que se aprueba la convocatoria de evaluación de la actividad investigadora. Aunque dicha obligatoriedad trae causa en el art. 14.2.e) de la Ley 39/2015, de 1 de octubre, igualmente se debe observar por los profesores e investigadores de universidades o centros privados que soliciten la evaluación de su actividad investigadora en virtud de los convenios correspondientes.

31 Téngase en cuenta que la DEH ha dejado de estar disponible desde el 31 de diciembre de 2022, pudiendo accederse a las notificaciones y comunicaciones de la Agencia Tributaria mediante su Sede electrónica o la Dirección Electrónica Habilitada Única (DEHú), de acuerdo con lo establecido en el art. 42.5 del Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del del sector público por medios electrónicos (*vid.* https://sede.agenciatributaria.gob.es/Sede/informacion-importante.html, consultada el 15.09.23).

32 Gómez-Linacero Corraliza, A.: "Diálogos para el futuro judicial XL. Los actos de comunicación en el marco de la Justicia Digital" (coord. por A. Perea González), *Diario La Ley*, 1 marzo 2022, núm. 10019, p. 7 (edición electrónica).

han venido empleando las TIC incluso para realizar dichos actos de comunicación partiendo de la "lógica presunción de que los medios tecnológicos siempre van a favorecer una mayor optimización de recursos y un incremento de la velocidad en la tramitación de los procesos judiciales"[33].

Pero, ¿era y es posible jurídicamente efectuar las primeras comunicaciones de forma electrónica conforme a la legislación procesal? ¿Y es conveniente?

1. Antes del Real Decreto-ley 6/2023.

Como dije en mi ponencia, el art. 155.1 LEC contemplaba que, cuando se tratase del primer emplazamiento o citación del demandado, el acto de comunicación se debía practicar de forma personal en el domicilio del litigante demandado (de forma, por tanto, tradicional, en papel), ya fuese por correo certificado o telegrama con acuse de recibo (art. 160 LEC) o, en caso de resultar infructuosa la comunicación (art. 158 LEC), por entrega de cédula de emplazamiento o citación por funcionario o procurador (art. 161 LEC) y, subsidiariamente, por publicación edictal (art. 164 LEC). Por tanto, en la medida en que el art. 155.1 no establecía excepción alguna en su ámbito de aplicación subjetivo, aun siendo el demandado una persona jurídica o ente sin personalidad (sujetos obligados a relacionarse electrónicamente con la Administración de Justicia), su emplazamiento se debía realizar en su domicilio personal.

Otro precepto crucial que apuntaba a igual solución era el art. 273.4, 2º. Y es que si su tenor literal indicaba que "únicamente de los escritos y documentos que se presenten vía telemática o electrónica que den lugar al primer emplazamiento, citación o requerimiento del demandado o ejecutado, se deberá aportar en soporte papel, en los tres días siguientes, tantas copias literales cuantas sean las otras partes", de ello se desprendía que la presentación en papel obedecía a que tales primeros actos se iban a realizar de forma tradicional.

Pero, además de los reseñados arts. 155.1 y 273.4 LEC, había otros preceptos que apuntaban a la necesaria notificación "tradicional" de los primeros emplazamientos y citaciones. Así, dentro de las "excepciones establecidas en la ley" y los "demás supuestos previstos en las leyes" a que aluden, respectivamente, los apartados 1 y 4 del art. 135 LEC -que no se han modificado por el Real Decreto-ley 6/2023, a diferencia de los citados arts. 155.1 y 273.4- en que los escritos deben presentarse en soporte papel, cabía incluir los primeros emplazamientos

33 Fierro Rodríguez, D.: "La confirmada obligatoriedad del uso de la tecnología en la Administración de Justicia", *Legaltoday.com*, 15 diciembre 2021 (accesible en https://www.legaltoday.com/opinion/articulos-de-opinion/la-confirmada-obligatoriedad-del-uso-de-la-tecnologia-en-la-administracion-de-justicia-2021-12-15/, consultada el 21.10.23).

o citaciones del demandado[34]. También del art. 152.2 LEC y, en concreto, de su expresión "sujetos intervinientes en un proceso" -que sigue en su redacción-, cabía inferir que no surgía la obligación de relacionarse electrónicamente con la Administración hasta que el sujeto no se persone en el proceso[35]. A mayor abundamiento, en apoyo de esta postura cabía esgrimir el art. 155.4, 2º[36] LEC, en la medida en que se remitía al art. 158[37] LEC que, a su vez, se remitía al art. 161[38] LEC, que trataba la comunicación en papel por medio de copia de la resolución o de cédula. E, inclusive, era posible apoyarse en el art. 162.1, 2º LEC, que decía -y sigue diciendo tras el Real Decreto-ley 6/2023, si bien con un lenguaje inclusivo-, que los "profesionales y destinatarios obligados a utilizar estos medios, así como los que opten por los mismos, deberán comunicar a las oficinas judiciales el hecho de disponer de los medios antes indicados y la dirección electrónica habilitada a tal efecto"; lo cual es posible si se entiende que esta forma electrónica de practicar la comunicación procesal "solo es viable después de que las partes se hagan personado en el proceso. Precisamente al personarse, será el momento oportuno para que hagan esa comunicación los sujetos obligados a utilizar medios electrónicos"[39].

A idéntica conclusión cabía llegar en el orden jurisdiccional laboral si estábamos a la LJS, porque sabemos que dicha Ley en su art. 53.1 se remitía -y se sigue remitiendo tras el Real Decreto-ley 6/2023- a lo dispuesto en la LEC sobre la forma de efectuar los actos de comunicación "con las especialidades previstas en esta Ley, debiendo siempre agotarse todas las posibles vías existentes para lograr la efectividad de las notificaciones"; remisión que también existía -y sigue existiendo, si bien con algún cambio en el tenor literal- con respecto a las comunicaciones electrónicas (art. 56.5 LJS).

34 Entre otros, Cerdá Meseguer, J. I.: "La notificación electrónica de la demanda a personas jurídicas: ¿innovación tecnológica o indefensión?", *Diario La Ley*, 2019, núm. 9388, p. 7 (edición electrónica), quien también cita en apoyo de su postura otros preceptos como el art. 17.2, 2º in fine del RD 1065/2015; Moreno García, L.: "Las notificaciones procesales por medios electrónicos a la luz de la reciente constitucional", en AA.VV.: *La Justicia digital en España y la Unión Europea: situación actual y perspectivas de futuro* (dir. por J. Conde Fuentes y G. Serrano Hoyo), Atelier, Barcelona, 2019, p. 63.

35 En este sentido, Ariza Colmenarejo, M. J.: "Incidencia de las comunicaciones electrónicas en la tutela judicial", en AA.VV.: *Aciertos, excesos y carencias en la tramitación del proceso* (dir. por J. F. Herrero Perezagua y J. López Sánchez), Atelier, Barcelona, 2020, p. 146; Cerdá Meseguer, J. I.: "La notificación", cit., pp. 3 y 4 (edición electrónica).

36 Disponía esta norma antes de la reforma operada por el Real Decreto-ley 6/2023 que "si la comunicación tuviese por objeto la personación en juicio o la realización o intervención personal de las partes en determinadas actuaciones procesales y no constare la recepción por el interesado, se estará a lo dispuesto en el artículo 158".

37 Dicho precepto ha sido modificado por el Real Decreto-ley 6/2023 para limitar la comunicación mediante entrega a los casos en que "el destinatario del acto de comunicación no venga obligado legal o contractualmente a relacionarse por medios electrónicos con la Administración de Justicia".

38 El Real Decreto-ley 6/2023 ha añadido en su primer apartado la posible entrega virtual "en la sede judicial electrónica".

39 Cubillo López, I. J.: *Actos procesales, comunicación procesal y medios electrónicos*, La Ley, Madrid, 2019, p. 164.

Sin embargo, había otros preceptos en la LEC de los que podría entenderse lo contrario (la posible notificación virtual de los primeros actos de comunicación). Así, a la luz de lo regulado en el art. 135.1, 1º LEC -apartado que no ha sido modificado por el Real Decreto-ley 6/2023- podía entenderse que los emplazamientos o citaciones a que alude el art. 155.1 sólo eran aplicables a quienes no están obligados a relacionarse electrónicamente con la Administración de Justicia. En efecto, en la medida en que el art. 135.1, 1º LEC prevé que cuando las oficinas judiciales y los sujetos que intervengan en un proceso deban comunicarse electrónicamente con la Administración de Justicia o, sin estar obligados, opten por esos medios de comunicación conforme al art. 273, "remitirán y «recibirán» todos los «escritos, iniciadores» o no, y demás documentos" (el entrecomillado es mío) a través de dichos sistemas electrónicos, cabía interpretar que, aun tratándose de actos iniciadores del proceso, era posible emplazar y citar electrónicamente al demandado[40].

Dado que el aparentemente "inequívoco" art. 155 LEC no lo era tanto a la luz de otras normas como la indicada, existiendo una contradicción conducente a una diferente interpretación en los tribunales y a una distinta forma de practicar los actos de comunicación, resultaba necesario una reforma legal para aclarar la voluntad del legislador y garantizar la seguridad jurídica (art. 9.3 CE).

2. En la normativa proyectada y en el Real Decreto-ley 6/2023.

A) Del papel al formato electrónico.

Desde luego lo más eficiente y coherente con la aludida obligación de relacionarse las personas jurídicas y los entes sin personalidad por medios electrónicos es que también la primera comunicación con dichas partes, aún no personadas, lo sea de esta forma, y no que en todo caso deba hacerse por remisión al domicilio de los litigantes. De ahí que ya se advirtiera de la existencia de iniciativas reformadoras para permitir que la notificación inicial pudiera practicarse en la dirección electrónica habilitada[41] y que, en esta línea del decaído Proyecto de

40 Para autores como Valero Canales, el art. 155 LEC no era óbice para que la primera comunicación a las partes procesales se realizara por medios electrónicos. Dicho autor, aunque no alude al citado art. 135 LEC, argumenta su postura en toda una serie de motivos (entre ellos, acudiendo a una interpretación sistemática del ordenamiento jurídico y la pretendida finalidad del legislador, con las reformas realizadas, de gestionar electrónicamente los procesos judiciales). Para más detalles *vid.* "Consideraciones procesales del expediente judicial electrónico", AA.VV.: *Modernización digital e innovación en la Administración de Justicia* (coord. por M. F. Gómez Manresa y M. Fernández Salmerón), Thomson Reuters Aranzadi, Cizur Menor (Navarra), 2019, pp. 361-363, donde se citan distintas resoluciones de la jurisprudencia menor en distinto sentido. Así, abogando por la postura del autor pueden verse las SSTSJ de Castilla-León 1398/2018, de 13 de abril, y 1271/2018, de 18 de abril; el AAP de Murcia (Sección 4ª) de 8 de marzo de 2018; el AAP de Murcia (Sección 5ª) 792/2018, de 17 de abril; y la SAP de Palma de Mallorca (Sección 3ª) 1740/2018 de 26 de abril. En sentido contrario, la STSJ de Murcia 426/2018, de 3 de mayo.

41 Herrero Perezagua, J. F.: "Crisis y medios tecnológicos: razón y ocasión para la reforma del proceso", en AA.VV.: *Proceso civil y nuevas tecnologías* (dir. por J. Sigüenza López), Thomson Reuters Aranzadi, Cizur Menor (Navarra), 2021, p. 126.

Ley de medidas de eficiencia procesal del servicio público de justicia, reformara el art. 155 LEC pasando su primer apartado a tener los siguientes términos:

"Cuando la parte no representada por procurador o procuradora venga obligada legal o contractualmente a relacionarse electrónicamente con la Administración de Justicia, el acto de comunicación se realizará por medios electrónicos de conformidad con el artículo 162 de esta ley.

No obstante, si el acto de comunicación tuviese por objeto el primer emplazamiento o citación, o la realización o intervención personal de las partes en determinadas actuaciones procesales y transcurrieran tres días sin que el destinatario acceda a su contenido, se procederá a su publicación por la vía del Tablón Edictal Judicial Único conforme a lo dispuesto en el artículo 164.

Además, en todo caso, también podrá practicarse mediante entrega de la copia de la resolución si el obligado se personase en la sede del órgano judicial, dejando constancia de ello en la diligencia que se extienda".

La anterior normativa proyecta reproducida ha sido acogida plenamente por el Real Decreto-ley 6/2023, que modifica el art. 155.1 en idénticos términos.

Pues bien, con independencia del carácter superfluo de lo previsto en el primer párrafo del art. 155.1[42], las dos ideas importantes que se desprenden de la nueva regulación son:

Por un lado, que el primer emplazamiento o citación a quienes deben relacionarse electrónicamente con la Administración (en principio solo personas jurídicas y entes sin personalidad) debe hacerse por medios electrónicos (ex art. 50.1, 1º del decaído Proyecto de Ley de medidas de eficiencia digital del servicio público de justicia y también al amparo de igual norma del Real Decreto-ley 6/2023, mediante comparecencia en la Carpeta Justicia, en la Sede Judicial Electrónica correspondiente a la Comunidad Autónoma que haya asumido competencias en materia de Justicia, en la Dirección Electrónica Habilitada Única prevista en la Ley 39/2015, de 1 de octubre, o por otros medios que reglamentariamente se determinen).

42 Era innecesario reiterar dicha obligación de relacionarse electrónicamente con la Administración de Justicia (ya prevista, como vimos, en otros preceptos como los art. 152 y 273 LEC) y remitirse al art. 162 LEC, que es el que regula los "actos de comunicación por medios electrónicos, informáticos y similares" y que, una vez más, apunta a tal obligación en el primer párrafo de su apartado. En este sentido, y considerando la rúbrica del art. 155 ("actos de comunicación con las partes aún no personadas o no representadas por procurador o procuradora. Domicilio"), hubiera bastado con indicar en su primer apartado que "Cuando la parte venga obligada legal o contractualmente a relacionarse electrónicamente con la Administración de Justicia y el acto de comunicación tuviese por objeto el primer emplazamiento o citación, o la realización o intervención personal de las partes en determinadas actuaciones procesales y transcurrieran tres días sin que el destinatario acceda a su contenido, se procederá a su publicación por la vía del Tablón Edictal Judicial Único conforme a lo dispuesto en el artículo 164 (…)".

Y, por otro lado, que en caso de que a la Administración no le conste que el destinatario haya accedido a su contenido en el plazo de tres días (lo que implica no solo acceder a la Carpeta o Sede correspondiente, sino abrir el archivo; si no, no hay comparecencia[43]), se llevará a cabo la publicación edictal del emplazamiento en el TEJU (Tablón Edictal Judicial Único)[44], Tablón en el que procede dar la publicidad a los edictos según el art. 236 LOPJ -tras la modificación operada por LO 4/2018, de 28 de diciembre- y el art. 54 del Real Decreto-ley 6/2023 (que viene a sustituir al art. 35 de la derogada Ley 18/2011, de 5 de julio[45]).

Si estamos al orden jurisdiccional social, la regulación es la misma. Basta recordar la ya citada remisión que el art. 53.1 LJS (este precepto regula el lugar de las comunicaciones) hace a la LEC.

En la misma línea se encuentran otros preceptos del Real Decreto-ley 6/2023, que también acogen la regulación del Proyecto de Ley de medidas de eficiencia digital del servicio público de justicia. Así:

En primer lugar, su art. 49.1 indica que "las comunicaciones en el ámbito de la Administración de Justicia se practicarán por medios electrónicos, inclusive los actos procesales de comunicación previstos en el artículo 149 de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil". Como se ve, en la medida en que dicha norma "incluye" todos los actos de comunicación previstos en el art. 149 LEC, hay que entender incluidos también los primeros emplazamientos y citaciones.

Y, en segundo lugar, del apartado 2 de igual precepto[46] se desprende a contrario sensu que las comunicaciones se deben realizar de forma electrónica sólo con quienes están obligados a relacionarse electrónicamente con la Administración de Justicia y con las personas que, sin estarlo, hayan optado por la comunicación por vía telemática u online.

Pues bien, siguiendo con los comentarios al nuevo art. 155.2 LEC, fíjese que estamos ante una norma especial en materia de comunicaciones electrónicas

43 Tal y como dispone el art. 50.1, 2º de los citados Proyecto y Real Decreto-ley 6/2023, "se entenderá por comparecencia en la Carpeta Justicia o en la sede judicial electrónica el acceso por la persona interesada o su representante debidamente identificado al contenido del acto de comunicación".

44 Este régimen jurídico era igualmente aplicable al proceso laboral: aunque el citado Proyecto de Ley de medidas de eficiencia procesal modificaba algunos preceptos reguladores de los actos de comunicación de la LJS (arts. 53, 55, 56 y 59), seguían la misma línea de los vigentes de remitirse a la LEC (remisiones que operaban, entre otros casos, cuando había que comunicar actos a sujetos obligados a relacionarse electrónicamente con la Administración de Justicia o que hubieran optado por ello).

45 Para más detalles sobre el particular *vid.* Marcos Francisco, D.: "¡Se acabó la dispersión! El Tablón Edictal Judicial Único… Y algunos descuidos del legislador", *Actualidad Jurídica Aranzadi*, 24 junio 2021, núm. 975, p. 47.

46 Su tenor literal es: "Los órganos, oficinas judiciales u oficinas fiscales llevarán a cabo las comunicaciones por otros medios cuando las personas no obligadas a relacionarse con la Administración de Justicia por medios electrónicos no elijan hacer uso de estos medios".

frente a la regla general prevista en el art. 162.2, 1º[47] LEC de que transcurridos tres días sin acceder al contenido del acto se presumirá -presunción iuris tantum- que la comunicación ha sido correctamente efectuada y desplegará sus efectos; regla más próxima al presunto rechazo previsto en el art. 43.2, 2º de la citada Ley 39/2015. En efecto, el art. 155.1 LEC no establece, como el aludido art. 43.2, 2º, la presunción irus tantum[48] propia del procedimiento administrativo: en caso de no constar la comparecencia en el plazo de tres días, se debe intentar otra vía de comunicación electrónica -la del TEJU- antes de dar por efectuada la comunicación con todos sus efectos.

Ahora bien, en caso de haberse tenido que practicar la publicación en el TEJU, nada debería impedir combatir o atacar la comunicación previa realizada por los canales aludidos y declarar la nulidad de lo actuado cuando su destinatario alegue y acredite no haber podido acceder al sistema de notificaciones durante los tres días, sea por motivos materiales o técnicos (art. 162.2, 2º[49] LEC), a pesar de "que conste la correcta remisión del acto de comunicación" (ATC -Pleno- 113/2020, de 22 de septiembre)[50]. En definitiva, como se desprende de la doctrina constitucional,

47 El nuevo art. 162.2, 1º LEC, modificado por el Real Decreto-ley 6/2023, ha aclarado in fine, acabando con los problemas prácticos sobre el cómputo de plazos, que "en este caso, los plazos para desarrollar actuaciones procesales comenzarán a computarse desde el día hábil siguiente al tercero". Esta previsión no hace sino acoger la postura del TS. Baste estar al Acuerdo no Jurisdiccional del Pleno de la Sala de lo Social de dicho Tribunal de 6 de julio de 2016, sobre notificaciones a través del sistema Lexnet en el orden social y plazos procesales, (punto SEGUNDO, letra A), accesible en https://www.poderjudicial.es/cgpj/es/Poder-Judicial/Tribunal-Supremo/Jurisprudencia-/Acuerdos-de-Sala/Acuerdo-del-Pleno-No-Jurisdiccional-de-la-Sala-de-lo-Social-del-Tribunal-Supremo-de-06-07-2016--sobre-notificaciones-a-traves-del-sistema-Lexnet-en-el-orden-social-y-plazos-procesales (consultada el 18.01.24).

48 Como dice Martín Delgado, I.: "Algunos aspectos problemáticos de la nueva regulación del uso de los medios electrónicos por las Administraciones Públicas", *Revista Jurídica de la Comunidad de Madrid*, 2018, pp. 39 y 40, aunque parece que el legislador quiso convertir la presunción iuris tantum del art. 28 de la anterior (ya derogada) Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, en presunción iuris et de iure, en coherencia con la jurisprudencia (p. ej., STS 26 mayo 2011 [Roj: STS 4107/2011]) hay que entender que dicha presunción admite prueba en contrario, so pena de causar indefensión al destinatario del acto, cuando no conste la puesta a disposición electrónica del acto o se acredite la imposibilidad técnica o material de acceder a él. En similar sentido, autores como Cotino Hueso, L.: "La preocupante falta de garantías constitucionales y administrativas en las notificaciones electrónicas", *Revista General de Derecho Administrativo*, 2021, núm. 57, pp. 9 y 10.

49 Esta norma, tras la modificación operada por el Real Decreto-ley 6/2023, exceptúa de la presunción establecida en el párrafo anterior de haberse comunicado correctamente el acto de comunicación, "aquellos supuestos en los que el destinatario justifique que no pudo acceder al sistema de notificaciones durante ese periodo. Si la falta de acceso se debiera a causas técnicas y éstas persistiesen en el momento de ponerse en conocimiento de la Administración de Justicia, el acto de comunicación se practicará mediante entrega de copia de la resolución. En este supuesto, no obstante, en el caso de producirse el acceso transcurrido dicho plazo, pero antes de efectuada la comunicación mediante entrega, se entenderá válidamente realizada la comunicación en la fecha que conste en el resguardo acreditativo de la recepción electrónica".

50 El ATC (Pleno) 113/2020, de 22 de septiembre (BOE núm. 289, de 2 de noviembre de 2020), que inadmite una cuestión de inconstitucionalidad planteada con respecto al art. 162.2 LEC, entiende: "No puede apreciarse que el precepto cuestionado, al otorgar plenos efectos a la notificación a los tres días de su recepción a pesar de que el destinatario no haya accedido a su contenido vulnere el art. 24.1 CE. En efecto, para que la notificación produzca plenos efectos es preciso (i) que los destinatarios de la comunicación estén obligados a la utilización de medios electrónicos, telemáticos o similares o que opten por la utilización de este tipo de medios (art. 162.1 LEC); (ii) que conste la correcta remisión del acto de comunicación –párrafo primero del art. 162.2 LEC– y (iii) que el destinatario pueda acceder al sistema de notificaciones, pues si por causas técnicas no fuera posible acceder al contenido de la notificación el acto de comunicación debe practicarse mediante entrega de copia de la resolución –párrafo segundo del art. 162.2 LEC–.

aunque haya habido un escrupuloso cumplimiento de la ley en la práctica del acto de comunicación, el acto de comunicación será ineficaz cuando el destinatario acredite que, pese a actuar con diligencia, no pudo llegar a tener un conocimiento real de su contenido (STC 58/2010, de 4 de octubre[51], FJ 3). Cuestión distinta es que la carga de la prueba sea un obstáculo muy difícil de superar considerando su gran complejidad en muchos casos, sobre todo cuando las causas son técnicas.

Por otro lado y como último comentario, el art. 155.1 LEC en consonancia con el art. 162.2, 1º LEC, fija el plazo en tres días (hay que entenderlos hábiles[52], aunque lo conveniente es que la propia norma lo hubiera indicado para garantizar la seguridad jurídica), en lugar de los diez naturales propios del procedimiento administrativo, lo que puede generar confusión en los destinatarios de los actos de comunicación (porque pueden serlo tanto en el ámbito procesal como administrativo y, sin embargo, las reglas son diferentes)[53]. Dicho plazo de tres días, equiparado al de cualquier otro acto de comunicación (*vid.* art. 162.2, 1º LEC), me parece desproporcionado, considerando que estamos hablando de actos iniciadores de un proceso que dan a conocer al demandado su existencia. En este sentido, podría ampliarse a diez[54].

B) Hablemos de garantías: garantías de lege ferenda.

Lo primero de que debe hablarse al articular la forma de practicar las notificaciones es de la necesaria observancia de las garantías procesales, especialmente cuando hablamos de comunicaciones mediante las que se pone

Si concurren las referidas circunstancias la falta de acceso al contenido de la notificación en el plazo de tres días debe considerarse imputable a la falta de diligencia del destinatario (…). La regulación que establece el precepto impugnado no vulnera, por tanto, el derecho que consagra el art. 24.1 CE, pues concilia el derecho a la tutela judicial efectiva del destinatario del acto de comunicación –la notificación no es eficaz si no puede acceder a su contenido por una incorrecta remisión o por una deficiencia del sistema de notificaciones– con el buen funcionamiento de la administración de Justicia, que exige que las resoluciones judiciales sean eficaces tan pronto como su destinatario tiene la posibilidad de conocer su contenido" (FJ 5). Aunque el TC en la presente resolución alude únicamente a causas técnicas, nada debería impedir alegar otro tipo de causas que impidan el acceso al acto para desvirtuar la eficacia del acto de comunicación.

51 STC 58/2010, de 4 de octubre (BOE núm. 262, de 29 de octubre de 2010).

52 *Vid.* el supra citado Acuerdo no Jurisdiccional del Pleno de la Sala de lo Social de dicho Tribunal de 6 de julio de 2016 (nótese que no estamos ante un plazo procesal y, por ende, no resulta aplicable el art. 133.2, 1º LEC).

53 Autores como Bauzá Martorell se han mostrado críticos con la dualidad de regulaciones en sede administrativa (art. 43.2, 2º de la Ley 39/2015) y judicial (art. 162.2, 1º LEC), defendiendo la unidad de criterios en ambas sedes al no existir motivos objetivos que justifiquen la diferencia. *Vid.* "Cómputo de plazos en el proceso judicial digital", AA.VV.: *Modernización digital e innovación en la Administración de Justicia* (coord. por M. F. Gómez Manresa y M. Fernández Salmerón), Thomson Reuters Aranzadi, Cizur Menor (Navarra), 2019, p. 445.

54 Así lo estimo excepcionalmente con respecto al primer acto de comunicación al demandado, pese a que el citado ATC (Pleno) 113/2020, de 22 de septiembre (BOE núm. 289, de 2 de noviembre de 2020) haya entendido que "el plazo de tres días que establece el art.162.2 LEC para que la notificación efectuada tenga plenos efectos otorga al destinatario de la comunicación un margen de tiempo suficiente para que pueda acceder al contenido del acto que se comunica, por lo que, si pudiendo acceder en ese plazo al sistema de notificaciones, no lo hace, las consecuencias que puedan derivarse solo pueden ser imputables a su falta de diligencia" (FJ 5).

en conocimiento del demandado la existencia de un proceso judicial contra él y que le permiten efectuar alegaciones en su defensa durante un plazo o mediante la comparecencia -física o virtual- en un lugar, fecha y hora determinados. No hay que perder de vista la enorme importancia que, según reiterada jurisprudencia del TC, tienen los actos de comunicación para garantizar el derecho fundamental a obtener una tutela judicial efectiva consagrado en el art. 24.1 CE y la prohibición de indefensión que le es inherente. Así, como recuerda la reciente e ilustrativa STC 179/2021, de 25 de octubre[55], "solo si la constitución de la *litis* tiene lugar en los términos debidos es posible garantizar el derecho a la defensa de quienes sean o puedan ser parte en dicho proceso y, muy en particular, la inexcusable observancia del principio de contradicción, sobre el que se erige el derecho a ser oído. De ahí la especial relevancia de los actos de comunicación del órgano judicial con las partes, en particular el emplazamiento, citación o notificación a quien ha de ser o puede ser parte en el procedimiento, pues en tal caso el acto de comunicación es el necesario instrumento que facilita la defensa en el proceso de los derechos e intereses cuestionados; de tal manera que su falta o deficiente realización, siempre que se frustre la finalidad con ellos perseguida, coloca al interesado en una situación de indefensión que vulnera el derecho de defensa (entre otras muchas, SSTC 115/1988, de 10 de junio, FJ 1; 195/1990, de 29 de noviembre, FJ 3; 326/1993, de 8 de noviembre, FJ 3; 77/1997, de 21 de abril, FJ 2; 219/1999, de 29 de noviembre, FJ 2; 128/2000, de 16 de mayo, FJ 5; 61/2010, de 18 de octubre, FJ 2; 30/2014, de 24 de febrero, FJ 3, y 169/2014, de 22 de octubre)" (FJ 2).

Dicho esto, centrándonos en la nueva regulación, hay una garantía fundamental para los derechos de las personas jurídicas y entes sin personalidad que sean demandados -y así se les comunique de forma electrónica conforme a la nueva normativa- que lamentablemente el Real Decreto-ley 6/2023 no ha tenido en cuenta. Me refiero a que, para garantizar que la notificación (que no es otra cosa que "dar noticia o hacer saber" la pendencia del proceso) se practique correctamente y sea una realidad por medios electrónicos, permitiendo a las personas jurídicas y entes sin personalidad la defensa de sus derechos, debería haberse hecho una campaña publicitaria o informativa, similar a las efectuadas por la Agencia Estatal Tributaria y la Tesorería General de la Seguridad Social, avisando de los cambios normativos que se iban a implementar en la práctica de estas primeras notificaciones (lo que incluye la advertencia de los criterios dispares en sede judicial y administrativa) mediante el uso de medios "tradicionales" que aseguraran que el destinatario (persona jurídica o ente sin personalidad) recibiese tal notificación y conociese los cambios. Para ello hubiera sido deseable que la propia legislación procesal, al estilo del Real Decreto 1363/2010, de 29

55 STC 179/2021, de 25 de octubre (BOE núm. 282, de 25 de noviembre de 2021).

de octubre, por el que se regulan supuestos de notificaciones y comunicaciones administrativas obligatorias por medios electrónicos en el ámbito de la Agencia Estatal de Administración Tributaria, condicionase la comentada obligatoriedad a la notificación de tal circunstancia en papel. Ahí es donde "la exigencia de las garantías debe exigirse en su máxima expresión"[56].

En íntima relación, debería la Administración de Justicia haberles otorgado un plazo para comunicar el hecho de disponer de dichos medios electrónicos y la dirección electrónica habilitada a tal efecto, que no es otra cosa que dar cumplimiento a lo dispuesto en el art. 162.1, 2º LEC (que tan sólo se ha cumplido con respecto a los profesionales de la justicia obligados al uso de estos medios)[57].

Para poder comunicar electrónicamente los actos procesales iniciales es indispensable garantizar: 1) que el destinatario sepa, sin lugar a dudas, que este es el nuevo proceder, para lo cual cabe hacer uso de la aludida campaña informativa; 2) que el destinatario disponga de los medios electrónicos adecuados (lo que -por cierto- no podemos afirmar suceda con respecto a todas las personas jurídicas y, mucho menos, con respecto a los entes sin personalidad, dado que los hay, como sucede con comunidades de propietarios, que carecen de los medios necesarios); 3) que la Administración de Justicia conozca el "domicilio" electrónico escogido por el destinatario, así como el dispositivo electrónico, servicio de mensajería simple o la dirección de correo electrónico que aquél haya identificado para informarle de la puesta a su disposición de un acto de comunicación, en los términos del art. 152.2 LEC[58]; 4) y que la Administración de Justicia ponga a disposición de los sujetos que, estando obligados a comunicarse electrónicamente, carecen de los correspondientes medios para ello o disponiendo les resulta muy difícil su uso, las herramientas oportunas para poder cumplir con su obligación. Ello implicaría poner a su disposición toda una serie de "puntos de ayuda digital" permanentes para facilitar el uso de herramientas electrónicas a los afectados por la brecha digital, proporcionando, en caso de ser necesario, los dispositivos electrónicos in situ.

56 En este sentido, García Moreno, V. A.: "Notificaciones electrónicas obligatorias y la aplicación del derecho a la tutela judicial efectiva en los procedimientos administrativos de carácter no sancionador. Sentencia del Tribunal Constitucional n.º 147/2022, de 29 de noviembre (recurso 3209/2019)", *Carta Tributaria. Revista de Opinión*, 2023, núm. 95, p. 2 (edición electrónica), con respecto a la inclusión obligatoria en el sistema de notificación electrónica de la AEAT.

57 Cerdá Meseguer, J. I.: "La notificación", cit., pp. 5 y 6 (edición electrónica).

58 Resultan muy ilustrativas resoluciones como la SAP de León (Sección 2ª) 15 junio 2018 (Roj: SAP LE 731/2018) y las SSAP de Salamanca (Sección 1ª) 30 noviembre 2018 (Roj: SAP SA 615/2018); 21 mayo 2019 (Roj: SAP SA 272/2019); y 11 julio 2019 (Roj: SAP SA 393/2019), que en sus respectivos FJ Terceros rezan que "no es lo mismo el primer emplazamiento, que conlleva la comunicación del procedimiento que se entabla contra la misma, el conocimiento cierto y real de que ha sido demandada, que los posteriores actos de comunicación, pues una vez que se tiene conciencia de la demanda, es cuando además de determinar cuál va a ser su postura frente a la misma, puede incluso identificarse el dispositivo electrónico que servirá para informar de los actos de comunicación subsiguientes, de no actuar representada por Procurador, en el caso de que fuera factible, o para cuando se trate de citaciones o notificaciones que han de hacerse personalmente al interesado".

Indicado lo anterior, si -pese a mis no pocas reticencias y a lo que infra comentaré- el legislador decide seguir en la línea de "papel cero" y mantener la realización de la primera comunicación con el demandado o ejecutado de forma virtual, resulta crucial hablar de dos garantías en la práctica de tales notificaciones:

- La primera de ellas tiene que ver con la permanencia del mensaje en el buzón asociado a la Carpeta Justicia, Sede Judicial Electrónica o DEHú. Resulta imprescindible que sea posible comparecer mientras sigan abiertos los plazos para que el destinatario del acto pueda efectuar alegaciones en su defensa (como sucede en el emplazamiento para contestar a la demanda en diez o veinte días en los juicios verbales y ordinarios, respectivamente), lo que debería contemplar la propia normativa[59]. Más difícil es establecer el plazo de permanencia del mensaje cuando de citaciones se trata, siendo lo más garantista que conste hasta el día y hora de la personación en determinado lugar. Algo similar cabe decir con respecto al tiempo otorgado en los requerimientos para realizar cierta conducta.

No obstante, en la medida en que, si no se accedió a los citados buzones electrónicos, será posible consultar los edictos de los que es destinatario un NIF concreto durante cuatro meses en el TEJU (consulta que puede efectuarse a través de las distintas sedes judiciales electrónicas), la imposibilidad de acceder a aquellos tras pasar los tres días tampoco sería tan problemático (para poder acceder posteriormente es necesario contar con el código de verificación correspondiente al anuncio[60]). Ello siempre y cuando se informe claramente de este dato al destinatario del acto.

- La segunda de ellas tiene que ver con el aviso complementario del acto de comunicación que informa al destinatario de la puesta a su disposición del mismo. Tal y como sucede en el ámbito administrativo[61], la falta de este aviso, previsto en el art. 152.2, 3º LEC, no impide la validez del acto de comunicación ni tiene consecuencia alguna.

59 En este sentido, con respecto al procedimiento administrativo, Martín Delgado, I.: "Algunos aspectos", cit., p. 41, quien indica seguidamente que "por ello es totalmente contrario al derecho de defensa –y, por tanto, ilegal– lo previsto en el art. 10 de la citada Orden PRE/878/2010, que encomienda al órgano, organismo o entidad al que corresponda la prestación del sistema de DEH la función de «impedir el acceso al contenido de las notificaciones que se entienden rechazadas por el transcurso de 10 días desde su puesta a disposición»".

60 *Vid.* art. 14.4 del Real Decreto 181/2008, de 8 de febrero, de ordenación del diario oficial "Boletín Oficial del Estado".

61 *Vid.* art. 41.6 in fine de la citada Ley 39/2015, según el cual "la falta de práctica de este aviso no impedirá que la notificación sea considerada plenamente válida", cuyos términos reproduce literalmente el art. 152.2, 3º in fine LEC.

Aunque es cierto que dicha previsión es respetuosa con la doctrina del TC, dado que se encuentra en la línea de la controvertida decisión[62] de la STC (Pleno) 6/2019, de 17 de enero[63], que declaró la constitucionalidad del controvertido art. 152.2, 3º in fine, desde mi punto de vista, más próximo al voto particular emitido por el magistrado XIOL RÍOS[64], al proporcionar los eventuales destinatarios de comunicaciones un dispositivo electrónico, servicio de mensajería simple o dirección de correo electrónico y aludir la norma a que la oficina judicial "enviará" -en imperativo- el referido aviso, se genera en ellos la confianza de que serán avisados en tales vías de la puesta a su disposición de un acto de comunicación (sin la necesidad de tener que estar accediendo continuamente en la sede judicial electrónica o buzón de la plataforma correspondiente para averiguar si han recibido algún acto de comunicación) y, al no cumplirse con tal expectativa, se les podría causar una indefensión proscrita por el art. 24.1 CE[65]. Y repárese en que, si bien puede resultar exigible a los profesionales del derecho o de la justicia que para el desarrollo de su profesión emplean sistemas electrónicos de comunicación como LexNet que los mismos lo consulten con cierta frecuencia, no podemos decir lo mismo con respecto a quienes no deben hacer uso de estas herramientas electrónicas para el desempeño de su trabajo, aunque deban emplearlas para comunicarse con la Administración (como son las personas jurídicas y los entes sin personalidad): en este segundo caso la diligencia exigible no puede ser igual que en el primer caso.

Prever la realización de estos avisos de forma obligatoria, con posibles consecuencias en caso de incumplimiento, constituye una garantía fundamental[66] que en la actualidad es muy fácilmente practicable al poderse automatizar muy fácilmente aquellos, y más cuando la nueva regulación ya prevé expresamente la posible automatización de actos procesales y el empleo de inteligencia artificial. Pero, como digo, lamentablemente el Real Decreto-ley 6/2023 no ha llevado a cabo modificación alguna al respecto, siendo la voluntad mantener el status quo.

62 Herrero Perezagua, J. F.: "Crisis y medios", cit., p. 126.

Otros autores como Cubillo López, I. J.: *Actos procesales*, cit., pp. 175 y 176, se muestran a favor se dicha decisión. Igualmente, autores como Moreno García, L.: "Las notificaciones", cit., p. 66.

63 STC 6/2019, de 17 de enero (BOE núm. 39, de 14 de febrero de 2019). De dicha resolución se ha hecho eco el TS en resoluciones como la STS 25 mayo 2022 (Roj: STS 2286/2022), FD Tercero.

64 Autores como Gómez Fernández comparten plenamente dicho voto particular. *Vid.* "El Tribunal Constitucional resuelve sobre la falta de aviso electrónico en Lexnet", publicado en https://www.derechoadministrativoyurbanismo.es/post/2019/01/25/el-tribunal-constitucional-resuelve-sobre-la-falta-de-aviso-electr%C3%B3nico-en-lexnet el 25 de enero de 2019 (consultada el 12.12.23), obra también publicada en el *Diario La Ley*, 2019, núm. 9347.

65 En este sentido, autores como Perea González, A.: "«Aviso» vs «Acto de comunicación»: análisis y comentario a la Sentencia de 17 de enero de 2019 del Tribunal Constitucional", *Elderecho.com*, 26 de febrero de 2019 (accesible en https://elderecho.com/aviso-vs-acto-comunicacion-analisis-comentario-constructivo-la-sentencia-17-enero-2019-del-tribunal-constitucional, consultada el 11.01.24).

66 Como indica Cotino Hueso con respecto al procedimiento administrativo, "los avisos de notificaciones son la clave de bóveda para garantizar el acceso efectivo a la notificación", siendo inaceptable "que no se imponga para la validez de la notificación el aviso" (*vid.* "La preocupante", cit., pp. 24 a 26).

De lege ferenda sería deseable integrar el aviso en la notificación y contemplar que su omisión determina la nulidad del acto de comunicación, excepto cuando el destinatario haya accedido en el plazo de tres días contemplado en el art. 162.2 LEC[67]; o, si se prefiere, considerando la mayor diligencia exigible a los profesionales del derecho (abogados, procuradores y graduados sociales)[68] que, conforme al art. 6.3 del Real Decreto-ley 6/2023, tienen el deber de emplear los medios electrónicos, podría contemplarse que la omisión del aviso determinara la nulidad del acto de comunicación cuando su destinatario fuera una persona jurídica o entidad sin personalidad y no constara que hubiesen accedido en el referido plazo de tres días. Si aún se deseara ser más restrictivos en cuanto a la nulidad del acto de comunicación, podría reservarse para los casos en que faltara el aviso de la puesta a disposición de un acto de comunicación consistente en el primer emplazamiento, citación o requerimiento del demandado o ejecutado, siendo -este demandado o ejecutado- una persona jurídica o entidad sin personalidad[69].

Si el prelegislador/legislador deseaba mantener la anterior regulación respetuosa con la doctrina del TC, debería haber clarificado la norma en aras de una mayor seguridad jurídica y, en esta línea, sustituir la expresión imperativa "se enviará" por la potestativa "podrá enviar"[70]. No lo ha hecho y, lo que aún me parece más criticable, es que en la nueva previsión la anterior posibilidad que se otorgaba a eventuales destinatarios de actos de comunicación de identificar un dispositivo electrónico, servicio de mensajería simple o dirección de correo electrónico, ha pasado a convertirse en una obligación (ésta es la tercera novedad fundamental introducida en el art. 152.2 LEC por el Real Decreto-ley 6/2023[71]) y, sin embargo,

67 Pérez Daudí, V.: "Diálogos para el futuro judicial XL. Los actos de comunicación en el marco de la Justicia Digital" (coord. por A. Perea González), *Diario La Ley*, 1 marzo 2022, núm. 10019, p. 16 (edición electrónica).

68 Conforme al art. 6.2.f) del Real decreto-ley 6/2023, y como una novedad importante y oportuna, se garantiza a estos profesionales su derecho a la desconexión digital, conciliación y descanso "en los períodos inhábiles procesalmente y en aquellos en que las personas profesionales de la Abogacía, la Procura y los Graduados y Graduadas Sociales estén haciendo uso de las posibilidades dispuestas a tal fin en las normas procesales".

69 Con respecto al procedimiento administrativo se han realizado otras propuestas, tales como que, en caso de faltar el aviso, se condicione la eficacia del acto administrativo a su acceso (*vid.* Gamero Casado, E. y Fernández Ramos, S.: *Manual Básico de Derecho Administrativo*, Tecnos, Madrid, 2016, pp. 568 y 569).

70 En esta línea, Moreno García, L.: "Las notificaciones", cit., p. 70; Perea González, A.: "«Aviso» vs", cit.

71 Ahora el precepto dice que "el destinatario «deberá» identificar". Cohonestando con dicha obligación, el Real Decreto-ley ha modificado el art. 399.1 LEC (sobre "la demanda y su contenido" en el juicio ordinario, aplicable al juicio verbal ex art. 437.1 LEC), al que añade un 2º párrafo, que establece, sin la claridad que sería deseable: "Igualmente, para aquellos supuestos en que legalmente sea necesario realizar notificaciones, requerimientos o emplazamientos personales directamente al demandante o cuando éste actúe sin procurador, y siempre que se trate de personas obligadas a relacionarse electrónicamente con la Administración de Justicia, o que elijan hacerlo pese a no venir obligadas a ello, se consignarán cualquiera de los medios previstos en el apartado 1 del artículo 162 o, en su caso, un número de teléfono y una dirección de correo electrónico haciéndose constar el compromiso del demandante de recibir a través de ellos cualquier comunicación que le dirija la oficina judicial. Dicho compromiso se extenderá al proceso de ejecución que dé lugar la resolución que ponga fin el juicio". En la misma línea, aquella norma ha modificado el art. 405.1 LEC (sobre "la contestación y forma de la contestación a la demanda" en el juicio ordinario, también aplicable al juicio verbal ex art. 438.1 LEC), de forma que en tal contestación el demandado debe asumir idéntico compromiso que hemos visto con respecto al actor. Siendo lógico y correcto que el demandante, que es quien voluntariamente inicia el proceso, deba proporcionar la aludida información en

la obligación también prevista de la oficina judicial de enviar los aludidos avisos sigue sin tener ninguna consecuencia o incidencia en el acto de comunicación[72], algo inaceptable[73].

3. En la jurisprudencia.

El problema con el que nos encontramos, que ya he adelantado supra, es que constitucionalmente tienen mucha importancia los actos de comunicación para garantizar los derechos fundamentales consagrados en el art. 24 CE (especialmente, con respecto a aquellos actos, como el primer emplazamiento o citación, al ser su finalidad hacer saber al demandado la pendencia del proceso[74]) y, según consolidada jurisprudencia del Tribunal Constitucional, no son admisibles los medios electrónicos para el primer emplazamiento o citación so pena de vulnerar el derecho fundamental a obtener una tutela judicial efectiva. En este sentido, tal y como puso de manifiesto el CGPJ en su Informe al Anteproyecto de Ley de medidas de eficiencia procesal del servicio público de justicia, aprobado por el Pleno en su reunión de 22 de julio de 2021[75]:

"En relación con los actos de comunicación del primer emplazamiento procesal por medios electrónicos, debe tenerse en cuenta la consolidada doctrina constitucional establecida sobre la vulneración del artículo 24.1 CE por la inadecuada utilización de la dirección electrónica habilitada como cauce de comunicación del primer emplazamiento procesal (SSTC 6/2019, de 17 de enero, 47/2019, de 8 de abril, 40/2020, de 27 de febrero, 43/2020, de 9 de marzo, 55/2020, de 15 de junio, 76/2020, de 29 de junio y 176/2020, de 9 de marzo, y más recientemente, SSTC 59/2021, de 15 de marzo, 86/2021, de 19 de abril, 89/2021, de 19 de abril,

la demanda, no lo es tanto con respecto al demandado. Y ello porque, si hablamos de sujetos obligados a relacionarse con la Administración de Justicia de forma electrónica, se les habrá emplazado para contestar a la demanda de esta forma careciendo aún la Administración de la relevante información que debe consignar en la contestación para practicar con mayores garantías las notificaciones electrónicas. Dichos datos podrán ser útiles para actos de comunicación posteriores a la contestación, pero no para notificarle la demanda y emplazarle para su contestación. Si es en este trámite donde el demandado, obligado a relacionarse electrónicamente, señala el hecho de disponer de los medios electrónicos "antes indicados y la dirección electrónica habilitada" para practicar actos de comunicación a que alude el art. 162.1, 2ª LEC, me pregunto a qué dirección electrónica debe notificarle la demanda y emplazarle para su contestación la oficina judicial sin disponer de la información.
Por otro lado, llama la atención que, sin embargo, el Real Decreto-ley 6/2023 no haya hecho referencia a tal deber con respecto a otros tipos de procedimientos (los especiales), como son el monitorio y el cambiario, o incluso en la demanda ejecutiva para los casos en que procede el requerimiento de pago al ejecutado ex art. 581 LEC.

72 Autores como Ariza Colmenarejo han defendido de *lege ferenda* la conveniencia de establecer en la propia norma las consecuencias de la falta de practicar el aviso. *Vid.* su obra "Incidencia de las comunicaciones", cit., p. 155.

73 En este sentido, con respecto al procedimiento administrativo, *vid.* Martín Delgado, I.: "Algunos aspectos", cit., p. 42.

74 Adan Domènech, F.: "Formas de realización del emplazamiento del demandado", *VLex.es*, última actualización julio 2023 (accesible en https://vlex.es/vid/formas-realizacion-demandado-395799562, consultada el 12.07.23).

75 *Vid.* pp. 122 y 123.

100/2021, de 10 de mayo, y 115/2021, de 31 de mayo), y la confusión del deber de las personas jurídicas de relacionarse con la administración de justicia por medio de comunicaciones electrónicas con la regulación del primera emplazamiento en los procesos civiles (STC 56/2021, de 15 de marzo). En ella se afirma *«[l]a garantía del emplazamiento personal del demandado o* ejecutado en los procesos regidos en esta materia por la LEC (directa o supletoriamente), como primera comunicación con el *órgano judicial competente, sin que pueda ser sustituida por una* comunicación electrónica» (STC 47/2019, con cita de la 6/2019), tal y como ocurre con la efectuada a través de la dirección electrónica habilitada (SSTC 56/2021, 59/2021, 86/2021 y 89/2021). El emplazamiento personal se exige en el artículo 155.1 LEC, y lo complementa la regla del artículo 273.4 LEC sobre la presentación en papel de las copias de los escritos y documentos para este primer emplazamiento, incluso para los demandados personas jurídicas que estén obligados a relacionarse electrónicamente con la Administración de Justicia (artículo 273.1 y 3 LEC), y el incumplimiento de este deber del órgano judicial acarrea por tanto la conculcación del derecho fundamental, tal y como ha declarado el alto tribunal en varios recursos de amparo referidos a procesos civiles, concursales y laborales. Como se indica en la STC 56/2021, *«[M]uestra de la vinculación de los poderes* públicos a la doctrina constitucional, de la que se ha hecho eco la STC 19/2020, de 10 de febrero, es que, tras la publicación de la citada STC 47/2019 en el "Boletín Oficial del Estado" de 19 de mayo de 2019, la Secretaría General de la Administración de Justicia del Ministerio de Justicia, con fecha 21 de mayo de 2019, dirigió una comunicación a las secretarías de gobierno del Tribunal Supremo, Audiencia Nacional y tribunales superiores de justicia de las comunidades autónomas, citando la STC 47/2019, en su fundamento jurídico 4, para que cuiden "que la doctrina interpretativa de las normas procesales reguladoras del primer emplazamiento de personas jurídicas sentada por el tribunal Constitucional, cuyo obligado acatamiento impone la Ley Orgánica del Poder Judicial, sea observada en todas las oficinas judiciales del territorio"»".

En efecto, es verdad que el TC ha venido partiendo en su jurisprudencia del inequívoco -así lo entiende el Alto Tribunal- art. 155.1 LEC, cuya aplicación ya sabemos no se exceptuaba para los sujetos obligados a relacionarse electrónicamente con la Administración de Justicia, así como del también citado art. 273.4, 2º LEC, y de vincularlos con el necesario respeto a las garantías procesales fundamentales, como es la tutela judicial efectiva consagrada en el art. 24.1 CE. Así lo hace, en relación con procesos laborales, en su STC 47/2019, de 8 de abril[76] (dictada en un procedimiento por sanción de empleo y sueldo a una

76 STC 47/2019, de 8 de abril (BOE núm. 116, de 15 de mayo de 2019). Repárese en que esta Sentencia, al igual que las posteriores, parten de lo sentado en la pionera STC 6/2019, de 17 de enero (BOE núm. 39, de 14 de febrero de 2019), a saber: "(iii) Como excepción, no se ha de llevar a cabo por medios electrónicos la comunicación al demandado aún no personado en el procedimiento, en cuanto al acto de citación o emplazamiento, conforme a lo previsto en el artículo 155.1 LEC, los cuales "se harán por remisión al

trabajadora que la somete a valoración de los tribunales), FJ 2 a 6[77], cuya doctrina se ha reiterado posteriormente en resoluciones como las seguidamente indicadas dictadas con respecto a asuntos conocidos en el orden jurisdiccional social y civil (la inmensa mayoría de las resoluciones más recientes versan sobre procedimientos de ejecución hipotecaria, a los que siguen juicios de reclamación de cantidad):

- En sede de procesos laborales: SSTC 102/2019, de 16 de septiembre[78], FJ 2; 150/2019, de 25 de noviembre[79], FJ 3; y 7/2020, de 27 de enero[80], FJ 2;

- En relación con procesos civiles: SSTC 122/2019, de 28 de octubre[81], FJ 3; 40/2020, de 27 de febrero[82], FJ 3; 25/2021, de 15 de febrero[83], FJ 2; 26/2021, de 15 de febrero[84], FJ Único; 27/2021, de 15 de febrero[85], FJ Único; 28/2021, de 15 de febrero[86], FJ Único; 32/2021, de 15 de febrero[87], FJ Único; 33/2021, de 15 de febrero[88], FJ 3; 45/2021, de 3 de marzo[89], FJ Único; 46/2021, de 3 de marzo[90], FJ Único; 47/2021, de 3 de marzo[91], FJ Único; 49/2021, de 3 de marzo[92], FJ Único;

domicilio de los litigantes", regla que también opera en el proceso laboral (art. 53.1 LJS) y de hecho así se hizo en la causa *a quo*" (FJ 4).

77 Cordón Moreno se muestra muy crítico con la pionera STC 47/2019, de 8 de abril, entendiendo que no se había producido ninguna indefensión en la medida en que la empresa demandada tenía conocimiento de los actos de conciliación y juicio, porque -como alegó la trabajadora sancionada demandante- los cuatro trabajadores citados al juicio pusieron en conocimiento de la empresa que no asistirían al lugar de trabajo por dicho motivo. Argumenta dicho autor: "Si, como dice la STC 181/2015, de 7 de septiembre, la falta o deficiente realización del acto de comunicación coloca al interesado en una situación de indefensión «siempre que se frustre la finalidad con ellos perseguida..., salvo que la situación de incomunicación sea imputable a la propia conducta del afectado», en el presente caso no se puede decir que la indefensión se haya producido, porque el objeto de la notificación es que el interesado tenga conocimiento del acto notificado y, en el presente caso lo tenía. Y si esto es así, habrá que preguntarse si no sería aplicable al caso la norma del artículo 166.2 LEC sobre subsanación de notificaciones defectuosas" (*vid.* "Los actos de comunicación que constituyen la primera citación del demandado por medios electrónicos o telemáticos", accesible en https://www.ga-p.com/publicaciones/los-actos-de-comunicacion-que-constituyen-la-primera-citacion-del-demandado-por-medios-electronicos-o-telematicos/ y publicada en el 18 de octubre de 2019 [consultada el 12.07.23]). Es cierto que si no hay una indefensión real carece de sentido hablar de la vulneración del art. 24.1 CE. Pero la mentada Sentencia indica que dicha afirmación no "aparece adverada por ningún tipo de prueba" (FJ 5).

78 STC 102/2019, de 16 de septiembre (BOE núm. 247, de 14 de octubre de 2019).

79 STC 150/2019, de 25 de noviembre (BOE núm. 5, de 6 de enero de 2020).

80 STC 7/2020, de 27 de enero (BOE núm. 52, de 29 de febrero de 2020).

81 STC 122/2019, de 28 de octubre (BOE núm. 293, de 6 de diciembre de 2019).

82 STC 40/2020, de 27 de febrero (BOE núm. 83, de 26 de marzo de 2020).

83 STC 25/2021, de 15 de febrero (BOE núm. 69, de 22 de marzo de 2021).

84 STC 26/2021, de 15 de febrero (BOE núm. 69, de 22 de marzo de 2021).

85 STC 27/2021, de 15 de febrero (BOE núm. 69, de 22 de marzo de 2021).

86 STC 28/2021, de 15 de febrero (BOE núm. 69, de 22 de marzo de 2021).

87 STC 32/2021, de 15 de febrero (BOE núm. 69, de 22 de marzo de 2021).

88 STC 33/2021, de 15 de febrero (BOE núm. 69, de 22 de marzo de 2021).

89 STC 45/2021, de 3 de marzo (BOE núm. 77, de 31 de marzo de 2021).

90 STC 46/2021, de 3 de marzo (BOE núm. 77, de 31 de marzo de 2021).

91 STC 47/2021, de 3 de marzo (BOE núm. 77, de 31 de marzo de 2021).

92 STC 49/2021, de 3 de marzo (BOE núm. 77, de 31 de marzo de 2021).

58/2021, de 15 de marzo[93], FJ Único; 59/2021, de 15 de marzo[94], FJ Único; 62/2021, de 15 de marzo[95], FJ 2; 64/2021, de 15 de marzo[96], FJ 3; 84/2021, de 19 de abril[97], FJ Único; 85/2021, de 19 de abril[98], FJ Único; 86/2021, de 19 de abril[99], FJ Único; 89/2021, de 19 de abril[100], FJ 2; 100/2021, de 10 de mayo[101], FJ Único; 103/2021, de 10 de mayo[102], FJ Único; 115/2021, de 31 de mayo[103], FJ 2; 142/2021, de 12 de julio[104], FJ 2; 176/2021, de 25 de octubre[105], FJ 2; 177/2021, de 25 de octubre[106], FJ Único; 179/2021, de 25 de octubre[107], FJ 2; 187/2021, de 13 de diciembre[108], FJ 2; 188/2021, de 13 de diciembre[109], FJ 2; 189/2021, de 13 de diciembre[110], FJ 2; 14/2022, de 7 de febrero[111], FJ 2; 109/2022, de 26 de septiembre[112], FJ 2; 120/2022, de 10 de octubre[113], FJ 2; 121/2022, de 10 de octubre[114], FJ 2; 140/2022, de 14 de noviembre[115], FJ 3; y 14/2023, de 6 de marzo[116], FJ 2;

- Y, siguiendo la clasificación de la propia jurisprudencia, en relación con procesos concursales (que en realidad son procesos civiles especiales), en resoluciones como la STC 129/2019, de 11 de noviembre[117], FJ 4.

De la aludida jurisprudencia constitucional se ha hecho eco el TS en resoluciones recientes como la STS 221/2021, de 23 de febrero[118], FD 5º; STS 424/2021, de 26

93 STC 58/2021, de 15 de marzo (BOE núm. 97, de 23 de abril de 2021).
94 STC 59/2021, de 15 de marzo (BOE núm. 97, de 23 de abril de 2021).
95 STC 62/2021, de 15 de marzo (BOE núm. 97, de 23 de abril de 2021).
96 STC 64/2021, de 15 de marzo (BOE núm. 97, de 23 de abril de 2021).
97 STC 84/2021, de 19 de abril (BOE núm. 119, de 19 de mayo de 2021).
98 STC 85/2021, de 19 de abril (BOE núm. 119, de 19 de mayo de 2021).
99 STC 86/2021, de 19 de abril (BOE núm. 119, de 19 de mayo de 2021).
100 STC 89/2021, de 19 de abril (BOE núm. 119, de 19 de mayo de 2021).
101 STC 100/2021, de 10 de mayo (BOE núm. 142, de 15 de junio de 2021).
102 STC 103/2021, de 10 de mayo (BOE núm. 142, de 15 de junio de 2021).
103 STC 115/2021, de 31 de mayo (BOE núm. 161, de 7 de julio de 2021).
104 STC 142/2021, de 12 de julio (BOE núm. 182, de 31 de julio de 2021).
105 STC 176/2021, de 25 de octubre (BOE núm. 282, de 25 de noviembre de 2021).
106 STC 177/2021, de 25 de octubre (BOE núm. 282, de 25 de noviembre de 2021).
107 STC 179/2021, de 25 de octubre (BOE núm. 282, de 25 de noviembre de 2021).
108 STC 187/2021, de 13 de diciembre (BOE núm. 17, de 20 de enero de 2022).
109 STC 188/2021, de 13 de diciembre (BOE núm. 17, de 20 de enero de 2022).
110 STC 189/2021, de 13 de diciembre (BOE núm. 17, de 20 de enero de 2022).
111 STC 14/2022, de 7 de febrero (BOE núm. 59, de 10 de marzo de 2022).
112 STC 109/2022, de 26 de septiembre (BOE núm. 262, de 1 de noviembre de 2022).
113 STC 120/2022, de 10 de octubre (BOE núm. 277, de 18 de noviembre de 2022).
114 STC 121/2022, de 10 de octubre (BOE núm. 277, de 18 de noviembre de 2022).
115 STC 140/2022, de 14 de noviembre (BOE núm. 308, de 24 de diciembre de 2022).
116 STC 14/2023, de 6 de marzo (BOE núm. 89, de 14 de abril de 2023).
117 STC 129/2019, de 11 de noviembre (BOE núm. 304, de 19 de diciembre de 2019).
118 STS 23 febrero 2021 (Roj: STS 876/2021).

de junio[119], FD 5º; STS 938/2021, de 28 de septiembre[120], FD 3º; la STS 256/2022, de 23 de marzo[121], FD 3º; y la STS 565/2022, de 15 de julio[122], FD 2º.

Podría pensarse que, a la luz de la anterior jurisprudencia, difícilmente resulte admisible, so pena de vulnerar la Carta Magna, una regulación en otro sentido (y, por ende, resulten inadmisibles unos primeros emplazamientos o citaciones electrónicos). Pero lo cierto es que la postura del TC de descartar los medios electrónicos para estos actos de comunicación está basada o parte de lo que disponía la ley y de la aludida interpretación, a mi parecer correcta, que el Alto Tribunal ha venido efectuando de los arts. 155.1 y 273.4, 2º LEC.

De ahí que el propio TC en otras resoluciones dictadas en el ámbito del procedimiento administrativo (como la destacable STC 147/2022, de 29 de noviembre[123]), no se cuestione la validez de la comunicación electrónica para comunicar al interesado el inicio del procedimiento, sino el modo de actuar de la Administración porque ésta, a pesar de cumplir la regulación vigente en materia de actos de comunicación[124], sabía que el interesado -obligado a comunicarse electrónicamente- no había accedido a la Dirección Electrónica Habilitada (y, por tanto, no podía tener conocimiento del acto por esta vía) y, pese a ello, no empleó formas alternativas de comunicación o agotó todas las vías posibles (que incluyen la "notificación personal en papel"), causándole indefensión y vulnerando el art. 24.1 CE al desconocer el acto y, por tanto, no poder impugnarlo, incluso en sede judicial. En definitiva, como postula la STC (Sala Primera) 84/2022, de 27 de junio[125], partiendo de no cuestionar que el destinatario del acto "estuviera obligado a comunicarse electrónicamente con la administración y, en consecuencia, a aceptar las notificaciones que aquella le dirigiera a la dirección electrónica habilitada que le fue asignada de oficio", "ante lo infructuoso de las comunicaciones practicadas por vía electrónica, la administración debería haber desplegado una conducta tendente a lograr que las mismas llegaran al efectivo conocimiento del interesado, pues a ello viene obligada conforme a la síntesis doctrinal expuesta" (FJ 4).

119 STS 22 junio 2021 (Roj: STS 2484/2021).

120 STS 28 septiembre 2021 (Roj: STS 3684/2021).

121 STS 23 marzo 2022 (Roj: STS 1342/2022).

122 STS 13 julio 2022 (Roj: STS 3032/2022).

123 STC 147/2022, de 29 de noviembre (BOE núm. 5, de 6 de enero de 2023).

124 El Alto Tribunal "constata que la actuación llevada a cabo por la Agencia Tributaria no incumplió la regulación entonces vigente en materia de notificaciones electrónicas, puesto que la mercantil demandante estaba obligada a recibir las comunicaciones por esa vía" (FJ 5 de la STC 147/2022). De entre la legislación en materia tributaria aplicable al caso en que trae causa esta Sentencia que establecía la obligatoriedad de efectuar las notificaciones por medios electrónicos (la misma se recoge en el FJ 3 de la citada STC), *vid.* los arts. 2, 4.1, 5 y 6.1, 2 y 5 del vigente Real Decreto 1363/2010, de 29 de octubre, por el que se regulan supuestos de notificaciones y comunicaciones administrativas obligatorias por medios electrónicos en el ámbito de la Agencia Estatal de Administración Tributaria.

125 STC 84/2022, de 27 de junio (BOE núm. 181, de 29 de julio de 2022).

Y es que hay que partir de que el TC ha dicho que algunas de las garantías consagradas en el art. 24 CE no operan solo en el ámbito procesal sino también en el administrativo sancionador, como son los derechos a la defensa y a ser informados de la acusación contemplados en el art. 24.2 CE, lo que presupone que al sancionado se le debe notificar debidamente la incoación del procedimiento, lo que a su vez implica "la exigencia de procurar el emplazamiento o citación personal de los interesados, siempre que sea factible" (STC 32/2008, de 25 de febrero[126], FJ 2). E inclusive el Alto Tribunal ha extendido y considerado aplicable a procedimientos administrativos no sancionadores dichas garantías de emplazamiento propias de los procesos judiciales -lo eran hasta la reforma del Real Decreto-ley 6/2023- en casos en que se han realizado las notificaciones a personas distintas de los interesados y estas terceras personas han incumplido su carga de hacerlas llegar a estos (*vid.* STC 113/2006, de 5 de abril[127], FJ 6, parcialmente reproducido por la reciente STC 147/2022, de 29 de noviembre[128], FJ 4). Y lo mismo cabe decir con respecto al derecho fundamental a obtener una tutela judicial efectiva consagrado en el art. 24.1 CE: como recuerda la citada STC 147/2022, de 29 de noviembre, FJ 4, cabe la posibilidad de que este derecho fundamental resulte vulnerado en el ámbito administrativo "«en aquellos casos que no se permite al interesado, o se le dificulte, el acceso a los tribunales» (STC 197/1988, de 24 de octubre, FJ 3), como ocurre, por ejemplo, cuando en virtud de una norma «quedara impedido u obstaculizado el derecho de acceso a los tribunales de justicia» (SSTC 90/1985, de 22 de julio, FJ 4; y 123/1987, de 1 de julio, FJ 6). La indefensión originada en vía administrativa tiene relevancia constitucional, entonces, cuando la causa que la provoque impida u obstaculice que el obligado tributario pueda impetrar la tutela judicial contra el acto administrativo en cuestión, eliminándole la posibilidad de utilizar los medios de impugnación que el ordenamiento tributario dispone específicamente contra los diferentes actos dictados en cada procedimiento (en sentido parecido, STC 291/2000, de 30 de noviembre, FJ 4)"[129].

III. CONCLUSIONES.

1ª. La nueva regulación ha acabado con la inseguridad jurídica que derivaba de la existencia de distintas normas que -así podía entenderse- apuntaban a distintas soluciones (legitimando o no, según la norma, el posible uso de medios

126 STC 32/2008, de 25 de febrero (BOE núm. 76, de 28 de marzo de 2008).

127 STC 113/2006, de 5 de abril (BOE núm. 110, de 9 de mayo de 2006).

128 STC 147/2022, de 29 de noviembre (BOE núm. 5, de 6 de enero de 2023).

129 Como he dicho, la citada STC 147/2022 resulta relevante: constituye un impulso crucial en la aplicación del art. 24.1 CE a procedimientos administrativos que no tengan carácter sancionador. Sobre el particular puede verse García Moreno, V. A.: "Notificaciones electrónicas", cit., pp. 1-9 (edición electrónica).
La también citada STC 84/2022 sigue la doctrina del TC (recogida ya hace años en resoluciones como su Sentencia 18/1981, de 8 de junio [BOE núm. 143, de 16 de junio de 1981]) de extender a los procedimientos administrativos de carácter sancionador la aplicación de los mencionados derechos fundamentales consagrados en el art. 24 CE.

electrónicos para notificar el primer acto de comunicación al demandado o, inclusive, ejecutado). Asimismo, siguiendo con las virtudes de la nueva regulación, el uso de medios electrónicos para llevar a cabo el primer acto de comunicación sin lugar a dudas constituye una nueva medida que permite aminorar costes para la Administración (en definitiva, para todos) y agilizar los procesos y, con ello, contribuir a la salvaguarda del derecho fundamental a un proceso sin dilaciones indebidas (art. 24.2 CE) del actor. En efecto, es evidente que con el establecimiento obligatorio de las comunicaciones electrónicas, sobre todo en lo que atañe a las primeras comunicaciones del tribunal con el demandado/ejecutado, lo que se pretende es agilizar los procedimientos (agilidad porque notificar de forma electrónica siempre es más rápido que hacerlo en papel y, además, al hacerlo a un "domicilio" o dirección electrónica permanente se evitan los enormes retrasos derivados de tener que averiguar el domicilio del demandado/ejecutado o efectuar varios intentos, en algunos casos -todo hay que decirlo- fallidos porque los destinatarios se aprovechan de la exigencia de la presencialidad), pero también ahorrar los enormes costes que implica para la Administración (que necesita mucho papel y, sobre todo, mucho personal para practicar las comunicaciones en este soporte).

2ª. Sin embargo -y dejando ya las bondades de lado- no puedo decir lo mismo con respecto al derecho fundamental a obtener una tutela judicial efectiva (art. 24.1 CE) del demandado o ejecutado. A la vista de la jurisprudencia analizada, llama la atención que la EM del citado Proyecto de Ley de medidas de eficiencia procesal dijera que "se da cabida a la doctrina establecida por el Tribunal Constitucional" (apartado X, 9º párrafo) y que el Real Decreto-ley 6/2023 diga en su Preámbulo que "todo lo anterior se lleva a cabo en la redacción normativa, como es obligado, con la observancia debida a la doctrina jurisprudencial del Tribunal Europeo de Derechos Humanos y del Tribunal Constitucional (…)"[130], dado que la nueva regulación no es respetuosa con la jurisprudencia del TC supra reseñada[131]. No

130 Y continúa diciendo: "asimilándose la perspectiva tecnológica desde una concepción instrumental en la que la relación electrónica entre los ciudadanos y ciudadanas y los órganos judiciales sólo se sitúa como un mecanismo de interacción más ágil, respetando como esencia insustituible de la potestad jurisdiccional las misiones de juzgar y hacer ejecutar lo juzgado, a cuyo servicio y al de las garantías procesales ha de adaptarse necesariamente la tecnología para permitir su plena satisfacción".

131 Y no es la única vez que el poder ejecutivo va en contra de la Justicia (poder judicial). Así, no me resisto a citar el empeño de aquél, en su propio beneficio, en obligar a las personas físicas a presentar la declaración del IRPF por medios electrónicos, a pesar de que la STS 11 julio 2023 (Roj: STS 3295/2023), anulara ciertos preceptos de la Orden del Ministerio de Hacienda HAC/277/2019, de 4 de marzo (en concreto, los arts. 9.1, 15.1 y 4, así como el apartado 1º de su Disposición final primera), que establecía dicha obligación.
Cierto es que el Tribunal Supremo se ha venido mostrando permisivo con la imposición del uso de medios electrónicos a personas físicas hasta su Sentencia de 6 de mayo de 2021 (Roj: STS 1587/2021) (*vid.* Cotino Hueso, L.: *La digitalización en las Administraciones Públicas en España*, Fundación Alternativas, Madrid, 2023, p. 56, donde cabe encontrar varias resoluciones en este sentido). Pero, pese a que el Alto tribunal cambió su criterio y, siguiendo esta nueva postura, ha fijado doctrina en dicha STS 953/2023 entendiendo que "se establece de manera general para todos los obligados tributarios sin determinar los supuestos y condiciones que justifiquen, en atención a razones de capacidad económica, técnica, dedicación profesional u otros motivos, que se imponga tal obligación, que constituye una excepción al derecho de los ciudadanos a ejercer sus derechos y cumplir con sus obligaciones a través de técnicas y medios electrónicos, informáticos

podemos afirmar que el nuevo art. 155.1 LEC, en su redacción dada por el repetido Proyecto o el Real Decreto-ley 6/2023, respeta la jurisprudencia del TC seguida en relación con procedimientos administrativos en los que la primera comunicación con el interesado, en cumplimiento de la normativa administrativa, se efectúa electrónicamente: conforme a la nueva normativa procesal, cuando le conste a la Administración que el destinatario del acto electrónico de comunicación no ha sido recibido (se haya accedido a su contenido) en el plazo de tres días desde su puesta a disposición, el mismo se publicará en el TEJU (por tanto, se hará uso de otro medio electrónico, en vez de intentar su comunicación personalmente en su domicilio)[132]. Y difícilmente pueda entenderse que la publicación electrónica en el TEJU es una conducta tendente a alcanzar el efectivo conocimiento por parte del destinatario del acto de comunicación. Recordemos las numerosas Sentencias del Alto Tribunal según las cuales practicar el emplazamiento mediante edictos del demandado sin haber agotado las posibilidades de notificación personal constituye una vulneración de la tutela judicial efectiva (entre las más recientes, *vid.* STC -Sala Primera- 28/2023, de 17 de abril, FJ 3[133]), precisamente por ser la notificación

o telemáticos con las garantías y requisitos previstos en cada procedimiento, reconocido en el art. 96.2 LGT" (FD 7º) y, lo que es aún más criticable, pese a que ha seguido dicha doctrina la SAN 5 diciembre 2023 (Roj: SAN 6332/2023), anulando ciertos preceptos de la posterior Orden HFP/310/2023, de 28 de marzo (arts. 9.1 y 15.1 y 4), el consecutivo Real Decreto-ley 8/2023, de 27 de diciembre, por el que se adoptan medidas para afrontar las consecuencias económicas y sociales derivadas de los conflictos de Ucrania y Oriente Próximo, así como para paliar los efectos de la sequía, ha modificado el art. 96 de la Ley 35/2006, de 28 de noviembre, del Impuesto sobre la Renta de las Personas Físicas, al que añade en su apartado 5, 2º, que por el Ministerio de Hacienda y Función Pública "podrá establecerse la obligación de presentación por medios electrónicos siempre que la Administración tributaria asegure la atención personalizada a los contribuyentes que precisen de asistencia para el cumplimiento de la obligación". Aunque -todo hay que decirlo- es verdad que el Gobierno no ha dado por supuesto que en todas las personas físicas concurren los necesarios requisitos de capacidad económica, técnica, etc. a que alude el Alto Tribunal para imponer tal obligación (y, por ello, dichos defectos deben ser suplidos con la necesaria asistencia personal por parte de la Administración), se me antoja difícil pensar que la ayuda de la Administración vaya a ser realmente suficiente para paliar los aludidos defectos. Y ello, aunque se acabe eliminando, como pretende el Gobierno, la cita previa obligatoria (*vid.* https://www.infobae.com/espana/2024/02/01/adios-a-la-cita-previa-obligatoria-para-hacer-tramites-en-organismos-de-la-administracion-publica-como-el-sepe-o-la-seguridad-social/, consultada el 01.02.24).

En cualquier caso, con la nueva regulación fíjese en que hay una disparidad de criterios y tratamiento diferenciado carente de justificación. Así, mientras ex art. 12.2 de la Ley 39/2015 los sujetos obligados a relacionarse electrónicamente con la Administración carecen de cualquier ayuda por la Administración (lo que Gamero Casado, con razón, criticó en "Panorámica de la Administración", cit., p. 3), tras la reforma operada en la Ley 35/2006, aun estando obligadas las personas físicas, ellas sí pueden acceder a esta ayuda.

132 El nuevo párrafo 3º del art. 155.1 LEC, que prevé la práctica en papel del acto de comunicación en la sede del órgano judicial si el interesado se persona en esta, lógicamente presupone que el destinatario ya tiene constancia de que la Administración pretende comunicarle algo. En tal caso (pensemos, p. ej., en que la oficina judicial haya mandado un aviso a la dirección de correo electrónico o mediante un mensaje al número de móvil del demandado que haya sido designada/o por el actor en la demanda, lo que curiosamente solo contempla de forma expresa el art. 155.2 LEC para las personas físicas), en aplicación del art. 155.4, 1º LEC, al haberse practicado el acto de comunicación varias veces hay que estar al art. 152.6, conforme al cual el dies a quo para el cómputo de plazos es la primera fecha en que el acto de comunicación se haya verificado, entendiendo -aunque no lo matiza la Ley- como tal verificación la recepción del acto de comunicación. Así, si el destinatario se personara en el Tribunal el segundo día siguiente a su puesta a disposición del acto en el buzón electrónico correspondiente, el cómputo del plazo se iniciaría al día siguiente del día de la entrega en papel. Si se personara transcurridos los tres días, el plazo se computaría desde la publicación del edicto de notificación en el TEJU.

133 Como pergeña el FJ 4 de dicha resolución, "tras resultar negativos los intentos de notificación personal, el juzgado debió agotar las averiguaciones pertinentes para conocer el domicilio real de la parte demandada, sin contentarse exclusivamente con la información proporcionada por la TGSS, antes de acudir a la comunicación edictal, tal y como dispone la interpretación conjunta de los arts. 57 LRJS, y 157 y 161 LEC,

edictal un medio de comunicación "de menor fiabilidad" (STC 48/2022, de 4 de abril[134], FJ 2).

3ª. No hay que perder de vista que los seres humanos muchas veces tendemos a ser irrealmente optimistas y pecamos de inoportunos entusiastas, tratando ciertos riesgos como si apenas tuvieran importancia, incluso como para no dedicarles tiempo y prestarles atención; optimismo que es fundamental para generar confianza y reducir ansiedades[135]. Sea porque el Consejo de Ministros ha sido "irrealmente optimista", sea por la urgencia en aprobar un conjunto de normas para seguir liderando el despliegue del Plan de Recuperación en Europa y obtener los fondos oportunos (el cuarto desembolso)[136], no podemos olvidar que la confianza no está interesada en buscar la verdad, sino en simplificar la vida y facilitarla. Quiero decir con esto que la generalización de los medios digitales bajo el paraguas de conseguir la maravillosa "eficiencia digital y procesal" no debería dejar de lado la búsqueda de la verdad y el pleno respeto a las garantías procesales que vienen siendo observadas en nuestro tradicional sistema "presencial". Creo que el prelegislador ha sido demasiado ambicioso en el uso de medios electrónicos al extenderlo a los primeros actos de comunicación.

Aunque el TC ha reiterado en distintas sentencias la posibilidad de establecer condiciones al ejercicio del derecho a la tutela judicial efectiva y, en este sentido, podríamos plantearnos la posibilidad de condicionar la forma de ejercerlo al uso de herramientas electrónicas, nunca hay que olvidar que debe existir una proporcionalidad. Y no me parece proporcionado y respetuoso con tal derecho que el primer emplazamiento, citación o requerimiento del demandado o ejecutado, cuando sea una persona jurídica o ente sin personalidad, se deba realizar por tales medios (cosa distinta es que así lo hayan decidido voluntariamente), dado que estamos ante actos de comunicación fundamentales -los más importantes precisamente- porque dan a conocer la existencia de procesos contra ellos y es excesivo pretender que dichas personas jurídicas y entidades sin personalidad deban estar constantemente pendientes del buzón electrónico por si se inicia un proceso contra ellos; buzón del que -por cierto- algunos de estos entes ni siquiera disponen. En definitiva, el art. 24.1 CE debe ser límite a tener en cuenta en toda

pues de otros registros públicos accesibles a través del punto neutro judicial podía obtenerse información completa y fiable para identificar el domicilio, posibilidad de acceso que el órgano judicial debía conocer".

134 STC 48/2022, de 4 de abril (BOE núm. 113, de 12 de mayo de 2022). Alguna jurisprudencia constitucional reciente sobre la necesidad de agotar las posibilidades de notificación personal antes de proceder al emplazamiento mediante edictos, particularmente en sede de ejecución hipotecaria, desahucios y proceso sumario para la inmediata recuperación de la posesión de la vivienda ilegalmente ocupada, puede verse en Romero Pradas, M. I.: "Actos de comunicación y acceso al proceso: el emplazamiento del demandado en pronunciamientos recientes del Tribunal Constitucional", en AA.VV.: *El proceso como garantía* (dir. por J. M. Asencio Mellado y O. Fuentes Soriano), Atelier, Barcelona, 2023, pp. 485-488.

135 González De la Garza, L. M.: *Justicia electrónica*, cit., p. 47.

136 *Vid.* el apartado I del Preámbulo del Real Decreto-ley 6/2023. Estamos ante uno de los tantos casos en que el Gobierno (sea el actual o pasado) ha hecho uso de la figura del Real Decreto-ley en casos de muy dudosa "extraordinaria y urgente necesidad" (art. 83.1 CE).

modernización e innovación[137], debiendo tener siempre presente que las TIC no dejan de ser un instrumento y no un fin en sí mismo.

4ª. A la luz de la precitada jurisprudencia, nada debería impedir prever la comunicación electrónica de los primeros emplazamientos o citaciones y, si la misma resulta infructuosa, acudir a la comunicación "tradicional" en papel, agotando todas las vías posibles de comunicación, como ha previsto el Real Decreto-ley 6/2023 en su art. 155.2.a).2º in fine para quienes no están obligados a relacionarse electrónicamente con la Administración de Justicia y como de hecho hemos visto ha mantenido el propio TC en el ámbito administrativo. Recordemos nuevamente la STC 147/2022, de 29 de noviembre: en Sentencias como ésta el TC no cuestiona la validez y garantías de la comunicación electrónica (si en otras resoluciones el Alto Tribunal cuestiona la validez y garantías del primer emplazamiento o citación electrónicos en los procesos judiciales civiles y laborales se debe a que la legislación ordinaria aplicable -fundamentalmente, los arts. 155.1 y 273.4, 2º LEC y los arts. 53 y 56 LJS- no contemplaban la vía telemática), sino el modo de actuar de la Agencia Tributaria que, pese a cumplir con la normativa de comunicaciones electrónicas, sabía que el interesado no había accedido a la Dirección Electrónica Habilitada (y, por tanto, no podía tener conocimiento del acto por esta vía) y, pese a ello, no agotó todas las vías de comunicación posibles, causándole indefensión y vulnerando el art. 24.1 CE al desconocer el acto y, por tanto, no poder impugnarlo, incluso en sede judicial.

En definitiva, nada obsta al empleo de medios electrónicos. Pero, de la misma forma que cabe extender la doctrina de la STC 147/2022 "a cualquier procedimiento de naturaleza administrativa cuyo acuerdo de incoación se notifique al interesado, cuando no se le permita o se le dificulte el acceso a los tribunales"[138], debería tenerse siempre presente en el ámbito procesal.

Así pues, para ser plenamente respetuosos con la jurisprudencia constitucional en la ahora estudiada reforma legal debería haberse previsto la comunicación por remisión personal al domicilio de los litigantes para el caso de que transcurrieran tres días sin que el destinatario accediera a su contenido como paso previo a la publicación en el TEJU, que únicamente debería practicarse agotadas las posibilidades de notificación personal. El problema es que, de ser así, quedaría en cuestión la eficiencia (que es precisamente lo que se pretende conseguir con

137 Gómez Manresa, M. F.: "Derecho a la tutela judicial efectiva, justicia abierta e innovación tecnológica", en AA.VV.: *Modernización digital e innovación en la Administración de Justicia* (coord. por M. F. Gómez Manresa y M. Fernández Salmerón), Thomson Reuters Aranzadi, Cizur Menor (Navarra), 2019, p. 45. En dicha obra pueden encontrarse distintos ejemplos de resoluciones del TEDH, TJUE y TC sobre la posibilidad de limitar y condicionar el derecho a la tutela judicial efectiva (pp. 39 y ss.).

138 García-valdecasas Dorrego M. J.: "El derecho de defensa se extiende a las notificaciones que la administración tributaria realiza en los procedimientos de gestión tributaria. STC 147/2022, de 22 de noviembre", *Actualidad Administrativa*, 2023, núm. 1, p. 3 (edición electrónica).

los cambios operados por el Real Decreto-ley 6/2023), dado que para obtener el pretendido resultado de hacer llegar al destinatario el acto de comunicación de la forma más respetuosa con los derechos fundamentales del art. 24 CE no sería suficiente con emplear el mínimo posible de recursos (nos encontraríamos con una duplicidad de estos: tanto recursos electrónicos como los tradicionales en papel).

5ª. La situación expuesta se ve agravada si consideramos que en las reformas que están siendo comentadas no se ha abordado la modificación del anterior art. 152.2, 3º in fine LEC, que preveía (y sigue previendo tras el Real Decreto-ley 6/2023, ahora en un 4º párrafo) que la falta de práctica del aviso al destinatario de la comunicación (en el dispositivo electrónico, servicio de mensajería simple o dirección de correo electrónico que aquél haya identificado) que le informe de que tiene a su disposición un acto de comunicación "no impedirá que la notificación correctamente efectuada sea considerada plenamente válida". Aunque la anterior -indicada en la 4ª conclusión-es mi propuesta de lege ferenda, como es difícil "volver atrás" (cuando las TIC llegan, lo hacen para quedarse), de lege ferenda sería deseable, al menos, como medida más garantista de la regulación actual, contemplar el aviso obligatorio en los términos indicados, por mucho que la regulación prevista -esta vez sí- es respetuosa con la jurisprudencia del TC. Y lo mismo cabe decir con respecto a la necesaria permanencia del mensaje en el buzón asociado a la Carpeta Justicia, Sede Judicial Electrónica o DEHú.

6ª. Así las cosas, ¿de verdad que estamos claramente -como dice el apartado II del Preámbulo del Real Decreto-ley 6/2023- ante una medida respetuosa con la tutela judicial efectiva[139]? Que juzgue el lector[140]. Y que juzgue, como debe hacerse, de acuerdo con el estado actual de la sociedad o la "realidad social del tiempo" (art. 3.1 CC). Aunque es probable que en un futuro no muy lejano las últimas generaciones (los conocidos como "Millenials", "Generación Z", los "Alfa", etc.), que ya han nacido inmersas en las TIC dando por hecho sus bondades (y, por cierto, lamentablemente en muchos casos haciendo un uso abusivo de ellas), cuando se relacionen con la Administración de Justicia no conciban otra forma de relacionarse que la electrónica, hoy en día muchos de los conocidos como "Baby Boomer" o la "generación X", que actualmente se están relacionando con la Administración y que han conocido la tradicional forma de relacionarse

139 Dice que este derecho fundamental es "en cualquier caso la prioridad absoluta".

140 En contra de mi opinión, no parecen ver problemas de constitucionalidad autores como Magro Servet, V., "Hacia un domicilio electrónico obligatorio de las personas físicas ante la Administración Pública en materia de notificaciones", *Revista CEF Legal*, 2022, núm. 263, p. 95 (quien va mucho más allá planteando la implantación de un domicilio electrónico obligatorio -DEO- para todas las personas físicas y para todo tipo de actos de comunicación, incluyendo los primeros actos de comunicación del tribunal con el demandado o ejecutado); o Martín Pastor, J.: "La digitalización de la Justicia y el reto de la garantía de los derechos fundamentales y de los principios del proceso", en AA.VV.: *El proceso como garantía* (dir. por J. M. Asencio Mellado y O. Fuentes Soriano), Atelier, Barcelona, 2023, p. 220 (con respecto a la reforma proyectada previa al Real Decreto-ley 6/2023).

en papel, siguen siendo muy reacios al uso de las TIC (algunos, de hecho, tienen enormes dificultades para entenderlas) y evitan su uso o las emplean lo mínimo indispensable (lo que no es muy compatible con la hiperconexión digital exigible por la nueva normativa ahora comentada). No olvidemos que estas personas físicas son las que, a la postre, están "detrás" de personas jurídicas y entes sin personalidad.

Con la nueva regulación es probable que existan procesos que se juzguen en rebeldía -involuntaria- del demandado o en que se embarguen bienes sin conocimiento del ejecutado, como ha venido sucediendo. Lo preocupante es que, si bien hasta el Real Decreto-Ley 6/2023 ha sido más fácil acordar la nulidad de lo actuado a la vista de la anterior normativa y de la precitada jurisprudencia constitucional (como sucede, por poner un ejemplo reciente, en el caso en que trae causa la SAP IB 493/2023, de 18 de octubre[141]), ahora ya no lo será tanto porque con la nueva normativa se exige un -discutible- mínimo deber de diligencia al destinatario del acto de comunicación, justificado sobre la base de que el medio de comunicación ha sido legalmente impuesto por el ordenamiento jurídico. Habrá que esperar al planteamiento de recursos o cuestiones de inconstitucionalidad ante el TC y a ver si el Alto Tribunal, en su línea anterior, estima inconstitucional la nueva regulación.

7ª. De la misma forma que hoy en día es inconcebible y sería mucho más problemático prever el primer emplazamiento o citación por vía electrónica, así como el resto de actos de comunicación, cuando el demandado/ejecutado no esté obligado a relacionarse con la Administración de Justicia por medios electrónicos (esto es, cuando sea una persona física), por la brecha digital y la posible indefensión que podría causarse[142], estoy convencida de que en cuestión de décadas será la forma normal y obligatoria de relacionarse y nadie la cuestionará. En efecto, no tengo dudas de que dentro de no muchos años se impondrá un "domicilio electrónico" obligatorio para todas las personas físicas como medio de comunicación con las Administraciones Públicas, incluidos los primeros emplazamientos, citaciones y requerimientos del demandado o ejecutado. Desconozco si será un único "domicilio" para todas las Administraciones Públicas y habrá una misma regulación de las comunicaciones electrónicas con independencia de la Administración con que nos relacionemos (como sería deseable en aras de garantizar la seguridad proclamada en el art. 9.3 CE) o seguiremos hablando de distintas sedes, buzones y regulaciones y si, como también sería deseable, dicho "domicilio" será bidireccional,

141 SAP IB 493/2023, de 18 de octubre (Roj: SAP IB 2740/2023). En tal caso se comunicó la demanda a una Comunidad de Propietarios a través de su dirección electrónica habilitada.

142 Pérez Daudí, V.: "Diálogos para el futuro", cit., p. 4. No así lo piensan otros autores como Magro Servet, para quien introducir la aludida obligatoriedad resulta necesaria y urgente, llevando consigo muchas más ventajas que inconvenientes, y no existiendo motivos que justifiquen la obligatoriedad para personas jurídicas y no para las personas físicas. *Vid.* "Hacia un domicilio", cit., pp. 72 y 79.

de tal manera que permitiera a las Administraciones ponerse en contacto con los ciudadanos y, a su vez, a estos con aquellas[143]. Pero lo más importante es que dicha obligatoriedad llegue en el momento oportuno (considero dicha obligatoriedad necesaria, pero no debe precipitarse como ha hecho el Real Decreto-ley 6/2023).

Y ese momento será -o debería serlo-, sin el apresuramiento con el que ha llegado la obligatoriedad para las personas jurídicas y entes sin personalidad en dicho Real Decreto-ley, cuando por el transcurso del tiempo y la llegada de nuevas generaciones ya no quepa hablar de la actual brecha digital por edad y haya más habilidades digitales y confianza en internet, cuando se haga la correspondiente campaña informativa acerca del carácter obligatorio de todas las comunicaciones electrónicas haciendo saber el alcance de la nueva normativa, que debería incluir los avisos obligatorios automatizados de puesta a disposición de una comunicación, cuando los softwares empleados sean mucho más intuitivos y de fácil manejo y cuando existan "puntos de ayuda digital" permanentes para facilitar el uso de herramientas electrónicas a los colectivos que sigan afectados por la brecha digital[144]. Será entonces cuando, de la misma forma que a partir de los 14 años todos debemos tener un DNI, con un número que nos identifique, a partir de los 18 años se nos podría exigir la asignación de un "domicilio electrónico" obligatorio, acudiendo presencialmente a determinada oficina (como debemos

143 Convengo con Magro Servet, V.: "Hacia un domicilio", cit., p. 99, en que esto sería lo más conveniente al hacerlo más tractivo para los ciudadanos que si se limitara a "recibir aspectos negativos".

144 Para saber cuándo es el momento oportuno para incluir la comentada obligatoriedad podríamos estar a las *Encuestas sobre Equipamiento y Uso de Tecnologías de Información y Comunicación (TIC) en los Hogare*s que el INE publica todos los años, un buen indicativo. Si estamos a la última de 2023 podemos ver cómo "el 95,4% de la población de 16 a 74 años ha usado Internet en los tres últimos meses (0,9 puntos más que en 2022)", que "el teléfono móvil está presente en el 99,5% de los hogares con al menos un miembro de 16 a74 años", que "el 96,4%, de los hogares disponen de acceso a Internet por banda ancha fija y/o móvil (frente al 96,1% en 2022)", que "el 66,2% poseen habilidades digitales básicas o avanzadas" (2,0 puntos más que en 2021), que "el 95,4% de las personas de 16 a 74 años ha utilizado Internet en los tres últimos meses (0,9 puntos más que en 2022) y el 90,0% diariamente (2,9 puntos más)" y que, como en 2022, "casi ocho de cada diez personas de 16 a 74 años (el 79,7%) ha contactado o interactuado con las administraciones o servicios públicos a través de Internet en los últimos 12 meses por motivos particulares", siendo "los contactos más habituales son para Concertar una cita o realizar una reserva (62,2%) y para Acceder a la información almacenada (60,8%)".
A la luz de dichos datos se concluye que, aunque como en años anteriores, el teléfono móvil está presente en casi todos los hogares, aún hay un porcentaje del 3,6% (aunque cada año que transcurre es menor) de hogares que no disponen de acceso a Internet (sea en el móvil u otro dispositivo electrónico), las habilidades digitales aún son muy mejorables (un 33,8% de personas de 16 a 74 años carece de las mismas, ni siquiera posee las básicas) y también es mejorable el porcentaje de personas del aludido rango de edad que se han relacionado electrónicamente con la Administración (casi un 80%), y más si tenemos en cuenta que la gran mayoría de los trámites efectuados por dicha vía han sido muy básicos. Y resulta crucial recordar que "las presentaciones electrónicas se articulan mediante plataformas específicas, en las que hay que cumplimentar una serie de formularios en línea, rodeados de exigencias y restricciones. Se piden como obligatorios datos o documentos que no vienen impuestos en la normativa de aplicación (teléfonos, direcciones de correo-e, certificados...), y además se limitan los formatos de los ficheros y su tamaño, complicando hasta el infinito la cumplimentación de los requisitos y llevando a los usuarios a niveles exasperantes de frustración. Una vez superada esta carrera de obstáculos, en la fase estricta de presentación, es tremendamente frecuente tropezarse con graves problemas de interoperabilidad, de suerte que no puede completarse el trámite porque se actualizó la versión de Java, porque no se ha descargado el applet de firma electrónica, o porque la versión del navegador es incompatible. Si el sufrido ciudadano no supera en plazo esta peculiar gymkhana, y no logra finalmente completar el trámite de presentación, perderá todos sus derechos. Este resultado es inaceptable" (Gamero Casado, E.: "Panorámica de la Administración", cit., p. 3).

acudir al hacernos el DNI) como medio de comunicación con las Administraciones Públicas, incluyendo los actos iniciadores de procedimientos. En ese momento y en ese contexto, quien no acceda electrónicamente al contenido de cualesquiera actos de comunicación (salvo que no lo haga alegando y acreditando motivos materiales o técnicos) no podrá posteriormente pretender que se declare la nulidad de lo actuado porque, como ha reiterado el TC, "la indefensión no se produce si la situación en la que el ciudadano se ha visto colocado se debió a una actitud voluntariamente adoptada por él o si le fue imputable por falta de la diligencia necesaria" (por todas, STC 48/1984, de 4 de abril[145], FJ Primero).

145 STC 48/1984, de 4 de abril (BOE núm. 99, de 25 de abril de 1984).

BIBLIOGRAFÍA

ADAN DOMÈNECH, F.: "Formas de realización del emplazamiento del demandado", *VLex*.es, última actualización julio 2023 (accesible en https://vlex.es/vid/formas-realizacion-demandado-395799562, consultada el 12.07.23).

ARIZA COLMENAREJO, M. J.: "Incidencia de las comunicaciones electrónicas en la tutela judicial", en AA.VV.: *Aciertos, excesos y carencias en la tramitación del proceso* (dir. por J. F. HERRERO PEREZAGUA y J. LÓPEZ SÁNCHEZ), Atelier, Barcelona, 2020, pp. 135-161.

BAUZÁ MARTORELL, F. J.: "Cómputo de plazos en el proceso judicial digital", AA.VV.: *Modernización digital e innovación en la Administración de Justicia* (coord. por M. F. GÓMEZ MANRESA y M. FERNÁNDEZ SALMERÓN), Thomson Reuters Aranzadi, Cizur Menor (Navarra), 2019, pp. 431-447.

CATALÁN CHAMORRO, M. J.: *La justicia digital en España: Retos y desafíos*, Tirant Lo Blanch, 2023.

CERDÁ MESEGUER, J. I.: "La notificación electrónica de la demanda a personas jurídicas: ¿innovación tecnológica o indefensión?", *Diario La Ley*, 2019, núm. 9388 (edición electrónica).

CERDÁ MESEGUER, J. I.: "Hacia una administración de justicia plenamente electrónica: disfunciones normativas y jurisprudenciales", AA.VV.: *Modernización digital e innovación en la Administración de Justicia* (coord. por M. F. GÓMEZ MANRESA y M. FERNÁNDEZ SALMERÓN), Thomson Reuters Aranzadi, Cizur Menor (Navarra), 2019, pp. 369-399.

CERNADA BADÍA, R.: "«LexNET» o la selección natural en el foro del siglo XXI", AA.VV.: *Modernización digital e innovación en la Administración de Justicia* (coord. por M. F. GÓMEZ MANRESA y M. FERNÁNDEZ SALMERÓN), Thomson Reuters Aranzadi, Cizur Menor (Navarra), 2019, pp. 401-429.

CORDÓN MORENO, F.: "Los actos de comunicación que constituyen la primera citación del demandado por medios electrónicos o telemáticos", accesible en https://www.ga-p.com/publicaciones/los-actos-de-comunicacion-que-constituyen-la-primera-citacion-del-demandado-por-medios-electronicos-o-telematicos/ y publicada en el 18 de octubre de 2019 (consultada el 12.07.23).

COTINO HUESO, L.: "La preocupante falta de garantías constitucionales y administrativas en las notificaciones electrónicas", *Revista General de Derecho Administrativo*, 2021, núm. 57, pp. 1-46.

Cotino Hueso, L.: *La digitalización en las Administraciones Públicas en España*, Fundación Alternativas, Madrid, 2023.

Cotino Hueso, L. y Montesinos García, A.: "Derechos de los ciudadanos y los profesionales en las relaciones electrónicas con la Administración de Justicia", en AA.VV.: *Las Tecnologías de la Información y la Comunicación en la Administración de Justicia. Análisis sistemático de la Ley 18/2011, de 5 de julio*, (coord. por E. Gamero Casado y J. Valero Torrijos), Thomson Reuters Aranzadi, Cizur Menor (Navarra), 2012, pp. 181-228.

Cubillo López, I. J.: *Actos procesales, comunicación procesal y medios electrónicos*, La Ley, Madrid, 2019.

Fierro Rodríguez, D.: "La confirmada obligatoriedad del uso de la tecnología en la Administración de Justicia", *Legaltoday.com*, 15 diciembre 2021 (accesible en https://www.legaltoday.com/opinion/articulos-de-opinion/la-confirmada-obligatoriedad-del-uso-de-la-tecnologia-en-la-administracion-de-justicia-2021-12-15/, consultada el 21.10.23).

Gamero Casado, E.: "Panorámica de la Administración electrónica en la nueva legislación administrativa básica", *Revista Española de Derecho Administrativo,* 2016, núm. 175, pp. 1-6 (edición electrónica).

Gamero Casado, E. y Fernández Ramos, S.: *Manual Básico de Derecho Administrativo*, Tecnos, Madrid, 2016.

García Moreno, V. A.: "Notificaciones electrónicas obligatorias y la aplicación del derecho a la tutela judicial efectiva en los procedimientos administrativos de carácter no sancionador. Sentencia del Tribunal Constitucional n.º 147/2022, de 29 de noviembre (recurso 3209/2019)", *Carta Tributaria. Revista de Opinión*, 2023, núm. 95, pp. 1-9 (edición electrónica).

García-valdecasas Dorrego M. J.: "El derecho de defensa se extiende a las notificaciones que la administración tributaria realiza en los procedimientos de gestión tributaria. STC 147/2022, de 22 de noviembre", *Actualidad Administrativa*, 2023, núm. 1, pp. 1-4 (edición electrónica).

Gómez Fernández, D.: "El Tribunal Constitucional resuelve sobre la falta de aviso electrónico en Lexnet", publicado en https://www.derechoadministrativoyurbanismo.es/post/2019/01/25/el-tribunal-constitucional-resuelve-sobre-la-falta-de-aviso-electr%C3%B3nico-en-lexnet el 25 de enero de 2019 (consultada el 12.12.23), obra también publicada en el *Diario La Ley*, 2019, núm. 9347.

Gómez-Linacero Corraliza, A.: "Diálogos para el futuro judicial XL. Los actos de comunicación en el marco de la Justicia Digital" (coord. por A. Perea González), *Diario La Ley*, 1 marzo 2022, núm. 10019 (edición electrónica).

Gómez Manresa, M. F.: "Derecho a la tutela judicial efectiva, justicia abierta e innovación tecnológica", en AA.VV.: *Modernización digital e innovación en la Administración de Justicia* (coord. por M. F. Gómez Manresa y M. Fernández Salmerón), Thomson Reuters Aranzadi, Cizur Menor (Navarra), 2019, pp. 37-61.

González De la Garza, L. M.: *Justicia electrónica y garantías constitucionales. Comentario a la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia*, La Ley, Las Rozas (Madrid), 2012.

Herrero Perezagua, J. F.: "Crisis y medios tecnológicos: razón y ocasión para la reforma del proceso", en AA.VV.: *Proceso civil y nuevas tecnologías* (dir. por J. Sigüenza López), Thomson Reuters Aranzadi, Cizur Menor (Navarra), 2021, pp. 111-137.

Magro Servet, V.: "Hacia un domicilio electrónico obligatorio de las personas físicas ante la Administración Pública en materia de notificaciones", *Revista CEF Legal*, 2022, núm. 263, pp. 69-100.

Marcos Francisco, D.: "¡Se acabó la dispersión! El Tablón Edictal Judicial Único… Y algunos descuidos del legislador", *Actualidad Jurídica Aranzadi*, 24 junio 2021, núm. 975, p. 47.

Martín Delgado, I.: "Algunos aspectos problemáticos de la nueva regulación del uso de los medios electrónicos por las Administraciones Públicas", *Revista Jurídica de la Comunidad de Madrid*, 2018, pp. 1-47.

Martín Pastor, J.: "La digitalización de la Justicia y el reto de la garantía de los derechos fundamentales y de los principios del proceso", en AA.VV.: *El proceso como garantía* (dir. por J. M. Asencio Mellado y O. Fuentes Soriano), Atelier, Barcelona, 2023, pp. 213-235.

Moreno García, L.: "Las notificaciones procesales por medios electrónicos a la luz de la reciente constitucional", en AA.VV.: *La Justicia digital en España y la Unión Europea: situación actual y perspectivas de futuro* (dir. por J. Conde Fuentes y G. Serrano Hoyo), Atelier, Barcelona, 2019, pp. 61-70.

Perea González, A.: "«Aviso» vs «Acto de comunicación»: análisis y comentario a la Sentencia de 17 de enero de 2019 del Tribunal Constitucional", *Elderecho.*

com, 26 de febrero de 2019 (accesible en https://elderecho.com/aviso-vs-acto-comunicacion-analisis-comentario-constructivo-la-sentencia-17-enero-2019-del-tribunal-constitucional, consultada el 11.01.24).

Pérez Daudí, V.: "Diálogos para el futuro judicial XL. Los actos de comunicación en el marco de la Justicia Digital" (coord. por A. Perea González), *Diario La Ley*, 1 marzo 2022, núm. 10019 (edición electrónica).

Romero Pradas, M. I.: "Actos de comunicación y acceso al proceso: el emplazamiento del demandado en pronunciamientos recientes del Tribunal Constitucional", en AA.VV.: *El proceso como garantía* (dir. por J. M. Asencio Mellado y O. Fuentes Soriano), Atelier, Barcelona, 2023, pp. 479-492.

Sánchez Lamelas, A.: "La reciente jurisprudencia sobre la obligación de utilizar medios electrónicos en las relaciones administrativas", *Revista de Administración Pública*, 2023, núm. 220, pp. 183-217.

Valero Canales, A. L.: "Consideraciones procesales del expediente judicial electrónico", AA.VV.: *Modernización digital e innovación en la Administración de Justicia* (coord. por M. F. Gómez Manresa y M. Fernández Salmerón), Thomson Reuters Aranzadi, Cizur Menor (Navarra), 2019, pp. 343-367.

EL REGLAMENTO (UE) NÚM. 2020/1784 Y SU CONTRIBUCIÓN AL IMPULSO DE LA DIGITALIZACIÓN DE LA COOPERACIÓN JUDICIAL EN MATERIA CIVIL Y MERCANTIL EN LA UNIÓN EUROPEA*

REGULATION (EU) NO. 2020/1784 AND ITS CONTRIBUTION TO THE PROMOTION OF DIGITISATION OF JUDICIAL COOPERATION IN CIVIL AND COMMERCIAL MATTERS IN THE EUROPEAN UNION

Actualidad Jurídica Iberoamericana Nº 21, agosto 2024, ISSN: 2386-4567, pp. 190-223

* Este trabajo se ha realizado en el marco del Proyecto I+D: PID2021-123170OB-I00, "Claves para una justicia digital y algorítmica con perspectiva de género".. Todas las páginas web visitadas fueron accedidas por última vez el 1 de abril de 2024.

Guillermo
PALAO
MORENO

ARTÍCULO RECIBIDO: 29 de mayo de 2023
ARTÍCULO APROBADO: 1 de julio de 2024

RESUMEN: Durante los últimos años, y con mayor intensidad desde la crisis provocada por el COVID-19, la Unión Europea se ha marcado como objetivo potenciar el desarrollo de un mercado único digital, afectando directamente a políticas como la de cooperación judicial en materia civil y mercantil. Como resultado de este impulso, se han multiplicado los esfuerzos regulatorios, como se manifiesta en la elaboración del Reglamento (UE) núm. 2020/1784 relativo a la notificación y traslado en los Estados miembros de documentos judiciales y extrajudiciales en materia civil o mercantil ("notificación y traslado de documentos") (versión refundida). El cual, a pesar de su corta vida y debido a la efervescencia de esta actividad legislativa, ha sufrido ya dos modificaciones, para adaptarse a la gran velocidad con la que se suceden los intentos para favorecer la incorporación de herramientas digitales en este ámbito. De ahí la necesidad de analizar, no ya sólo los mecanismos digitales de notificación y traslado que ofrece el Reglamento (UE) núm. 2020/1784, sino poner este significativo instrumento en el contexto más amplio que supone la plena digitalización de cooperación judicial europea en materia civil o mercantil.

PALABRAS CLAVE: Unión Europea; digitalización de la justicia; cooperación judicial europea en materia civil y mercantil; notificación y traslado transfronterizo electrónico de documentos judiciales y extrajudiciales.

ABSTRACT: *During the past few years, and with greater intensity since the COVID-19 crisis, the European Union has set itself the objective of boosting the development of a digital single market, directly affecting policies such as judicial cooperation in civil and commercial matters. As a result of this impulse, regulatory efforts have multiplied, as illustrated by the elaboration of Regulation (EU) No 2020/1784 on the service in the Member States of judicial and extrajudicial documents in civil or commercial matters ("service of documents") (recast version). Despite its short life and due to the effervescence of this legislative activity, it has already undergone two amendments, in order to adapt to the rapid pace of attempts to promote the incorporation of digital tools in this field. Therefore, there is a need not only to analyse the digital service mechanisms offered by Regulation (EU) No 2020/1784, but also to place this significant instrument in the broader context of the full digitisation of European judicial cooperation in Civil or Commercial matters.*

KEY WORDS: European Union; digitalisation of justice; European judicial cooperation in Civil and commercial matters; cross-border electronic service of judicial and extrajudicial documents.

SUMARIO.- I. EL REGLAMENTO (UE) NÚM. 2020/1784 EN EL CONTEXTO DEL ESFUERZO EUROPEO PARA LA DIGITALIZACIÓN DE LA COOPERACIÓN JUDICIAL EN MATERIA CIVIL Y MERCANTIL.- 1. El imparable proceso de digitalización de la Justicia en la Unión Europea: desafíos y ventajas.- 2. Mercado único digital y cooperación judicial en materia civil y mercantil europea.- 3. La "refundición" del Reglamento europeo de notificaciones y la apuesta por la cooperación digitalizada.- II. NOVEDADES QUE INCORPORA EL REGLAMENTO (UE) NÚM. 2020/1784 PARA FAVORECER LA NOTIFICACIÓN TRANSFRONTERIZA DE DOCUMENTOS JUDICALES POR MEDIOS DIGITALES.- 1. La transmisión y notificación o traslado digital directa de documentos entre organismos estatales.- *A) Elementos del sistema informático descentralizado.- B) Funcionamiento del sistema informático descentralizado.* 2. La notificación y traslado electrónica y directa de documentos judiciales. 3. La notificación y traslado electrónicos mediante el punto de acceso electrónico europeo.- III. ASPECTOS PROBLEMÁTICOS Y CUESTIONES PENDIENTES: A MODO DE CONCLUSIÓN.

I. EL REGLAMENTO (UE) NÚM. 2020/1784 EN EL CONTEXTO DEL ESFUERZO EUROPEO PARA LA DIGITALIZACIÓN DE LA COOPERACIÓN JUDICIAL EN MATERIA CIVIL Y MERCANTIL.

Hoy por hoy resulta un lugar común destacar como las "Nuevas Tecnologías de la Información y de la Comunicación" (NTIC), están afectando a casi todas las esferas de nuestra vida en sociedad. Una incidencia que se concibe como más drástica en el caso de la paulatina entrada en juego de tecnologías disruptivas como la Inteligencia Artificial (IA), resultado de la conocida como Cuarta Revolución Industrial (4RI). Uno de los ámbitos donde esta afección digital se manifiesta, desde la perspectiva jurídica, lo constituye la propia administración de Justicia –pudiéndose hablar de Justicia electrónica o incluso algorítmica con la incorporación de la IA- vinculada a la propia digitalización que experimente la administración pública[1]. Un proceso que, a su vez, se habría visto acelerado en los últimos años, a partir de la vulnerabilidad demostrada por un sistema tradicional y puramente analógico de impartición de justicia, como se puso de manifiesto con la crisis global provocada por la pandemia del COVID-19[2].

1 Barona Vilar, S.: *Algoritmización del Derecho y de la Justicia. De la inteligencia artificial a la Smart Justice,* Tirant lo Blanch, Valencia, 2021, pp. 344 y ss.; Gómez Manresa, M.F.: "Derecho a la tutela judicial efectiva, Justicia abierta e innovación tecnológica", en AA.VV.: *Modernización digital e innovación en la administración de Justicia* (coord. por M.F. Gómez Manresa y M. Fernández Salmerón), Thomson Reuters Aranzadi, Pamplona, 2019, pp. 37-62; Kramer, X.: "Access to Justice and Technology: Trasnforming the Face of Cross-Border Civil Litigation and Adjudication in the EU", en AA.VV.: *eAccess to Justice* (ed. por K. Benyekhlef, J. Bailey, J. Burkell y F. Gelinas), University of Ottawa Press, Ottawa, 2023, pp. 351-375, p. 353.

2 Hernández López, A.: "La digitalización de la cooperación judicial en materia penal en la Unión Europea: propuestas y perspectivas legislativas", en AA.VV.: *El proceso penal ante la nueva realidad tecnológica europea*, (dir. por C. Arangüena Fanego, M. De Hoyos Sancho y E. Pillado González), Thomson Reuters Aranzadi, Pamplona, 2023, pp. pp. 281-306, pp. 281-282; Kramer, X., "Digitising access to justice: the next steps in the digitalisation of judicial cooperation in Europe", *Revista General de Derecho Europeo*, 2022, núm. 56, pp. 1-9, pp. 1-2; Ontanu, E.A.: "The digitalisation of European Union Procedures: A New Impetus Following a Time of prolonged Crisis", *Law, Tecnnology and Humans*, 2023, vol. 5 (1), pp. 93-110, p. 94; Ross, G.: "El traslado

• Guillermo Palao Moreno
Catedrático de Derecho Internacional privado, Universitat de Valéncia.
Correo electrónico: guillermo.palao@uv.es.

1. El imparable proceso de digitalización de la Justicia en la Unión Europea: desafíos y ventajas.

Las amplias y complejas repercusiones que se derivan de la mayor presencia de esta realidad tecnológica en la Justicia, habría dado lugar a diversas iniciativas institucionales -en primer lugar nacionales y, con posterioridad, desde distintos centros de codificación regional e internacional–; aunque en este estudio se hará referencia de forma señalada al interés que habría despertado en la Unión Europea (UE)[3]. Una atención y acción normativa que se vería motivada fundamentalmente por el objetivo doble de: tanto minimizar los evidentes riesgos que se encontrarían aparejados a la incorporación de las NTIC, así como en vistas de maximizar las también ventajas que ofrecen para la impartición de Justicia[4].

En otras palabras, como ha destacado reiteradamente -y constituiría un auténtico punto de arranque empleado por los legisladores, para justificar cada iniciativa surgida en este ámbito-, desde hace años la UE estaría impulsando profundos cambios legislativos, con la mencionada finalidad doble de: tanto fomentar la eficacia y la eficiencia de la Justicia –como beneficio más directo derivado de su modernización tecnológica, al que podría sumarse favorecer su resiliencia en supuestos de crisis globales-, como garantizar el acceso a la justicia y su correcta administración, afectando así al respeto de los derechos y de las garantías de un debido proceso a los ciudadanos –como riesgo más palpable derivado de la incorporación de estas innovaciones tecnológicas-[5].

Los retos y beneficios a los que se acaba de hacer mención se manifiestan, además y de una forma más evidente, en el contexto de la litigación civil o comercial internacional; entre otros, por las dificultades que entraña el hecho de que en tale casos entren en contacto distintos ordenamientos jurídicos estatales[6]. Y ello, no sólo por elevarse exponencialmente los riesgos señalados, sino también por el incremento de los costes del litigio y, de modo singular, los relacionados con el desarrollo de los actos de cooperación judicial que les dan soporte –sector

de los tribunales a la red: las lecciones que debemos aprender a partir de los errores ajenos", en AA.VV.: *Justicia digital, mercado y resolución de litigios de consumo. Innovación en el diseño del acceso a la justicia* (dir. por F. Esteban De La Rosa), Thomson Reuters Aranzadi, Pamplona, 2021, pp. 119-131, pp. 119-120.

3 Sobre la relevancia normativa de estos avances tecnológicos y su incidencia jurídico-privada en Europa, Fernández-Tresguerres, A.: *El Derecho privado europeo en la transformación digital*, Thamson Reuters Aranzadi, Pamplona, 2021, pp. 221-254.

4 Catalán Chamorro, M.J.: *La Justicia digital en España. Retos y desafíos*, Tirant lo Blanch, Valencia, 2023, pp. 53-60; Verbic, F.: "Application of New Technologies in Judicial Proceedings", en AA.VV.: *Technology, the Global Economy and other New Challenges for Civil Justice* (ed. por K. Miki), Intersentia, Cambridge, 2021, pp. 381-394, pp. 392-393.

5 Themeli, E.: "The frontiers of digital justice in Europe", en AA.VV.; *Frontiers in Civil Justice*, (ed. por X. Karnmer, J. Hoevernaas, B. Kas y E. Themeli), Edward Elgar, Cheltenham, 2022, pp. 102-120, pp. 103-104 y 119.

6 Gascón Inchausti, F.: "Electronic Service of Documents National and International Aspects", en AA.VV.: *Electronic Technology and Civil Procedure. New Paths to Justice from Around the World* (ed. por M. Kengyel y Z. Nemessányi), Springer, Heidelberg, 2012, pp. 137-180, pp. 176-177.

clave para la tutela de los derechos de defensa y en el que se centrará el presente análisis-; en el sentido, también doble, de: promocionar la eficacia y eficiencia en los procesos civiles y mercantiles con elementos de extranjería, así como garantizar el cumplimiento de los fines y principios que informan este sector, de modo particular, la seguridad jurídica y la tutela judicial efectiva[7].

De ahí que las implicaciones que actualmente supone la interfaz entre la cooperación judicial internacional y las NTICs, así como que esta cuestión haya despertado una legítima preocupación, no sólo para el legislador nacional[8], sino también para relevantes instituciones de ámbito universal y también regional[9]. Tal y como así sucede, en nuestro caso, con relación a la UE; como claramente se aprecia de la batería de instrumentos normativos que se han ido elaborado en su seno durante los últimos años, acudiendo principalmente a la base legal que proporcionaría el art. 81 del Tratado de Funcionamiento de la Unión Europa (TFUE), previsto para las situaciones carácter transfronterizo -esto es, entre un Estado miembro y otro-.

Un creciente y complejo conjunto normativo que, como se verá seguidamente y más allá del recurso a expedientes regulatorios más tradicionales -como el juego de principios como el de "neutralidad tecnológica" de las soluciones normativas o el de "equivalencia funcional" entre los documentos y herramientas analógicas y digitales-, habrían dado un paso más allá en la integración digital en la administración de la justicia en supuestos transfronterizos. Algo que se aprecia, no sólo al integrarse elementos relativos a la realidad digital en diversos preceptos y por recurrirse a las herramientas que proporcionan las NTICs, sino incluso llegando a privilegiarlas frente otras formas de cooperación, por medio de la inclusión del principio "digital por defecto" en los nuevos instrumentos europeos –como se verá seguidamente-.

2. Mercado único digital y cooperación judicial en materia civil y mercantil europea.

La preocupación que, en los últimos años, ha demostrado el legislador europeo en relación a la incidencia que el proceso de digitalización posee en el ámbito de la cooperación judicial internacional, debe analizarse en el contexto del desarrollo de un mercado único digital para Europa. Una potente iniciativa con la

7 Marchal Escalona, N.: *Garantías procesales y notificación internacional*, Comares, Granada, 2001, pp. 2-5; Virgós Soriano, M. y Garcimartín Alférez, F.J.: *Derecho Procesal Civil internacional. Litigación internacional*, Thomson Civitas, Madrid, 2007 (2ª ed.), pp. 439-440.

8 Ontanu, E.A.: "The digitalisation", cit., pp. 95-96.

9 Téngase en cuenta la "Hoja de ruta para la cooperación digital: aplicación de las recomendaciones del Panel de Alto Nivel sobre la Cooperación Digital" publicado en 2020 por la Organización de Naciones Unidas (ONU) (A/74/821), la "*OECD Framework and Good Practice Principles for People-Centred Justice*" (OECD Publishing, París, 2021) o el "2022-2025 CEPEJ Action plan: "Digitalisation for a better Justice" elaborado por la European Commission for the Efficiency of Justice (CEPEJ) (accesible en: https://rm.coe.int/cepej-2021-12-en-cepej-action-plan-2022-2025-digitalisation-justice/1680a4cf2c).

que se perseguiría, de forma principal, superar la fragmentación legal existente, aprovechar los beneficios de la economía digital para garantizar su soberanía digital, la eficiencia y sostenibilidad, al igual que para promover la existencia de sociedades abiertas, inclusivas, accesibles, justas y democráticas[10]. En definitiva, se encontraría motivada en el objetivo de favorecer "Una Europa Adaptada a la Era Digital"[11], como se subraya en el Programa "Europa Digital"[12], y en la Comunicación de 2020 "Configurar el futuro digital de Europa"[13]. Así las cosas, y como resultado directo de este impulso, cabría mencionar:

a) En primer lugar, los distintos textos centrados en el mencionado mercado único digital, como son el Reglamento (UE) núm. 2022/2065 del Parlamento Europeo y del Consejo, de 19 de octubre de 2022, relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales)[14], o el Reglamento (UE) núm. 2022/1925 del Parlamento Europeo y del Consejo de 14 de septiembre de 2022, sobre mercados disputables y equitativos en el sector digital y por el que se modifican las Directivas (UE) 2019/1937 y (UE) 2020/1828 (Reglamento de Mercados Digitales)[15].

b) Aunque sin por ello olvidar su preocupación, en segundo término, por las "personas" en el este contexto electrónico, como se precia en la "Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital"[16] que, por lo que a este estudio interesa, afecta a dos aspectos fundamentalmente: por un lado, la gobernanza europea de los datos, que obligaría a reconsiderar el Reglamento (UE) núm. 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)[17]. Tal y como subraya la "Estrategia europea de datos 2020" y se aprecia en el

10 En: https://www.consilium.europa.eu/es/policies/green-deal/.

11 En: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_es.

12 En: https://digital-strategy.ec.europa.eu/en/activities/digital-programme.

13 COM (2020) 67 final. Igualmente, Comunicación de la Comisión "eEuropa: una sociedad de la información para todos" (COM (1999) 687 final), a la que siguieron las Comunicaciones "Una Estrategia para el mercado único digital de Europa" (COM (2015) 192 final) o "Brújula Digital 2030: el enfoque de Europa para el decenio digital" (COM (2021) 118 final). *Vid.* Fernández Hernández, C.: "El nuevo marco regulatorio digital de la Unión Europea", en AA.VV.: *Marco normativo de la UE para la transformación digital* (dir. por E. Velasco Núñez), La Ley, Madrid, 2023, pp. 23-70, pp. 40-62.

14 *DO* núm. L 277, de 17 de octubre de 2022. Igualmente, Reglamento de Ejecución (UE) núm. 2023/1201 de la Comisión de 21 de junio de 2023, relativo a las disposiciones detalladas para la tramitación de determinados procedimientos por parte de la Comisión con arreglo al Reglamento (UE) núm. 2022/2065 del Parlamento Europeo y del Consejo («Ley de servicios digitales»). *DO* núm. L 159, de 22 de junio de 2023.

15 *DO* núm. L 265, de 12 de octubre de 2022. *Vid.* Fernández, J.: "Una panorámica del puzle de la regulación digital en la Unión Europea: telecomunicaciones, audiovisual, mercados y servicios digitales, datos, inteligencia artificial, ciberseguridad y derechos digitales", *Revista General de Derecho de los Sectores Regulados,* 2022, núm. 10, pp. 345-376.

16 COM (2022) 28 final.

17 *DO* núm. L 119, de 4 de mayo de 2016.

Reglamento (UE) núm. 2022/868 del Parlamento Europeo y del Consejo de 30 de mayo de 2022, relativo a la gobernanza europea de datos y por el que se modifica el Reglamento 2018/1724 (Reglamento de Gobernanza de Datos[18]. Por otro lado, igualmente afectaría a la generación de una Identidad Digital Europea[19], regulada actualmente por el Reglamento (UE) núm. 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE –también conocido como Reglamento eIDAS-[20], necesitado de una revisión para cumplir con los fines que marca la actual agenda digital UE[21].

Así las cosas, es en este complejo y altamente fragmentado contexto regulatorio europeo[22], donde se sitúa actualmente el proceso normativo dirigido a favorecer la digitalización en relación con la política de cooperación judicial en materia civil y mercantil de la UE; aportando, de este modo, el marco donde se desarrollan los distintos impulsos legislativos estratégicos desarrollados en el ámbito de la conocida como e-Justicia europea. Y ello, con la vista puesta en superar la actual fragmentación normativa y favorecer un mayor armonización digital procesal[23], así como fomentar la eficacia y la eficiencia en la administración de Justicia europea; garantizando a un tiempo tanto el acceso a la Justicia para todos como la tutela judicial efectiva referida en los arts. 4 del TFUE, 6 del Convenio Europeo de Derechos Humanos (CEDH) y 47 de la Carta de Derechos Fundamentales de la Unión Europea (CDFUE)[24].

18 *DO* núm. L 152, de 3 de junio de 2022.

19 En: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_es.

20 *DO* núm. L 257, 28 de agosto de 2014. También, Decisión de ejecución (UE) 2015/296 de la Comisión de 24 de febrero de 2015 por la que se establecen las modalidades de procedimiento para la cooperación entre los Estados miembros en materia de identificación electrónica con arreglo al art. 12, apartado 7, del Reglamento (UE) núm. 910/2014 del Parlamento Europeo y del Consejo relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (*DO* núm. L 53, de 25 de febrero de 2015).

21 Así la Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se modifica el Reglamento (UE) núm. 910/2014 en lo que respecta al establecimiento de un Marco para una Identidad Digital Europea (COM (2021) 281 final).

22 Wachowicz, M. y De Predigao Lana, P.: "Entendendo a fragmentação da Internet a partir de aspectos fundamentais sobre regulação, soberania digital e a experiência da União Europeia", en AA.VV.: *Direito e Ciberespaço* (coord. por E. Vera-Cruz Pinto y M.A. Marques da Silva), Quartier Latin, Sao Paulo, 2023, pp. 1-24.

23 Marchal Escalona, N.: "El nuevo marco europeo sobre notificación y obtención de pruebas en el extranjero: hacia un espacio judicial europeo digitalizado", *Revista Española de Derecho Internacional,* 2022, vol. 72, núm. 1, pp. 155-179, pp. 158-159.

24 Kramer, X.: "Access to Justice", cit., pp. 352 y 366-367; Merchán Murillo, A.: "Digitalización de las normas en materia de cooperación judicial internacional", *Latin American Journal of European Studies*, 2019, vol. 3, núm. 1, 2023, pp. 152-179, pp. 157-159.

Unos loables objetivos que, a su vez, se han hecho presentes en: los "Planes Plurianuales de Acción" que se han sucedido desde 2007[25]; las Conclusiones del Consejo sobre Eurojust de 2019[26]; la Comunicación "La digitalización de la Justicia en la UE un abanico de oportunidades" de 2020[27]; o la "Estrategia Europea Relativa a la Justicia en Red para 2024-2028" de 2023[28].

Nos situamos, por lo tanto, ante un nutrido conjunto de documentos de origen europeo a partir de los cuales se habrían desarrollo diversos instrumentos legislativos y herramientas técnicas, que despliegan una gran transcendencia para favorecer la digitalización este ámbito:

a) Así, por lo que hace a esta segunda dimensión técnica, cabe destacar la generación del "Portal Europeo de e-Justicia" y del "Atlas Civil Europeo"[29]; la constitución de la "Agencia de la Unión Europea para la gestión operativa de sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia" (EU-LISA)[30]; la publicación del "*Justice scoreboard*"[31]. Al igual que donde se enmarcan los destacados Reglamentos (UE) núm. 2019/818, marco para la interoperabilidad de los sistemas de información de la UE, y núm. 2022/850, sistema informatizado para la distribución y el intercambio electrónico transfronterizo de datos procesales en el ámbito de la Cooperación judicial en materia civil y penal -esto es, el sistema e-CODEX (*e-Justice Communication via on-line Data Exchange*)-[32]. Con lo que, de algún modo, se estaría procediendo a institucionalizar

25 Su arranque, sin embargo, podría situarse en 2003, a partir de las distintas peticiones cursadas a la Comisión, por el Consejo y el Parlamento Europeo, como destaca Arangüena Fanego, C.: "La acción de la Unión Europea en materia de e-Justicia", en AA.VV.: *La e-Justicia en la Unión Europea. Desarrollos en el Ámbito Europeo y en los ordenamientos nacionales* (coord. por A. de la Oliva Santos, F. Gascón Inchausti y M. Aguilera Morales), Thomson Reuters Aranzadi, Pamplona, 2012, pp. 23-68, p. 25.

26 *DO* núm. L 412, de 9 de diciembre de 2019. La cual habría dado lugar, entre otros, a la creación de "La Unidad Europea de Cooperación Judicial en la era digital".

27 COM (2020) 710 final.

28 En: https://www.consilium.europa.eu/es/press/press-releases/2023/12/08/eu-takes-important-step-towards-digitalisation-of-justice-systems/.

29 En: https://e-justice.europa.eu/home?action=home.

30 Reglamento (UE) núm. 2018/1726 del Parlamento Europeo y del Consejo de 14 de noviembre de 2018, relativo a la Agencia de la Unión Europea para la Gestión Operativa de Sistemas Informáticos de Gran Magnitud en el Espacio de Libertad, Seguridad y Justicia (eu-LISA), y por el que se modifican el Reglamento (CE) núm. 1987/2006 y la Decisión 2007/533/JAI del Consejo y se deroga el Reglamento (UE) núm. 1077/2011 (*DO* núm. L 259, de 21 de noviembre de 2018). Igualmente, el Reglamento (UE) 2019/818 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, relativo al establecimiento de un marco para la interoperabilidad entre los sistemas de información de la UE en el ámbito de la cooperación policial y judicial, el asilo y la migración y por el que se modifican los Reglamentos (UE) 2018/1726, (UE) 2018/1862 y (UE) 2019/816 (*DO* núm. L 135, de 22 de mayo de 2019).

31 En: https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/upholding-rule-law/eu-justice-scoreboard_en#assessingnationaljusticesystems.

32 Sobre el e-CODEX, Cristian, N., Dragos, S. y Haldi, K.: "L'e-CODEX et la plateforme europèenne de transmission des documents", en AA.VV. : *La signification des actes judiciaires et extrjudiciaires en Europe. Anlyses, jurisprudences et perspectives du Règlement UE núm. 2020/1784* (dir. por M. Schmitz), Bruylant, Brusleas, 2022, pp. 105-119; Velicogna, M.: "Coming to Terms with Complexity Overload in Transborder e-Justice: The e-CODEX Platform", en AA.VV.: *The Circulation of Agency in E-Justice Law* (ed. por F. Contini y G.F. Lanzara), Springer, Heidelberg, 2014, pp. 309-330.

al e-CODEX, como el sistema de gestión de las comunicaciones en situaciones transfronterizas estándar[33].

b) Mientras que, desde una perspectiva legislativa, y como resultado de la Comunicación de 2020 "La digitalización de la Justicia en la UE un abanico de oportunidades", varios instrumentos en materia de cooperación judicial en materia civil (y penal) europea que, con una base en el art. 81 TFUE y diseñados para situaciones transfronterizas, contemplan la incorporación de las NTICs. En este sentido, cabe citar los Reglamento (UE) núm. 2020/1783 del Parlamento Europeo y del Consejo de 25 de noviembre de 2020, relativo a la cooperación entre los órganos jurisdiccionales de los Estados miembros en el ámbito de la obtención de pruebas en materia civil o mercantil ("obtención de pruebas") (versión refundida); el Reglamento (UE) núm. 2020/1784 del Parlamento Europeo y del Consejo de 25 de noviembre de 2020, relativo a la notificación y traslado en los Estados miembros de documentos judiciales y extrajudiciales en materia civil o mercantil ("notificación y traslado de documentos") (versión refundida)[34]; el Reglamento de Ejecución (UE) núm. 2022/422 de la Comisión de 14 de marzo de 2022, por el que se establecen las especificaciones técnicas, las medidas y otros requisitos para la implementación del sistema informático descentralizado a que se refiere el Reglamento (UE) núm. 2020/1783 del Parlamento Europeo y del Consejo; el Reglamento de Ejecución (UE) núm. 2022/423 de la Comisión de 14 de marzo de 2022, por el que se establecen las especificaciones técnicas, las medidas y otros requisitos para la implementación del sistema informático descentralizado a que se refiere el Reglamento (UE) núm. 2020/1784 del Parlamento Europeo y del Consejo[35]; o el Reglamento (UE) núm. 2023/2844 del Parlamento Europeo y del Consejo de 13 de diciembre de 2023, sobre la digitalización de la cooperación judicial y del acceso a la justicia en asuntos transfronterizos civiles, mercantiles y penales, y por el que se modifican determinados actos jurídicos en el ámbito de la cooperación judicial; así como la Directiva (UE) núm. 2023/2843 del Parlamento Europeo y del Consejo de 13 de diciembre de 2023, por la que se modifican las Directivas 2011/99/UE y 2014/41/UE del Parlamento Europeo y del Consejo, la Directiva 2003/8/CE del Consejo y las Decisiones Marco 2002/584/JAI, 2003/577/JAI, 2005/214/JAI, 2006/783/JAI, 2008/909/JAI, 2008/947/JAI, 2009/829/JAI y

33 Al respecto, Ontanu, E.A.: "The digitalisation", cit., p. 105; Requejo Isidro, M.: "Article 5. Means of communication to be used by transmitting agencies, receiving agencies and central bodies", en AA.VV. *The European Service Regulation* (ed. por A. Anthimos y M. Requejo Isidro), Edward Elgar, Cheltenham, 2023, pp. 71-75, p. 72; Themeli, E.: "The frontiers", cit., pp. 112-114; Vicario Pérez, A.M.: "Cooperación judicial digital en la Unión Europea, e-CODEX como sistema de intercambio electrónico transfronterizo de datos procesales", en AA.VV.: *Cooperación judicial civil y penal en la Unión Europea. Retos pendientes y nuevos desafíos ante la transformación digital del proceso* (dir. por P.R. Suárez Xavier y A.M. Vicario Pérez), Bosch, Barcelona, 2023, pp. 233-266, pp. 240-262.

34 *DO* núm. L 405, de 2 de diciembre de 2020. Sobre el segundo, téngase la corrección de errores publicada en *DO* núm. L 188, de 27 de julio de 2023.

35 *DO* núm. L 87, de 15 de marzo de 2022.

2009/948/JAI del Consejo, en lo que respecta a la digitalización de la cooperación judicial[36].

Sin embargo, antes de continuar con la exposición, resulta de interés dejar constancia de cómo, con anterioridad a la mencionada Comunicación de 2020[37], los elementos digitales ya habían hecho acto de presencia –aunque de forma tímida- en textos de gran calado en el contexto de esta política europea[38]. Como así habría sucedido con: el Reglamento (UE) núm. 1215/2012 del Parlamento Europeo y del Consejo, de 12 de diciembre de 2012 , relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil (versión refundida)[39]; el Reglamento (UE) núm. 524/2013 del Parlamento Europeo y del Consejo, de 21 de mayo de 2013, sobre resolución de litigios en línea en materia de consumo y por el que se modifica el Reglamento (CE) núm. 2006/2004 y la Directiva 2009/22/CE, donde se contempla la resolución d este tipo de controversias por medio del empleo a una Plataforma europea de Resolución de los Litigios en Línea[40], los Reglamentos (CE) núm. 861/2007 del Parlamento Europeo y del Consejo, de 11 de julio de 2007, por el que se establece un proceso europeo de escasa cuantía y Reglamento (CE) núm. 1896/2006 del Parlamento Europeo y del Consejo, de 12 de diciembre de 2006 , por el que se establece un proceso monitorio europeo[41].

Pues bien, ha sido en este comprometido y fértil contexto –al igual que fragmentado, a pesar de la intervención del legislador de la UE- donde se enmarca la publicación del mencionado Reglamento (UE) núm. 2020/1784 –que, como se ha señalado, se habría visto acompañado posteriormente del Reglamento de Ejecución (UE) núm. 2022/423 y más recientemente modificado por el Reglamento (UE) núm. 2023/2844-. La elección del mismo respondería, por consiguiente, a su importancia en este proceso legislativo europeo. No en vano, la notificación y traslado de documentos transfronteriza constituye un ámbito privilegiado que habría centrado la atención regulatoria del legislador europeo, ya desde el inicio del proceso codificador en materia de cooperación judicial en materia civil o

36 *DO* núm. L, de 27 de diciembre de 2023. El Reglamento (UE) 2022/2844 ha sido aprovechado, a su vez, para realizar una modificación puntual del Reglamento (UE) núm. 2020/1784, modificando sus arts. 12.7 y 13.3, así como incorporando un nuevo art. 19 *bis*, por medio de su art. 24.

37 Kramer, X.: "Access to Justice", cit., pp. 354-362; Themeli, E.: "The frontiers", cit., pp. 110-112.

38 Ontanu, E.A.: "The digitalisation", cit., p. 97.

39 *DO* núm. L 351, de 20 de diciembre de 2012. Así, por medio del principio de "equivalencia funcional", al establecer en su art. 25.1 la garantía de la validez de los acuerdos de sumisión a foro celebrados por medios electrónicos.

40 *DO* núm. L 165, de 18 de junio de 2013.

41 Respectivamente en *DO* núm. L 199, de 31 de julio de 2007 y *DO* núm. L 399, de 30 de diciembre de 2006. *Vid.* Barel, B.: "Le notificazioni nello spazio giuridico europeo dopo il regolamento (UE) 2020/1784", *Riv. dir.int.pr.proc.* 2022, núm. 3, pp. 531-561, p. 560; Hernández López, A.: "La digitalización", cit., pp. 285-305; Kramer, X.: "Digitising access to justice", cit., p. 4-5.

mercantil[42]; siendo que se trata de uno de los primeros Reglamentos europeos donde se ha apostado claramente por la incorporación de las herramientas que proporcionan las NTICs. Por lo que, en resumidas cuentas, el Reglamento "notificación y traslado de documentos"–sin restar importancia al Reglamento de "obtención de pruebas"- se nos presenta como un instrumento de singular importancia en este ámbito, para poder comprobar el alcance y la proyección del proceso de digitalización del sistema de cooperación judicial civil y comercial europeo en su conjunto.

3. La "refundición" del Reglamento europeo de notificaciones y la apuesta por una cooperación transfronteriza digitalizada.

Como se puede observar, uno de los primeros resultados palpables de este impulso legislativo europeo hacia la digitalización de la cooperación judicial civil o comercial –y al margen de lo previsto en el coetáneo Reglamento (UE) núm. 2020/1783 ("obtención de pruebas")[43]– ha sido la elaboración de Reglamento (UE) núm. 2020/1784 ("notificación y traslado de documentos"). A este respecto ha de subrayarse que, por medio de este instrumento, no sólo se ha procedido a actualizar y a refundir del Reglamento (CE) núm. 1393/2007 del Parlamento Europeo y del Consejo, de 13 de noviembre de 2007, relativo a la notificación y al traslado en los Estados miembros de documentos judiciales y extrajudiciales en materia civil o mercantil («notificación y traslado de documentos») y por el que se deroga el Reglamento (CE) núm. 1348/2000 del Consejo[44], al igual que incorporar la jurisprudencia emitida por el TJUE durante su vigencia[45], sino que se han dado importantes pasos en el camino de la digitalización del sector de la notificación y traslado de documentos judiciales y extrajudiciales en la UE.

Sin embargo, de forma previa al estudio de las novedades tecnológicas que incorpora el Reglamento (UE) núm. 2020/1784 ("notificación y traslado de documentos"), resulta necesario enfrentarse –aunque sea brevemente- a sus elementos esenciales y hacer mención de las novedades que -al margen de las

42 *Vid.* Gielen, P.: "Entreaide judiciaire au sein de l'union européenne: origne", en AA.VV. : *La signification,* cit., pp. 11-22.

43 Sobre el mismo y las novedades que incorpora, Fumagalli, L.: "Problemi vecchi e nuovi nella cooperazione per l'assunzione delle prove all'estero in materia civile: la rifusione della disciplina nell'unione europa", *Riv. dir.int.pr.proc.*, 2021, núm. 4, pp. 844-877; Richard, V.: "La refonte du règlement sur l'obtention des preuves en matière civile", *Rev. Crit. DIP*, 2021, 1(1) pp. 67-77.

44 *DO* núm. L 324, de 10 de diciembre de 2007. Modificado por el Reglamento (UE) núm. 517/2013 del Consejo, de 13 de mayo de 2013, por el que se adaptan determinados Reglamentos y Decisiones en los ámbitos de la libre circulación de mercancías, la libre circulación de personas, el derecho de sociedades, la política de competencia, la agricultura, la seguridad alimentaria, la política veterinaria y fitosanitaria, la política de transportes, la energía, la fiscalidad, las estadísticas, las redes trans-europeas, el poder judicial y los derechos fundamentales, la justicia, la libertad y la seguridad, el medio ambiente, la unión aduanera, las relaciones exteriores, la política exterior, de seguridad y defensa y las instituciones, con motivo de la adhesión de la República de Croacia (*DO* núm. L 158 de 10 de junio de 2013).

45 Payan, G.: "Actualité jurispridentielle européenne du Règlement (CE) núm. 1393/2007 du novembre 2007", en AA.VV. : *La signification,* cit., pp. 23-48.

digitales- incorpora frente a su antecesor directo, el Reglamento (CE) núm. 1393/2007.

a) Así, por lo que hace a sus elementos esenciales, cabe destacar como entre los objetivos que perseguiría el Reglamento "notificación y traslado de documentos" se situarían: la mejora y la agilización de los procedimientos de notificación y traslado de documentos transfronteriza; favoreciendo, en consecuencia, tanto la garantía de la tutela judicial efectiva, el acceso a la justicia, la transparencia, la seguridad jurídica y la tutela de los derechos fundamentales, como la eficacia, la eficiencia, la sostenibilidad y la resiliencia del sistema, a partir de favorecer la celeridad, simplificación, racionalización del sistema y –como no- su digitalización[46].

Por lo que hace a su contenido y estructura, el Reglamento "notificación y traslado de documentos" consta de 4 Capítulos, dedicados sucesivamente a cuestiones como: establecer las "*Disposiciones generales*" (Capítulo I), regular el régimen de transmisión de los "*Documentos judiciales*" (Capítulo II), y de los "Documentos extrajudiciales" (Capítulo III), al que se acompañan por último unas "*Disposiciones finales*" (Capítulo IV). Por su parte, este instrumento europeo incorpora 3 Anexos donde se incluyen: tanto los formularios que van a ser utilizados a lo largo del procedimiento de notificación y traslado de documentos (Anexo I, numerados de la A a la I), la referencia al Reglamento (CE) núm. 1393/2007 derogado y sus modificaciones (Anexo II), y la tabla de correspondencias del articulado entre su antecesor y el nuevo Reglamento (Anexo III).

En relación a la concreción de su ámbito de juego, su art. 1 se refiere a su ámbito de aplicación material –afectado a este tipo de actos de cooperación transfronteriza en materia civil y mercantil, cuando un documento judicial o extrajudicial deba transmitirse de un Estado miembro otro con el fin de ser notificado o trasladado a este último[47]-, siguiendo en gran medida la delimitación objetiva seguida por sus precedentes -al margen de los que se mencionarán a continuación, acompañado de las definiciones que recoge de forma novedosa el art. 2-[48]. A su vez, el Reglamento resulta territorialmente de aplicación para y entre todos los Estados miembros de la UE, siempre que el domicilio de la persona destinataria de la notificación o del traslado del documento sea desconocido, como dispone su art. 1.2[49] –salvo la lógica exclusión del Reino Unido tras el

46 Considerado 3. Marchal Escalona, N.: "El nuevo marco europeo", cit., pp. 158 y 168-171.

47 Téngase en cuenta lo establecido en los Considerandos 6 y 7. Richard, V.: "La refonte du règlement sur la notification des actes judiciaires et extrajudiciaries", *Rev.crit. DIP*, 2021, núm. 2, pp. 349-360, p. 351. Sobre los problemas que todavía suscita la delimitación de su carácter "transfronterizo", Aguilera Morales, M.: "El Reglamento (UE) 2020/1784 sobre notificación y traslado trasfronterizo de documentos: novedades e implicaciones internas", *Revista General de Derecho Europeo*, 2022, núm. 57, pp. 6-36, pp. 10-12.

48 Ibid.: pp. 9-10.

49 Sobre esta cuestión, el mecanismo de asistencia en la determinación de dicha dirección que incorpora su art. 7. *Vid.* Aguilera Morales, M.: "El Reglamento (UE) 2020/1784", cit., pp. 12-14; Marchal Escalona, N.: "El nuevo marco europeo", cit., pp. 170-171.

Brexit[50]- gracias a la voluntad de Irlanda de participar en el mismo y la firma de un acuerdo *ad hoc* con Dinamarca que permite su juego al respecto de este país[51].

Por último, y sobre la aplicación del Reglamento "notificación y traslado de documentos" desde una perspectiva temporal, y según lo previsto en su art. 35, este instrumentos europeo entró en vigor el 1 de julio de 2022; claro está, a excepción de lo dispuesto en sus arts. 5, 8 y 10 –relativos al sistema de transmisión directa de documentos por vía electrónica-, que se aplicarán a partir del primer día del mes siguiente al período de tres años después de la entrada en vigor de los actos de ejecución que debe adoptar la Comisión a los que se refiere el art. 25 –relativos al establecimiento del sistema informático centralizado-, como así se prevé en su art. 37.2; así como habrá que esperar dos años, tras la entrada en vigor de los actos de ejecución a los que hace referencia el art. 10.3, a) del Reglamento (UE) 2023/2844, para la puesta en aplicación del art. 19 *bis*, como se contempla en el art. 37.3[52].

b) Por otra parte, y por lo que hace a las novedades incorporadas por medio del Reglamento (UE) núm. 2020/1784, y al margen de los aspectos puramente digitales –de los que se dará debida cuenta en el apartado II-, cabe destacar dos de modo principal, los cuales se ven referidos a sus arts. 1 y 2.

Así, por un lado, y por lo que hace al primero, cabe destacar dos previsiones que afectan a los numerales 2 y 3 del art. 1. De este modo, para empezar, al establecer su ámbito de aplicación material, este precepto incorpora una excepción a su delimitación negativa en su numeral 2º, directamente relacionada con los supuestos de desconocimiento de la dirección de la persona a quien haya de realizarse la notificación o el traslado; buscando, de este modo, cubrir aquellos casos de asistencia en vistas a su determinación a los que se refiere –igualmente de forma novedosa- el art. 7. Asimismo, al respecto de su numeral 3º, se incluye una nueva excepción, relativa a los casos de notificación o traslado de documentos en el propio Estado miembro del foro, cuando se tratase de un representante autorizado por la persona quien tuviera que recibirla, sin consideración del lugar donde residiera esta persona.

Por otro lado, en el art. 2 incluye e*x novo* dos definiciones de interés -también al respecto de la digitalización de estos actos de auxilio judicial transfronterizo, entre Estados miembros-, sobre dos conceptos que se utilizan a lo largo del

50 A pesar de lo establecido en su Considerando 47.

51 Por lo que respecta a Irlanda, téngase en cuenta el Considerando 47. Sobre Dinamarca, a pesar de lo dispuesto en el Considerando 48, véase el Acuerdo entre la Comunidad Europea y el Reino de Dinamarca relativo a la notificación y al traslado de documentos judiciales y extrajudiciales en materia civil o mercantil (*DO* núm. L 19, de 21 de enero de 2021).

52 Éste último, incorporado a partir de la modificación que realiza el art. 24, 4) del Reglamento (UE) 2023/2844.

articulado del Reglamento. Así, en su apartado 1 se delimita "Estado miembro del foro" como aquel país donde se va a desarrollar el procedimiento judicial en cuestión, en cuyo marco se va a solicitar la cooperación a la autoridad judicial de otro Estado miembro. Junto a ello, en el 2º apartado se define el central "sistema informático descentralizado", de singular importancia para este estudio –y que se examinará con más detalle en el próximo apartado-, con el siguiente tenor: "una red de sistemas informáticos nacionales y puntos de acceso interoperables, que opera bajo la responsabilidad y la gestión individuales de cada Estado miembro y permite un intercambio transfronterizo de información seguro y fiable entre los sistemas informáticos nacionales"[53].

Sin embargo, no cabe duda alguna de que entre las novedades más destacables que ofrece el Reglamento (UE) núm. 2020/1784, se sitúan aquellas relativas a al fomento de la digitalización de los actos de comunicación judicial transfronterizos que este instrumento ordena. Las cuales se encuentran directamente vinculadas, como se ha mencionado anteriormente, a la apuesta realizada por el legislador europeo en incorporar herramientas digitales en los distintos instrumentos relacionados con la cooperación judicial europea[54]. Una firme voluntad que, en términos generales, se manifiesta principalmente en contemplar diversas formas de notificación o traslado de documentos por medio del recurso a herramientas digitales –con el fin de aprovechar todo el potencial que ofrecen las NTICs y siempre atento a los riesgos que estas herramientas implican-; aunque, sobre todo, a partir de la prioridad que se proporciona a la vía digital de cooperación frente a otras formas más tradicionales de comunicación judicial –en atención al principio "digital por defecto" en que se fundamenta el instrumento europeo-.

Así, como se expondrá con más detalle en el siguiente apartado, cabe destacar como el Reglamento "notificación y traslado de documentos" se apoya en una serie elementos técnicos y jurídicos por medio de los que va a potenciar esta incorporación tecnológica, sin olvidar la necesidad de garantizar la tutela de los derechos procesales fundamentales previsto en el derecho de la UE, así como la protección de la privacidad y de los datos personales que se hubieran transmitidos que únicamente podrán utilizarse para tales fines[55]. Todo ello, como se ha expuesto al inicio de este estudio, con la finalidad de favorecer la confianza de los particulares en un mercado interior europeo crecientemente digital.

Una apuesta tecnológica que se manifiesta principalmente por medio de tres novedades especialmente significativas. Esto es, con un ánimo puramente

53 *Vid.* Ontanu, E.A.: "Article 2. Definitions", en AA.VV. :*The European Service Regulation,* cit., pp. 59-63, pp. 61-62.

54 Barel, B.: "Le notificazioni", cit., p. 535; Richard, V.: "La refonte du règlement sur la notification", cit., p. 352.

55 Arts. 31 y 32. Considerandos 41 y 42.

enunciativo, contemplando no sólo la cooperación directa entre organismos transmisores y receptores en los diversos Estados miembros por medio de un sistema informático descentralizado seguro y fiable -como se prevé principalmente en sus arts. 5 y 8 a 15-; sino incorporando también la eventualidad de acudir alternativa y excepcionalmente a otras vías de auxilio judicial[56], como sería la notificación o traslado electrónico de documentos -como se recoge en su art. 19- o el recurso a la posibilidad de llevar a cabo la notificación y traslado electrónicos mediante el punto de acceso electrónico europeo -como prevé el art. 19 *bis*-[57]. A tales supuestos se hará referencia sucesivamente a continuación.

II. NOVEDADES QUE INCORPORA EL REGLAMENTO (UE) NÚM. 2020/1784 PARA FAVORECER LA NOTIFCACIÓN TRANSFRONTERIZA DE DOCUMENTOS JUDICIALES POR MEDIOS DIGITALES.

El Reglamento (UE) núm. 2020/1784 apuesta fuertemente por la digitalización de los procedimientos transfronterizos de notificación y traslado de documentos judiciales -y extrajudiciales, como recuerda su art. 21[58]-, respondiendo así a la agenda que habría marcado la Comunicación "La digitalización de la Justicia en la UE un abanico de oportunidades" de 2020. En este sentido, son diversas las menciones que se realizan en su articulado a esta incorporación tecnológica que, en último extremo, se concreta en la previsión de tres medios de asistencia judicial basados en los NTICs. Por un lado y con carácter principal, la cooperación directa entre organismos estatales por medio de un sistema informático descentralizado; mientras que, por otro lado, de forma subsidiaria y alternativos entre sí, se sitúan tanto la notificación y el traslado electrónico directo de documentos, como la notificación y traslado electrónicos mediante el punto de acceso electrónico europeo.

En consecuencia, por medio de la incorporación se perseguiría fundamentalmente aprovechar los beneficios que tales herramientas de comunicación proporcionan y reducir así los riesgos que presenta su empleo en la práctica. Unos objetivos que, en concreto, pretenden alcanzarse mediante una armonización legislativa a escala europea. Hay que tener presente, a este respecto, como esta realidad tecnológica ya se encuentra presente en la normativa procesal de diversos Estados miembros, aunque coexistiendo ciertas desigualdades que generan distorsiones en el mercado interior. De ahí este esfuerzo armonizador que, debido a la base jurídica empleada –el art. 81 TFUE- únicamente puede referirse a los supuestos

56 Richard, V.: "La refonte du règlement sur la notification", cit., p. 353.

57 Aguilera Morales, M.: "El Reglamento (UE) 2020/1784", cit., p. 9; Kramer, X.: "Frontiers of Civil Justice – Privatizing, Digitizing and Funding Justice", en AA.VV.: *Frontiers in Civil Justice: Privatisation, Monetisation and Digitisation*, (ed. por X. Kramer, J. Hoevernaars, B. Kas y E. Themeli), Cheltenham, Edward Elgar, 2020, pp. 1-20, pp. 5-6.

58 Considerado 8.

de naturaleza transfronteriza. Sin embargo, no cabe duda de que esta regulación a servir igualmente de catalizador y de modelo para los Estados miembros en relación con las situaciones de notificación o traslado puramente internas, estando así llamada así a favorecer un deseado proceso de aproximación legislativa en los Estados miembros en este ámbito en el seno de la UE.

1. La transmisión y notificación o traslado digital directa de documentos entre organismos estatales.

Una de las novedades que, desde la perspectiva de la digitalización, resulta más reseñable del Reglamento (UE) núm. 2020/1784, consiste en prever un mecanismo electrónico de transmisión documental directa entre las autoridades de los Estados miembros, a través del mencionado sistema informático descentralizado; tal y como se regula en la Sección 1ª de su Capítulo II[59]. Así, por medio de esta inclusión, se da un importante paso a favor del empleo de las NTICs en este ámbito[60], a diferencia del silencio que había guardado el Reglamento (CE) núm. 1393/2007 sobre este extremo –a pesar de que en varios Estados miembros ya se contaba con tales medios en el momento de su publicación-[61]. No obstante, como se ha expuesto anteriormente, su plena eficacia dependerá de la puesta en marcha de los actos de ejecución a los que se refiere el art. 25, debido a que habrá que esperar a que transcurran 3 años tras su entrada en vigor, como nos recuerda el art. 37.2[62].

A) Elementos del sistema informático descentralizado.

En este sentido, los elementos principales de este mecanismos de comunicación digital, tanto personales, como materiales, van a ser: tanto los organismos transmisores y receptores de solicitudes de cooperación, al igual que el órgano central en cada Estado miembro, así como el desarrollo de un sistema informático descentralizado que les de soporte al respecto de la puesta en práctica de los actos de comunicación que lleven a cabo entre tales organismos[63]:

59 Considerando 10.

60 Su incorporación ya había sido prevista en las propuestas que condujeron al actual Reglamento, como destaca Dominelli, S.: *Current and future perspectives on Cross-birder Service of Documents*, Aracne, Canterano, 2018, p. 161.

61 Aguilera Morales, M.: "El Reglamento (UE) 2020/1784", cit., p. 15. Un silencio que ya había sido criticado por la doctrina. Así, Cebrián Salvat, M.A.: *La notificación internacional en materia civil y mercantil en la Unión Europa*, Comares, Granada, 2018, pp. 100-102; Ybarra Bores, A.: "El sistema de notificaciones en la Unión Europea en el marco del Reglamento 1393/2007 y su aplicación judicial", *Cuadernos de Derecho Transnacional*, 2013, vol. 5, núm. 2, pp. 481-500, p, 500.

62 Richard, V.: "La refonte du règlement sur la notification", cit., p. 352.

63 Barel, B.: "Le notificazioni", cit., p. 535; Marchal Escalona, N.: "El nuevo marco europeo", cit., pp. 159-162. Al respecto de sus implicaciones técnicas, normativas y costes, Hernández López, A.: "La digitalización", cit., pp. 300-301; Merchán Murillo, A.: "Digitalización de las normas", cit., pp. 159-167.

a) Por una parte, como ya sucedía con anterioridad y desde una perspectiva personal, tal y como se establece en el art. 3, cabe subrayar la importancia que van a seguir teniendo los organismos transmisores y receptores; concebidos para enviar y recibir los documentos judiciales y extrajudiciales en cuestión –o cumplir con ambas funciones-. Los cuáles –ya sean funcionarios públicos, autoridades u otras personas competentes- y como se dispone en los numerales 1 a 3, van a estar designados por cada Estado miembro -por períodos de cinco años-, así como –en atención a lo establecido en el numeral 4- estos igualmente habrán de facilitar a la Comisión la información relativa a estos organismos –entre la que se encontraría, su nombre y dirección, ámbito territorial, medios de recepción y lenguas utilizables para cumplimentar los formularios incluidos en el anexo I-[64].

Junto a ello, como contempla el art. 4, los Estados miembros también habrán de designar un órgano central –o más de uno, en el caso de Estados miembros federales-, llamados a desempeñar funciones de facilitación de información, resolución de las dificultades que pudieran surgir en la transmisión, así como expedir solicitudes de notificación y traslado de documentos en casos excepcionales y a petición del organismo transmisor competente. Al respecto se debe destacar que, como exige el art. 37.2, la información relativa a estos organismos y al funcionamiento del Reglamento, también se va a tener que facilitar por cada Estado miembros a la Comisión, para su publicación en el *DOUE* –estando disponible en el portal e-*Justice*-, con el fin de elaborar y actualizar regularmente un manual con todas estas informaciones, como se prevé en el art. 23[65].

b) Por otra parte, desde un punto de vista material, el elemento más novedoso por lo que respecta a la digitalización de los actos de transmisión y notificación o traslado de documentos de carácter transfronterizo, sería la previsión del desarrollo de un sistema informático descentralizado. Al mismo se refiere el art. 5.1 al establecer los "Medios de comunicación que deben utilizar los organismos transmisores, los organismos receptores y los órganos centrales". Un relevante precepto donde se prevé que las comunicaciones cubiertas por el Reglamento "notificación y traslado de documentos" tengan que llevarse a cabo por medio del empleo de un sistema informático descentralizado, interoperable, seguro y fiable; cuya definición se sitúa en el art. 2.2 antes mencionado, refiriéndose al mismo como una red de sistemas nacionales y de puntos de acceso de gestión que serán de responsabilidad nacional, donde se debe garantizar tanto la interconectividad y la interoperabilidad segura y fiable de los sistemas informáticos nacionales, como que permita el intercambio de datos[66]. A este respecto, y como se dispone en

64 Marchal Escalona, N.: "El nuevo marco europeo", cit., pp. 162-163; Requejo Isidro, M.: "Article 3. Transmitting and receiving agencies", en AA.VV.: *The European Service Regulation,* cit., pp. 64-67.

65 Considerando 36.

66 Barel, B.: "Le notificazioni", cit., pp. 544-545; Chardon, M.: "Le novueau Règlement (UE) 2020/1784 présenté aux practciens"; en AA.VV.: *La signification,* cit., pp. 75-103, pp. 93-94; Prats Jané, S.: *La cooperación*

sus apartados 2 y 3, cuando se recurra a servicios de confianza cualificados o si se tuviera que utilizar un sello electrónico cualificado o una firma electrónica cualificada, habrá que tener en cuenta lo previsto en el Reglamento 910/2014, ya citado.

Nos situamos ante un sistema que, en definitiva, resultará de uso obligatorio para las autoridades transmisoras y receptoras, al consagrarse en este precepto el principio "digital por defecto"[67]; modificando así la anterior doctrina establecida por el TJUE, por medio de la que se consideraban todos los medios de comunicación como alternativos y sin que existirá una jerarquía entre los mismos, como sí se establece en el nuevo Reglamento. No obstante, como se recoge en el art. 5.4, en caso de que resultara imposible acudir al mismo, se podrá optar por una vía de transmisión alternativa rápida y adecuada, por medio de la que se avale la fiabilidad y la seguridad en la transmisión[68].

Por lo que respecta a aquellos extremos de carácter más directamente técnico, el sistema que diseña el Reglamento "notificación y traslado de documentos" consistirá, en un primer momento, en el desarrollo de un sistema informático que, con las notas características de descentralizado seguro y fiable, permitiría la interconexión y la interoperabilidad de los sistemas informáticos nacionales. Y ello, a partir del sistema informático de código abierto que permite la interconectividad de los sistemas nacionales con el e-CODEX[69], que actualmente se gestiona por la agencia europea eu-LISA.

Un sistema informático de referencia del que, como indica el art. 27, la Comisión se responsabilizará de su creación, mantenimiento y desarrollo[70]; mientras que, como se dispone en el art. 28, los Estados miembros asumirán la instalación, funcionamiento y mantenimiento de los puntos de acceso interconectados e interoperables al sistema informático descentralizado[71]. Mientras que, en una segunda fase de ejecución, se procedería a su sustitución por un programa informático de aplicación de referencia que, elaborado por la propia Comisión, se encontraría disponible para su uso para los Estados miembros; garantizando de este modo, tanto la integridad y la fiabilidad del documento transmitido, así

jurídica internacional en el ámbito civil y mercantil en España: notificaciones, obtención y practica de prueba, Bosch, Barcelona, 2022, pp. 54-55; Requejo Isidro, M.: "Article 5", cit., pp. 72-74.

67 STJUE de 9 de febrero de 2006, en el asunto C-473/04, *Plumex* (ECLI:EU:C:2006:96). Al respecto, Marchal Escalona, N.: "El nuevo marco europeo", cit., p. 160; Ontanu, E.A.: "The digitalisation", cit., p. 99; Requejo Isidro, M.: "Article 3", cit., pp. 65-66; Sujecki, B.: "Neufassung der Europäischen Zustellungsverordnung", *EuZW*, 2021, pp. 286-290, p. 288.

68 Considerando 15.

69 Aguilera Morales, M.: "El Reglamento (UE) 2020/1784", cit., pp. 16-17. Crítico, Richard, V.: "La refonte du règlement sur la notification", cit., p. 353.

70 Considerandos 12 y 13.

71 Aguilera Morales, M.: "El Reglamento (UE) 2020/1784", cit., p. 32.

como la necesaria seguridad e interoperabilidad del sistema para el intercambio de información entre las autoridades estatales[72].

Para la viabilidad de este sistema, al margen de la significativa consagración del principio "digital por defecto" que consagra el art. 5, el Reglamento "notificación y traslado de documentos" incorpora igualmente dos preceptos de gran relevancia práctica en el ámbito analizado[73].

a) Por un lado, resultaba imprescindible que se otorguen plenos efectos jurídicos de los documentos electrónicos, como establece su art. 6; incorporando así en el texto reglamentario la aplicación de los principios antes mencionados de "neutralidad tecnológica" y de "equivalencia funcional"[74]. De tal forma que, a partir de este momento, no se podrá denegar los efectos jurídicos a los documentos en formato electrónico que se pudieran transmitir a través del sistema informático descentralizado, ni se podrán considerar inadmisibles como prueba en los procedimientos judiciales.

b) Por otro lado, el art. 7 contempla que el Estado miembro requerido ofrezca asistencia al requirente en la determinación de la dirección de la persona a quien hubiera de notificarse o trasladarse el documento, según las opciones previstas, cuando se desconociera la misma[75]. Así, como dispone su numeral 1º y por lo que hace a las formas de esta asistencia, tanto nombrando autoridades a las que pudieran dirigir sus solicitudes, como por medio de solicitudes de información por vía electrónica o directamente proporcionando esta información (así como su modificación posterior) en el Portal Europeo e-Justicia. Una información que, como establece el apartado 2º, habrá de ser facilitada por cada Estado a la Comisión para, con posterioridad, estar disponible en el Portal Europeo de e-Justicia, comprendiendo: los medios de asistencia que se prevean, los nombres y datos de contacto de las autoridades, así como las iniciativas de averiguación que, acudiendo a los registros o utilizando bases de datos, puedan desarrollar las autoridades del Estado requerido, si la dirección indicada no fuera correcta.

B) Funcionamiento del sistema informático descentralizado.

Por lo que respecta a la operativa de la transmisión y notificación o traslado directo, que descansa en el sistema informático descentralizado europeo –tal y como se desarrolla en los arts. 8 a 15 del Reglamento (UE) núm. 2020/1784-

72 Así, el mencionado Reglamento (UE) núm. 2022/850.

73 Aguilera Morales, M.: "El Reglamento (UE) 2020/1784", cit., p. 15.

74 Considerando 16. *Vid.* Hess, B.: "Article 6. Legal effects of electronic documents", en AA.VV. : *The European Service Regulation,* cit., pp. 76-78; Prats Jané, S.: *La cooperación,* cit., p. 55; Richard, V.: "La refonte du règlement sur la notification", cit., p. 353.

75 Aguilera Morales, M.: "El Reglamento (UE) 2020/1784", cit., pp. 31-32.

, señalar de modo inicial cómo está previsto que se desarrolle en tres fases sucesivas –que, en su mayor medida y a salvo de los novedosos elementos digitales, corresponden en estructura y dinámica con lo establecido en los arts. 4 a 11 de su precedente el Reglamento (CE) núm. 1393/2007-, para la que se dispondría de una serie de formularios estandarizados de uso obligatorio, que se encuentran incorporados en el anexo I diseñados para facilitar su puesta en funcionamiento de modo uniforme[76].

a) En primer lugar, el art. 8 regula la fase de transmisión de documentos judiciales entre los organismos responsables de la transmisión y recepción[77]. Una acción que, como disponen sus numerales 1º y 2º, se llevará a cabo directamente y lo antes posible[78], utilizando para acompañar la solicitud el formulario A del anexo 1, en la lengua oficial del Estado miembro requerido –o una de ellas si cuenta con varias-, o la que el país requerido hubiera indicado a la Comisión como posible para cumplimentar el formulario. Como resulta habitual en este tipo de instrumentos, el numeral 3 recuerda que los documentos transmitidos están exentos de legalización o trámite equivalente. Por último, en el apartado 4 se recuerda a la autoridad solicitante la necesidad de que remita el documento por duplicado, en aquellos caos en los que solicitara que se le devolviera una copia del documento en soporte papel, tal y como contempla el art. 5.4, con el certificado que dispone el art. 14 al ordenar el certificado y copia del documento notificado o trasladado.

b) En segundo lugar, el art. 10 se consagra a la fase de recepción de los documentos[79]. El cual, como recoge su numeral 1º, consistirá en un acuse de recibo al órgano transmisor utilizando el formulario D del anexo I, con la mayor celeridad posible y siempre antes de los siete días desde su recepción. En todo caso, como se prevé en el apartado 2, caso de que surgieran contingencias por deficiencias en la información documentación transmitida, el organismo receptor contactará al efecto con el transmisor a la mayor brevedad, utilizando el formulario E del anexo I; mientras que, en atención al numeral 3, si la solicitud escapara del ámbito de aplicación del Reglamento "notificación y traslado de documentos" o le resultara imposible realizar la notificación o traslado por no cumplir con las formalidades, se comunicará en el menor plazo de tiempo posible con la autoridad solicitante empleando el formulario F del anexo I.

76 Anexo I. Considerandos 17-24 y 38.

77 Marchal Escalona, N.: "El nuevo marco europeo", cit., pp. 163-164; Stürner, M.: "Article 8. Transmission of documents", en AA.VV.: *The European Service Regulation,* cit., pp. 86-92.

78 Aunque no se prevé sanción alguna en caso de retraso injustificado, como señala Stürner, M.: "Article 8", cit., p. 87.

79 Aguilera Morales, M.: "El Reglamento (UE) 2020/1784", cit., p. 17; Stürner, M.: "Article 10. Receipt of documents by receiving agency", en AA.VV.: *The European Service Regulation,* cit., pp. 96-100.

El precepto no prevé negativa alguna a recibir el documento por motivos de orden público[80]. Sin embargo, caso de que la dificultad en la notificación residiera en la falta de competencia territorial del organismo receptor, el apartado 4 establece que la autoridad requerida trasmitirá la solicitud a quien lo fuera en su país, informando de ello a la solicitante por medio del formulario G del anexo I; una vez recibida la solicitud y el documento por el efectivamente competente, este organismo enviara un acuse de recibió a la requirente original, por medio del formulario H de dicho nexo.

c) En tercer lugar, el art. 11 prevé la última fase de entrega de la notificación o traslado del documento[81]. Un acto procesal sobre el que no se disponen reglas uniformes y que se llevará a cabo, como consigna su apartado 1, bien según lo establecido en la normativa del país requerido –remitiendo así a la legislación del foro-, o bien según la forma requerida por el transmisor, siempre que no resultase incompatible con el Derecho del receptor. Para cumplir con esta solicitud, como establece el numeral 2º, contra con un plazo de 1 mes desde su recepción. Sin embargo, caso de resultar imposible cumplir con este plazo, informará al solicitante por medio del formulario K o, si I transmisor hubiera solicitado información por medio del formulario I, responderá utilizando el anexo J; y, además, continuará con las diligencias, si previera un plazo razonable para lograrlo, mientras que la autoridad requirente no le indique que ya no resultase necesario.

Por último, y como dispone el art. 14.1, cumplidos los trámites por parte del organismo receptor, éste remitirá al transmisor un certificado donde se acredite dicho cumplimiento utilizando el formulario K del anexo I y, caso de que se hubiera solicitado una copia del documento ex art. 8.4, se adjuntará el mismo. El régimen lingüístico de este certificado y el correspondiente anexo K se desarrolla en el apartado 2º del art. 14, debiendo redactarse en la lengua –o una de las oficiales- del país solicitante, o aquella que hubiera indicado como admisible.

Por lo que respecta a otras previsiones relevantes incorporadas en el Reglamento "notificación y traslado de documentos", para el funcionamiento del sistema se refieren a extremos como: la traducción de los documentos, la negativa del destinatario a aceptar la notificación o traslado del documento o al pago de los gastos que supone esta actuación. A las mismas se hará referencia sucinta, ya que éstas no incorporan diferencias reseñables al modelo precedente. Sobre el primer extremo, el art. 9 contempla la tradicional negativa del destinatario a aceptar el documento si no estuviera redactado en una de las lenguas a las que se refiere el art. 12; siendo que, en principio, será el requirente quien sufrague dicha

80 Ibid.: p. 97.

81 Al respecto, Marchal Escalona, N.: "El nuevo marco europeo", cit., pp. 164; Stürner, M.: "Article 11. Service of documents", en AA.VV.: *The European Service Regulation,* cit., pp. 101-104.

traducción, salvo que no se alcanzara una decisión posterior sobre este tema por la autoridad competente.

Por su parte, el régimen de gastos se establece en el art. 15, reiterando el modelo establecido con anterioridad en el Reglamento europeo de notificaciones precedente. Un precepto donde se contempla la exclusión de toda obligación de abono o reembolso de tasas o costas al Estado miembro requerido, salvo en los supuestos en que a petición del organismo transmisor se acudiera a un funcionario judicial o persona competente, o se hubiera empleado un modo particular de notificación o traslado.

Tampoco plantea grandes novedades sobre el modelo anterior, el particularmente significativo desde un punto de vista práctico art. 12 –cuyos precedentes habrían dado lugar a una fértil casuística en el seno del TJUE-, al establecer el importante derecho con el que cuenta el destinatario de no aceptar la notificación o traslado –principalmente por no cumplir con el régimen lingüístico al que se refiere el Reglamento, como se subraya en sus apartados 1 y 2-[82]. Y ello, de forma principal, a salvo de: incorporar evidentes mejoras de redacción -como se precia de modo significativo en su apartado 5, cuando aborda la cuestión de la subsanación de la notificación o traslado no aceptado-, las variaciones que ha sufrido la numeración de los formularios a utilizar en la notificación o traslado –resultando utilizable principalmente para este fin el formulario L, junto a antes mencionado K del anexo I-, o la más reciente modificación de su numeral 7 –a partir de la previsión contenida en el art. 24, 1) del Reglamento (UE) núm. 2023/2844[83].

2. La notificación y traslado electrónica y directa de documentos judiciales.

Otra de las novedades más reseñables que, en vistas a garantizar la eficiencia y celeridad de los procedimientos judiciales transfronterizos, desde la perspectiva de la digitalización de la cooperación judicial en materia civil y mercantil transfronteriza, ofrece el Reglamento (UE) núm. 2020/1784 se centra en la posibilidad de realizar la notificación y traslado electrónico directo de los documentos judiciales, como se regula en su art. 19[84]; donde se incorpora un medio de transmisión subsidiario al "sistema informático centralizado", de entre las diversas alternativas que, con una

82 Marchal Escalona, N.: "El nuevo marco europeo", cit., pp. 164-165.

83 Así, el nuevo tenor de este apartado s el siguiente: "7. A efectos de los apartados 1 y 2, los agentes diplomáticos o funcionarios consulares, cuando se efectúe la notificación o el traslado con arreglo al artículo 17, o la autoridad o la persona, cuando se efectúe con arreglo a los artículos 18, 19, 19 bis o 20, informarán al destinatario de que puede negarse a aceptar la notificación o el traslado del documento y de que el formulario L del anexo I o la declaración escrita de negativa de aceptación deben enviarse a esos agentes o funcionarios o a esa autoridad o persona, respectivamente.".

84 Considerando 31. *Vid.* Anthimos, A.: "Article 19. Electronic service", en AA.VV.: *The European Service Regulation,* cit., pp. 177-190; Barel, B.: "Le notificazioni", cit., pp. 554-556; Chardon, M.: "Le novueau Règlement", cit., pp. 94-96; Marchal Escalona, N.: "El nuevo marco europeo", cit., pp. 173-176.

validez equivalente y sin jerarquización, se prevén en la Sección 2ª de su Capítulo II[85].

Al respecto de los mismos cabe apuntar, de forma inicial, como no cabe duda de que este mecanismo de cooperación se presenta como singularmente ágil y eficiente en la práctica en relación con la litigación de naturaleza transfronteriza, siendo de hecho ya una realidad plena en diversos Estados miembros[86]; por lo que, de forma indirecta, su plasmación en el texto reglamentario estaría llamada a dar un impulso significativo en la armonización legislativa que persigue el legislador europeo, con respecto a aquellos Estados miembros que todavía no cuentan con esta alternativa de cooperación judicial[87]. No obstante, este avance y su efectividad real debe valorarse de forma cauta, si se advierte el modo y alcance como ha sido incorporado por parte del legislador europeo[88].

Pues bien, pasando a su análisis, en el art. 19.1 se contempla la posibilidad de llevar a cabo una notificación o un traslado de forma directa en otro Estado miembro. Para empezar, esto podrá ser así, en los supuestos en los que tales personas cuenten con una dirección conocida. Para cumplir con este fin, se podrán acudir a cualquier medio electrónico que estuviera disponible en el ordenamiento del Estado miembro del foro[89].

De ahí que, como se dispone en su numeral 2º, con el objetivo de garantizar la seguridad de la transmisión que se llevase a cabo, así como la integridad de su contenido y su recepción, todo Estado miembro puede comunicar a la Comisión aquellas condiciones que estime como adicionales en vistas a aceptar la notificación o el traslado electrónico. Tal y como se contempla en el numeral 1, b), siempre y cuando en su ordenamiento se estipulen requisitos más estrictos o cuando no se prevea la notificación o traslado por medio del correo electrónico.

Sobre este medio de comunicación, y por lo que hace a los requisitos exigibles, como se especifica en sus letras a) y b), podrá resultar empleado siempre y cuando estos documentos: o bien se envíen y reciban por medio de la utilización de servicios cualificados de entrega electrónica certificada –tal y como prescribe

85 Stürner, M.: "Article 8", cit., p. 89; Sujecki, B.: "Neufassung", cit., p. 289.

86 Téngase en cuenta, el Informe final publicado en 2016 del proyecto JUST/2014/JCOO/PR/CIVI/0049, titulado" Study on the Service of Documents. Comparative legal analysis of the relevant laws and practices of the Member States". Al respecto, Aguilera Morales, M.: "El Reglamento (UE) 2020/1784", cit., p. 23; Marchal Escalona, N.: "El nuevo marco europeo", cit., pp. 173-174; Ontanu, E.A.: "The digitalisation", cit., p. 100; Richard, V.: "La refonte du règlement sur la notification", cit., p. 354; Sujecki, B.: "Neufassung", cit., p. 290.

87 Anthimos, A.: "Article 19", cit., p. 178-179. Para el caso español, Aguilera Morales, M.: "El Reglamento (UE) 2020/1784", cit., pp. 35-36.

88 Anthimos, A.: "Article 19", cit., pp. 179-180; Stein, A.: "The European Service Regulation: Introduction", en AA.VV.: *The European Service Regulation,* cit., pp. 1-25, p. 6.

89 Sobre sus implicaciones internas, Aguilera Morales, M.: "El Reglamento (UE) 2020/1784", cit., pp. 32-34.

el anteriormente mencionado Reglamento 910/2014[90]- y el destinatario hubiera prestado su consentimiento expreso para el empleo de estas herramientas; o bien que se recurra un correo electrónico a una dirección electrónica concreta a los efectos de la notificación y traslado, así como cuando el destinatario hubiera prestado un consentimiento expreso y previo a la autoridad competente o a la parte encargada de realizar esta actuación[91].

Al respecto de dicho consentimiento, en particular, hay que tener en cuenta que de forma general, éste podrá manifestarse durante los procedimientos judiciales, por medio del recurso a servicios cualificados de entrega electrónica certificada[92]; mientras que si se prestara en un procedimiento concreto, sin que se hubiera recurrido a dicho servicio cualificado, debería poder acreditarse que se hubiera recibido del documento por parte de su destinatario, en atención a los requisitos previstos normativamente por los propios Estados miembros, en vistas a garantizar la seguridad de la transmisión que se hubiera efectuado[93].

La posibilidad que ofrece este medio de transmisión cuenta con indudables beneficios, entre los que se situarían el ahorro de tiempo y de costes, más aún para la litigación de carácter transfronteriza, alineándose con los objetivos de eficacia y de eficiencia que persigue el legislador de la UE. No obstante, su potencial armonizador se ve minimizado en cierta medida, debido tanto consentimiento que se exige sobre el empleo de los mecanismos que prevé, así como por razón de las numerosas cuestiones que deja abiertas y las remisiones que se realiza a la *lex fori*[94]. Además, la diversidad regulatoria al respecto de esta forma de comunicación entre los Estados miembros y los riesgos que suscita la brecha digital en este ámbito, podría suscitar problemas con su propia compatibilidad de este modo de comunicación con el derecho a la tutela judicial efectiva previsto en los arts. 47 de la CDFUE y 6.1 de CEDH[95]. Aunque, tal vez se trataba de la reforma posible, aunque no la deseable, como primer paso a una incorporación tecnológica d mayor calado y con menos requisitos en próximas reformas del Reglamento[96].

90 Al respecto, Anthimos, A.: "Article 19", cit., p. 185.

91 Por lo que, además de no poder imponerse, no se aceptará cualquier mecanismo digital de comunicación, Aguilera Morales, M.: "El Reglamento (UE) 2020/1784", cit., p. 24; Richard, V.: "La refonte du règlement sur la notification", cit., p. 354.

92 Considerando 32. Esto es, como se establece en el mencionado Reglamento (UE) núm. 910/2014.

93 Considerando 33. *Vid.* Ontanu, E.A.: "The digitalisation", cit., p. 101.

94 Aguilera Morales, M.: "El Reglamento (UE) 2020/1784", cit., pp. 25-26; Anthimos, A.: "Article 19", cit., pp. 187-190; Ontanu, E.A.: "The digitalisation", cit., p. 100; Sujecki, B.: "Neufassung", cit., p. 289.

95 Marchal Escalona, N.: "El nuevo marco europeo", cit., p. 158.

96 Stein, A.: "The European Service Regulation", cit., p. 7.

3. La notificación y traslado electrónicos mediante el punto de acceso electrónico europeo.

Junto a los anteriores modos de cooperación judicial internacional electrónica, recientemente se habría previsto un nuevo mecanismo de comunicación donde igualmente se recurre a herramientas digitales, y que opera como alternativo al que acaba de mencionarse en el apartado anterior. En este sentido, el art. 19 *bis* establece la posibilidad de acudir a una notificación y traslado electrónicos mediante el denominado como punto de acceso electrónico europeo. Una posibilidad no incluida *ab initio*, sino que se habría incorporado a partir de la previsión de modificación del Reglamento (UE) núm. 2020/1784, por medio de lo dispuesto en el art. 24, 4) del Reglamento (UE) núm. 2023/2844.

En este sentido, destaca como en el art. 4 del Reglamento (UE) núm. 2023/2844 se introduce e*x novo* la creación de un punto de acceso electrónico europeo dentro del Portal Europeo de e-Justicia, para garantizar el acceso a la justicia de todos[97], y de cuya gestión técnica, desarrollo, accesibilidad, mantenimiento, seguridad y asistencia técnica a los usuarios será responsable la Comisión –como dispone su apartado 3º-[98]. A este respecto, su art. 2, 4) lo define como "un portal accesible a las personas físicas y jurídicas o a sus representantes, en toda la Unión, que está conectado a un punto de acceso interoperable en el contexto del sistema informático descentralizado".

Así las cosas, este portal podrá ser empleado para la comunicación electrónica entre personas físicas o jurídicas o sus representantes y las autoridades competentes en relación con, entre otros instrumentos europeos en materia de cooperación judicial en materia civil y mercantil, el Reglamento (UE) núm. 2020/1784; incorporando, de esta manera, una nueva vía digital de notificación y traslado de documentos judiciales con carácter transfronterizo en seno de la UE.

De este modo, en atención a lo establecido en su numeral 1º, igualmente se podrá notificar o trasladar documentos judiciales directamente en otro Estado miembro, siempre que la dirección de la persona destinataria de la misma fuera conocida, por medio del punto de acceso electrónico europeo que se ha establecido a partir del artículo 4.1 del Reglamento (UE) 2023/2844. Para ello, además de que se conozca su dirección, se requerirá que el destinatario hubiera prestado su consentimiento de forma previa y expresa, a favor del empleo de este medio electrónico a efectos de la notificación y de traslado de documentos durante el transcurso del procedimiento judicial en cuestión[99].

97 Considerandos 10. 27 y 30 del Reglamento (UE) núm. 2023/2844.

98 Art. 10 del Reglamento (UE) núm. 2023/2844. Incluidos los costes aparejados al mismo, como se destaca en su art. 13.6.

99 Art. 4.6 del Reglamento (UE) núm. 2023/2844.

En esta línea, en su apartado 2 se contempla que en estos supuestos el destinatario habrá de confirmar la recepción de los documentos por medio de un acuse de recibo donde figure constancia de la fecha de recepción; siendo que la fecha de la notificación y del traslado de tales documentos se encontrará indicada en el acuse de recibo. A este respecto, por lo que se refiere a los supuestos de subsanación de una notificación o un traslado de documentos que no hubieran sido no aceptados de documentos en atención a los previsto en el artículo 12.5, resultará de aplicación esta misma norma.

III. ASPECTOS PROBLEMÁTICOS Y CUESTIONES PENDIENTES: A MODO DE CONCLUSIÓN.

Dentro de los múltiples esfuerzos encaminados por el legislador europeo para consolidar un Mercado único digital, se sitúan aquellos que, como el Reglamento (UE) núm. 2020/1784 "notificación y traslado de documentos", se centran en promocionar la digitalización de la Justicia civil y mercantil en el interior de la UE. Una acción normativa que, por lo que respecta a esta política, en particular y en estos momentos, en atención a las propias limitaciones competenciales de las instituciones europeas, se despliega con una gran intensidad y con un ímpetu muy significativo en la incorporación de herramientas digitales en la Cooperación judicial civil y mercantil europea, cuyo objeto lo constituyen las situaciones transfronterizas.

En este efervescente contexto regulatorio hay que dar la bienvenida a la publicación del Reglamento (UE) núm. 2020/1784 –todavía de aplicación parcial-, por medio del que el legislador europeo no sólo refunde su precedente anterior, sino que también provecha para adaptar su articulado a los avances que había experimentado la jurisprudencia del TJUE, al igual que –por lo que importa para este estudio- con el objeto de incorporar las herramientas informáticas que ofrecen las NTICs, al respecto de los actos de comunicación entre las autoridades judiciales de los Estados miembros –junto a la incorporación novedades tecnológicas actos de ejecución-. Así, por lo que hace a este último extremo, destaca como a partir de este Reglamento, no sólo se contempla la obligatoriedad de la comunicación digital en situaciones intracomunitarias - por medio de un sistema informático descentralizado seguro y fiable-, sino que se admite sin ambages la posibilidad de realizar comunicaciones digitales directas entre los jueces estatales –por medios del correo electrónico o el recurso a un punto de acceso electrónico europeo-, impulsando la intervención de servicios de identificación y confianza para su gestión, impulsando igualmente la institucionalización de e-CODEX.

No cabe duda que el resultado finalmente alcanzado cuenta con ciertas limitaciones que ofrecen un golpe de realidad a la euforia que podría implicar este

significativo avance en términos tecnológico. Aunque también es cierto es que supone un paso de una indudable relevancia en este sentido de incorporación de las NTICs en la regulación europeo relativa a la notificación y traslado de documentos y por ofrecer un destacable nivel de confianza en el recurso a estos avances tecnológicos. Una modernización que merece una valoración positiva, no ya sólo para estos concretos actos de comunicación, sino para el conjunto de actos que van a ir desarrollándose con posterioridad en el ámbito de la Cooperación judicial civil europea en su conjunto. Todo ello sin dejar de lado el impulso que está llamado a significar a favor de la armonización legislativa autónoma interna entre los Estados miembros al respecto de las situaciones de cooperación judicial doméstica por medios digitales y, en general, de la Justicia electrónica.

Esta valoración positiva no esconde, empero, el hecho de que los resultados alcanzados por medio del Reglamento (UE) núm. 2020/1784, muestren ciertas limitaciones y deficiencias, así como que todavía exista un amplio margen de mejora, por razón de los aspectos regulatorios que deja pendientes. Podría decirse que al legislador europeo le ha faltado algo de arrojo, pero no hemos de olvidar que la redacción final de este instrumento europeo responde a un compromiso político en un medio normativo ampliamente fragmentado, donde la incorporación de los medios electrónicos en la administración de Justicia resulta desigual, existiendo profundas diferencias en el nivel de su digitalización y confianza en estos medios entre los Estados miembros.

Así las cosas, para empezar y en esta línea crítica, se ha de llamar la atención a las numerosas remisiones que se realizan a la *lex fori* a lo largo del articulado del Reglamento, como se ha advertido en el presente estudio, derivando en una uniformidad normativa parcial de las cuestiones que ordena. Junto a ello, por lo que respecta a la notificación o traslado electrónico de documentos, en los supuestos de imposibilidad de utilizar la plataforma, impide el pleno impulso de la digitalización de la cooperación judicial, el hecho de la voluntariedad en el empleo del correo electrónico.

En otro orden de ideas, no menos importante es tener en consideración que, para la plena implantación de todas las posibilidades que ofrece el Reglamento "notificación y traslado de documentos" hay que esperar todavía a la consecución de los actos de ejecución que, diseñados hasta 2025, van a tener que acometerse para dotar de las infraestructuras informáticas y programas necesarios para su plena puesta en marca -como son el programa informático e referencia, la mencionada plataforma y el propio punto de acceso electrónico europeo-. En definitiva, aunque en estos momentos no resultaba posible llegar más lejos fuera de este consenso y que hemos de estar atentos a los actos de ejecución que permitan comprobar todas las potencialidades que ofrece el Reglamento (UE)

núm. 2020/1784, lo cierto es que por medio del mismo se han sentado unas bases sólidas para el anclaje y evolución futura de la e-Justicia en la UE.

BIBLIOGRAFÍA

ANTHIMOS, A.: "Article 19. Electronic service", en AA.VV.: *The European Service Regulation* (ed. por A. ANTHIMOS y M. REQUEJO ISIDRO), Edward Elgar, Cheltenham, 2023, pp. 177-190.

AGUILERA MORALES, M.: "El Reglamento (UE) 2020/1784 sobre notificación y traslado trasfronterizo de documentos: novedades e implicaciones internas", *Revista General de Derecho Europeo*, 2022, núm. 57, pp. 6-36.

ARANGÜENA FANEGO, C.: "La acción de la Unión Europea en materia de e-Justicia", en AA.VV.: *La e-Justicia en la Unión Europea. Desarrollos en el Ámbito Europeo y en los ordenamientos nacionales* (coord. por A. DE LA OLIVA SANTOS, F. GASCÓN INCHAUSTI y M. AGUILERA MORALES), Thomson Reuters Aranzadi, Pamplona, 2012, pp. 23-68.

BAREL, B.: "Le notificazioni nello spazio giuridico europeo dopo il regolamento (UE) 2020/1784", *Riv.dir.int.pr.proc.* 2022, núm. 3, pp. 531-561.

BARONA VILAR, S.: *Algoritmización del Derecho y de la Justicia. De la inteligencia artificial a la Smart Justice,* Tirant lo Blanch, Valencia, 2021.

CATALÁN CHAMORRO, M.J.: *La Justicia digital en España. Retos y desafíos*, Tirant lo Blanch, Valencia, 2023.

CEBRIÁN SALVAT, M.A.: La notificación internacional en materia civil y mercantil en la Unión Europa, Comares, Granada, 2018.

CHARDON, M.: "Le novueau Règlement (UE) 2020/1784 présenté aux practciens"; AA.VV. : *La signification des actes judiciaires et extrjudiciaires en Europe. Anlyses, jurisprudences et perspectives du Règlement UE núm. 2020/1784* (dir. por M. SCHMITZ), Bruylant, Brusleas, 2022, pp. 75-103.

CRISTIAN, N., DRAGOS, S. y HALDI, K.: "L'e-CODEX et la plateforme europèenne de transmission des documents", en AA.VV. : *La signification des actes judiciaires et extrjudiciaires en Europe. Anlyses, jurisprudences et perspectives du Règlement UE núm. 2020/1784* (dir. por M. SCHMITZ), Bruylant, Brusleas, 2022, pp. 105-119.

DOMINELLI, S.: *Current and future perspectives on Cross-birder Service of Documents*, Aracne, Canterano, 2018.

FERNÁNDEZ HERNÁNDEZ, C.: "El nuevo marco regulatorio digital de la Unión Europea", en AA.VV.: *Marco normativo de la UE para la transformación digital* (dir. por E. VELASCO NÚÑEZ), La Ley, Madrid, 2023, pp. 23-70.

Fernández, J.: "Una panorámica del puzle de la regulación digital en la Unión Europea: telecomunicaciones, audiovisual, mercados y servicios digitales, datos, inteligencia artificial, ciberseguridad y derechos digitales", *Revista General de Derecho de los Sectores Regulados,* 2022, núm. 10, pp. 345-376.

Fernández-Tresguerres, A.: *El Derecho privado europeo en la transformación digital*, Thamson Reuters Aranzadi, Pamplona, 2021.

Fumagalli, L.: "Problemi vecchi e nuovi nella cooperazione per l'assunzione delle prove all'estero in materia civile: la rifusione della disciplina nell'unione europa", *Riv.dir.int.pr.proc.*, 2021, núm. 4, pp. 844-877.

Gascón Inchausti, F.: "Electronic Service of Documents National and International Aspects", en AA.VV.: *Electronic Technology and Civil Procedure. New Paths to Justice from Around the World* (ed. por M. Kengyel y Z. Nemessányi), Springer, Heidelberg, 2012, pp. 137-180.

Gielen, P.: "Entreaide judiciaire au sein de l'union européenne: origne", en AA.VV. : *La signification des actes judiciaires et extrjudiciaires en Europe. Anlyses, jurisprudences et perspectives du Règlement UE núm. 2020/1784* (dir. por M. Schmitz), Bruylant, Brusleas, 2022, pp. 11-22.

Gómez Manresa, M.F.: "Derecho a la tutela judicial efectiva, Justicia abierta e innovación tecnológica", en AA.VV.: *Modernización digital e innovación en la administración de Justicia* (coord. por M.F. Gómez Manresa y M. Fernández Salmerón), Thomson Reuters Aranzadi, Pamplona, 2019, pp. 37-62.

Hernández López, A.: "La digitalización de la cooperación judicial en materia penal en la Unión Europea: propuestas y perspectivas legislativas", en AA.VV.: *El proceso penal ante la nueva realidad tecnológica europea*, (dir. por C. Arangüena Fanego, M. De Hoyos Sancho y E. Pillado González), Thomson Reuters Aranzadi, Pamplona, 2023, pp. pp. 281-306.

Hess, B.: "Article 6. Legal effects of electronic documents", en en AA.VV.: *The European Service Regulation* (ed. por A. Anthimos y M. Requejo Isidro), Edward Elgar, Cheltenham, 2023, pp. 76-78

Kramer, X.: "Digitising access to justice: the next steps in the digitalisation of judicial cooperation in Europe", *Revista General de Derecho Europeo*, 2022, núm. 56, pp. 1-9.

Kramer, X.: "Access to Justice and Technology: Trasnforming the Face of Cross-Border Civil Litigation and Adjudication in the EU", en AA.VV.: *eAccess to Justice*

(ed. por K. Benyekhlef, J. Bailey, J. Burkell y F. Gelinas), University of Ottawa Press, Ottawa, 2023, pp. 351-375.

Kramer, X.: "Frontiers of Civil Justice – Privatizing, Digitizing and Funding Justice", en AA.VV.: *Frontiers in Civil Justice: Privatisation, Monetisation and Digitisation*, (ed. por X. Kramer, J. Hoevernaars, B. Kas y E. Themeli), Cheltenham, Edward Elgar, 2020, pp. 1-20, pp. 5-6.

Marchal Escalona, N.: "El nuevo marco europeo sobre notificación y obtención de pruebas en el extranjero: hacia un espacio judicial europeo digitalizado", *Revista Española de Derecho Internacional,* 2022, vol. 72, núm. 1, pp. 155-179.

Marchal Escalona, N.: *Garantías procesales y notificación internacional*, Comares, Granada, 2001. Virgós Soriano, M. y Garcimartín Alférez, F.J.: *Derecho Procesal Civil internacional. Litigación internacional*, Thomson Civitas, Madrid, 2007 (2ª ed.).

Merchán Murillo, A.: "Digitalización de las normas en materia de cooperación judicial internacional", *Latin American Journal of European Studies*, 2019, vol. 3, núm. 1, 2023, pp. 152-179.

Ontanu, E.A.: "The digitalisation of European Union Procedures: A New Impetus Following a Time of prolonged Crisis", *Law, Tecnnology and Humans*, 2023, vol. 5 (1), pp. 93-110.

Ontanu, E.A.: "Article 2. Definitions", en AA.VV.: *The European Service Regulation* (ed. por A. Anthimos y M. Requejo Isidro), Edward Elgar, Cheltenham, 2023, pp. 59-63

Payan, G.: "Actualité jurispridentielle européenne du Règlement (CE) núm. 1393/2007 du novembre 2007", AA.VV. : *La signification des actes judiciaires et extrjudiciaires en Europe. Anlyses, jurisprudences et perspectives du Règlement UE núm. 2020/1784* (dir. por M. Schmitz), Bruylant, Brusleas, 2022, pp. 23-48.

Prats Jané, S.: *La cooperación jurídica internacional en el ámbito civil y mercantil en España: notificaciones, obtención y practica de prueba*, Bosch, Barcelona, 2022

Requejo Isidro, M.: "Article 3. Transmitting and rceiving agencies" y "Article 5. Means of communication to be used by transmitting agencies, receiving agencies and central bodies", en AA.VV.: *The European Service Regulation* (ed. por A. Anthimos y M. Requejo Isidro), Edward Elgar, Cheltenham, 2023, pp. 64-67 y 71-75.

Richard, V.: "La refonte du règlement sur l'obtention des preuves en matière civile", *Rev. Crit. DIP*, 2021, 1(1) pp. 67-77.

RICHARD, V.: "La refonte du règlement sur la notification des actes judiciaires et extrajudiciaries", *Rev.crit. DIP*, 2021, núm. 2, pp. 349-360.

ROSS, G.: "El traslado de los tribunales a la red: las lecciones que debemos aprender a partir de los errores ajenos", en AA.VV.: *Justicia digital, mercado y resolución de litigios de consumo. Innovación en el diseño del acceso a la justicia* (dir. por F. ESTEBAN DE LA ROSA), Thomson Reuters Aranzadi, Pamplona, 2021, pp. 119-131.

STEIN, A.: "The European Service Regulation: Introduction", en AA.VV.: *The European Service Regulation* (ed. por A. ANTHIMOS Y M. REQUEJO ISIDRO), Edward Elgar, Cheltenham, 2023, pp. 1-25

STÜRNER, M.: "Article 8. Transmission of documents", "Article 10. Receipt of documents by receiving agency" y "Article 11. Service of documents" en AA.VV.: *The European Service Regulation* (ed. por A. ANTHIMOS Y M. REQUEJO ISIDRO), Edward Elgar, Cheltenham, 2023, pp. 86-92, 96-100 y 101-104.

SUJECKI, B.: "Neufassung der Europäischen Zustellungsverordnung", *EuZW*, 2021, pp. 286-290.

THEMELI, E.: "The frontiers of digital justice in Europe", en AA.VV.: *Frontiers in Civil Justice*, (ed. por X. KARNMER, J. HOEVERNAAS, B. KAS Y E. THEMELI), Edward Elgar, Cheltenham, 2022, pp. 102-120.

VELICOGNA, M.: "Coming to Terms with Complexity Overload in Transborder e-Justice: The e-CODEX Platform", en AA.VV.: *The Circulation of Agency in E-Justice Law* (ed. por F. CONTINI Y G.F. LANZARA), Springer, Heidelberg, 2014, pp. 309-330.

VERBIC, F.: "Application of New Technologies in Judicial Proceedings", en AA.VV.: *Technology, the Global Economy and other New Challenges for Civil Justice* (ed. por K. MIKI), Intersentia, Cambridge, 2021, pp. 381-394.

VICARIO PÉREZ, A.M.: "Cooperación judicial digital en la Unión Europea, e-CODEX como sistema de intercambio electrónico transfronterizo de datos procesales", en AA.VV.: *Cooperación judicial civil y penal en la Unión Europea. Retos pendientes y nuevos desafíos ante la transformación digital del proceso* (dir. por P.R. SUÁREZ XAVIER Y A.M. VICARIO PÉREZ), Bosch, Barcelona, 2023, pp. 233-266.

WACHOWICZ, M. Y DE PREDIGAO LANA, P.: "Entendendo a fragmentação da Internet a partir de aspectos fundamentais sobre regulação, soberania digital e a experiência da União Europeia", en AA.VV.: Direito e Ciberespaço (coord. por E.

VERA-CRUZ PINTO Y M.A. MARQUES DA SILVA), Quartier Latin, Sao Paulo, 2023, pp. 1-24.

YBARRA BORES, A.: "El sistema de notificaciones en la Unión Europea en el marco del Reglamento 1393/2007 y su aplicación judicial", *Cuadernos de Derecho Transnacional*, 2013, vol. 5, núm. 2, pp. 481-500.

LOS PRINCIPIOS DEL NUEVO PROCESO JUDICIAL DIGITAL TRAS LA REFORMA DEL RD-LEY 6/2023

THE PRINCIPLES OF THE NEW DIGITAL JUDICIAL PROCESS AFTER THE REFORM OF RD-LAW 6/2023

Actualidad Jurídica Iberoamericana Nº 21, agosto 2024, ISSN: 2386-4567, pp. 224-239

* Este trabajo se redacta en el marco del Proyecto "Claves para una justicia digital y algorítmica con perspectiva de género", PID2021-123170OB-I00 financiado por MCIN/ AEI/10.13039/501100011033. Además, dentro del Proyecto "Invitación general para participar en el impulso a la implementación de la Carta de derechos digitales y en la creación del espacio de observación de derechos digitales", CO46/22-OT.

Miren Josune
PÉREZ
ESTRADA

ARTÍCULO RECIBIDO: 29 de mayo de 2023
ARTÍCULO APROBADO: 1 de julio de 2024

RESUMEN: El texto destaca los nuevos principios emergentes del proceso judicial digital introducidos por el RD-Ley 6/2023. Estos principios se corresponden con la integridad del proceso, la autenticidad de las actuaciones judiciales, la seguridad y transparencia en el manejo de datos, y el principio general de orientación al dato. Este último principio refleja la importancia de la gestión eficiente de datos para mejorar la interoperabilidad de los sistemas, la tramitación electrónica del proceso, la toma de decisiones judiciales y otras funciones relacionadas con la Administración de justicia.

PALABRAS CLAVE: Proceso judicial digital, integridad, autenticidad, seguridad, orientación al dato.

ABSTRACT: *The text also highlights new emerging principles of the digital judicial process introduced by RD-Law 6/2023. Among these principles, the integrity of the process, the authenticity of judicial proceedings, security and transparency in data management, and the general principle of data orientation are emphasized. This last principle reflects the importance of efficient data management to improve the interoperability of systems, electronic processing, judicial decision-making and other functions related to the administration of justice.*

KEY WORDS: *Digital judicial process, integrity, authenticity, security, data orientation.*

SUMARIO.- I. INTRODUCCIÓN: CONTENIDO Y FINALIDAD DE LA NORMA. II. LOS PRINCIPIOS DEL PROCESO JUDICIAL DIGITAL. 1. Integridad del proceso. 2. Autenticidad de las actuaciones judiciales. 3. Seguridad y transparencia. 4. Principio general de orientación al dato. III. CONCLUSIONES.

I. INTRODUCCIÓN: CONTENIDO Y FINALIDAD DE LA NORMA.

El reciente 20 de marzo de 2024 entró en vigor la reforma de eficiencia procesal introducida por el Real Decreto-Ley 6/2023, de 19 de diciembre, por el que se aprueban medidas urgentes para la ejecución del Plan de Recuperación, Transformación y Resiliencia en materia de servicio público de justicia, función pública, régimen local y mecenazgo (en adelante, RD-Ley 6/2023), publicado en el BOE al día siguiente de su promulgación[1] y convalidado por Acuerdo del Congreso de los Diputados de 10 de enero de 2024.

La presente reforma constituye la base legislativa del "Plan Justicia 2030", enmarcado en el Plan de Recuperación, Transformación y Resiliencia y en conexión con el Plan de la Unión Europea Next Generation, con el que se pretende transformar el servicio de Justicia para hacerlo más eficiente y afrontar los desafíos surgidos como consecuencia de la pandemia de la Covid-19, y cuyo desarrollo parlamentario ordinario del proyecto de Ley de Medidas de Eficiencia Digital se vió interrumpido por la convocatoria de elecciones generales. Con la aprobación de estas medidas en plazo, España cumple el compromiso asumido con Bruselas, lo que contribuirá a la recepción del cuarto desembolso de los fondos Next Generation EU, por un importe de 10.000 millones de euros lo cual motiva la urgencia del instrumento legislativo elegido[2].

Las medidas, incluidas en el Libro Primero del RD-Ley 6/2023, se articulan en dos grandes bloques. El primero de ellos tiene como objetivo adaptar la realidad judicial española al marco tecnológico y digital actual; y el segundo bloque está orientado a la eficiencia procesal y tiene como objetivos garantizar procedimientos más ágiles y hacer frente al incremento de la litigiosidad. La norma se orienta a la agilización de la actividad de la "Justicia como servicio público" en términos estructurales, para lo cual se implementan herramientas de dos

1 Publicado en el BOE núm. 303, de 20/12/202, que dispone que las previsiones en materia de eficiencia previstas en el título VIII del libro primero y en las disposiciones finales primera, segunda y cuarta procesal entraran en vigor el 20 de marzo de 2024, a los 3 meses de su publicación en el Boletín oficial del Estado.

2 Significativa, cuanto menos, la opción del legislador de aprobar el texto mediante la técnica del RD-Ley y no mediante Ley Orgánica como estaba previsto en el caducado Proyecto de eficiencia digital, marco normativo para la digitalización de la Justicia.

• Miren Josune Pérez Estrada
Profesora Titular de Derecho procesal, Universidad del País Vasco. UPV/EHU.
Correo electrónico: mirenjosune.perez@ehu.eus

tipos que se regulan en la norma: las primeras, comprendidas en los Títulos I a VII, implementan medidas para lograr la transformación digital del proceso: se generaliza la celebración de vistas y declaraciones mediante videoconferencias y se regulan los sistemas de autentificación e identificación, evitando tanto los desplazamientos de la ciudadanía a las sedes como la concentración de personas en las oficinas judiciales; las segundas, contenidas en el Título VIII, vienen referidas a reformar las leyes procesales con la finalidad de aumentar la agilidad, celeridad y eficiencia de los procedimientos en el orden penal, contencioso-administrativo, civil y social, como así se recoge en el preámbulo del RD-Ley 6/2023.

Precisamente, a estos objetivos de lograr una tramitación eficiente, apostar por la utilización racional de los recursos y conseguir agilizar los procedimientos para una más rápida resolución judicial responde las modificaciones establecidas en el articulado del RD-Ley 6/2023 y que se concretan en las siguientes modificaciones tales como las introducidas en: el ámbito del juicio verbal (elevación de la cuantía, ampliación del ámbito de aplicación por razón de la materia, no necesidad de vista, posibilidad de sentencias orales con posterior documentación); incorporación al proceso civil de figuras ya conocidas en la jurisdicción contenciosa-administrativa (pleito testigo y extensión de efectos para los supuestos de litigación en masa); los cambios operados en el marco de los procesos especiales: monitorio (simplificación del incidente por posible existencia de cláusulas abusivas en el contrato) y familia (sentencias orales); en la ejecución extensión de efectos en los procedimientos en que se ejerciten acciones individuales relativas a condiciones generales de contratación, agilización y transparencia del modelo de subasta electrónica; la jurisdicción voluntaria; o el recurso de apelación, que se interpone directamente ante el órgano competente para su conocimiento.

En este trabajo nos centraremos en los nuevos principios que surgen de la implantación de un proceso judicial netamente digital, con motivo de las medidas que se adoptan en los Títulos I a VII del RD- Ley 6/2023, relativas a adaptar la realidad judicial española al marco tecnológico y digital actual.

II. LOS PRINCIPIOS DEL PROCESO JUDICIAL DIGITAL

No se trata en este apartado de cuestionar los principios tradicionales del proceso judicial, que evidentemente, siguen siendo los mismos, aunque haya variado el soporte en el que se sustenta el proceso, pasando del formato papel al formato digital, con la derogada Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia[3], y, ahora, con la promulgación del RD-Ley 6/2023, a la Justicia orientada

3 Derogada por la Disposición derogatoria única del RD-Ley 6/2023.

al dato[4]. Lo que se pretende, en esta parte del trabajo, es analizar si como consecuencia de esta nueva manera en la que se va a desarrollar el proceso judicial, la digital orientada al dato, aparecen nuevos principios que deberían respetarse para garantizar, precisamente, la esencia del proceso judicial como instrumento mediante el que se garantiza el derecho a la tutela judicial efectiva[5].

La utilización de nuevas herramientas tecnológicas en el desarrollo del proceso judicial influye, sobremanera, en la ordenación del proceso. La formación de los autos judiciales se contempla en el art. 454, punto 1, LOPJ, donde establece que la función de documentación comprende la formación de los autos y los expedientes[6]. El cambio en el desarrollo de esta función se produce por el paso del papel al soporte digital y cómo afecta a la formación de los autos. La formación de los autos en el expediente judicial electrónico[7] es más compleja al estar constituida por archivos digitales que no pueden variar o modificar, sin más, su orden como ocurre con los actos judiciales dentro del expediente judicial en formato papel; por lo tanto, la ordenación de los autos resulta más complicada y no sólo requiere de una mayor diligencia para realizarla sino mayores conocimientos telemáticos, informáticos o, incluso, técnicos para confeccionarla. El resultado de unos archivos electrónicos desordenados o incluso mal nominados podrá provocar una vulneración de los derechos de las partes en el proceso o, incluso, una lesión de la tutela judicial efectiva.

El proceso judicial digital se debe configurar en base a una serie de principios rectores no sólo con el objetivo de conseguir una ordenación óptima del proceso digital sino de procurar su realización e integridad. En el propio art. 1, dedicado al objeto y principios, el punto 2 del RD-Ley 6/2023 enumera los siguientes, de esta manera, "En la Administración de Justicia se utilizarán las tecnologías de la información de acuerdo con lo dispuesto en el presente real decreto-ley, asegurando la seguridad jurídica digital, el acceso, autenticidad, confidencialidad, integridad, disponibilidad, trazabilidad, conservación, portabilidad e interoperabilidad de los datos, informaciones y servicios que gestione en el ejercicio de sus funciones", disponiendo a modo de recordatorio en el punto 3 que "las tecnologías de la

4 Así, expresamente, en el Preámbulo del RD-Ley 6/2023, apartado II, "se potencia el Expediente Judicial Electrónico mediante un cambio de paradigma, pasando de la orientación al documento a la orientación al dato. Esto supone un gran avance respecto de la Ley 18/2011, de 5 de julio, que hace una década se planteaba como objetivo la transición del papel a lo digital, siendo así que se trata ahora de lograr mejoras sustanciales ya en el entorno de lo digital".
También vid. Pérez Estrada, M. J.: *El proceso judicial digital,* Tirant Lo Blanch, Valencia, 2021 y Catalán Chamorro, M. J.: *La justicia digital en España: Retos y desafíos*, Tirant Lo Blanch, Valencia, 2023.

5 Precisamente, Valero Canales, A. L.: "El proceso judicial electrónico. Requisitos para su formación. Comunicaciones y plazos", *Práctica de tribunales: revista de derecho procesal civil y mercantil*, 2018, núm. 131, contempla los nuevos principios de ordenación del proceso judicial electrónico.

6 Dispone el art. 454.1 LOPJ: "Los letrados de la Administración de Justicia son responsables de la función de documentación que les es propia, así como de la formación de los autos y expedientes, dejando constancia de las resoluciones que dicten los jueces y magistrados, o ellos mismos cuando así lo autorice la ley."

7 La referencia a los términos "electrónico" o "digital" es análoga.

información en el ámbito de la Administración de Justicia tendrán carácter instrumental de soporte y apoyo a la actividad jurisdiccional, con pleno respeto a las garantías procesales y constitucionales".

1. Integridad del proceso.

Este principio hace referencia al contenido o configuración del proceso digital. Se trata de que contenga todas las actuaciones judiciales que se han ido realizando a lo largo del proceso y que deberán estar recogidas en soporte digital. El contenido íntegro del proceso, i.e., que consten en el mismo todas las actuaciones procesales realizadas, está en directa relación con los principios generales del proceso; en concreto, con los principios tradicionales de contradicción y derecho de defensa[8].

La plenitud del proceso afecta a la función de documentación de las actuaciones judiciales encomendada al letrado de la Administración de Justicia (en adelante, LAJ) en lo referente a la actividad de formación de los autos judiciales, que se recoge en los arts. 453.1 LOPJ y 146 LEC. El contenido de esta función de documentación ha variado desde la aplicación de las TICs al proceso y ha ido evolucionando; en un primer momento, la incorporación al proceso de actuaciones judiciales recogidas en formato digital, como grabaciones de determinados actos procesales, audiencias previas o vistas o documentos de las partes se incorporaban al proceso en el formato original sin necesidad de una transposición al papel; es decir, quedaban incorporadas al proceso mediante las diligencias de ordenación que dejan constancia de esas actuaciones judiciales pero no aparecían integrados como ocurre en el expediente judicial electrónico[9].

La cuestión es distinta en el caso de la confección del expediente judicial en formato digital puesto que todos los actos procesales que se realizan en el proceso se incorporan a las actuaciones directamente, atendiendo al orden de su realización, sin que sea necesario una diligencia de constancia que indique el momento de su incorporación a las actuaciones. Lo mismo ocurrirá con la incorporación al expediente judicial electrónico de los documentos y escritos y solo en el caso de la presentación de escritos perentorios y ante la imposibilidad de su presentación con motivo de la naturaleza del documento o el tamaño del archivo se presentará el escrito por medios electrónicos en la oficina judicial dentro del primer día hábil siguiente el documento o documentos que no haya

8 Recordemos el contenido de estos principios generales del proceso, principio de contradicción y derecho de defensa en Gómez Colomer, J. L.: "Cuestiones generales del proceso", en Introducción al Derecho Procesal. Derecho Procesal I, 3ª ed., Tirant lo Blanch, Valencia, 2023, pp. 247-250.

9 Concluía sobre las mismas Valero Canales, A. L.: "El proceso judicial", cit., p. 3, que la constancia en los autos de actuaciones recogidas en formato distinto del papel no afecta al principio de integridad del proceso.

podido adjuntar[10]. Sin perjuicio de lo establecido en el art. 135.4 LEC en el caso excepcional de presentación de escritos y documentos en soporte papel[11].

En el expediente judicial electrónico todas las actuaciones deben estar digitalizadas para que consten efectivamente integradas. No obstante, pueden existir documentos no incorporados físicamente en el expediente judicial; en este caso hay que dejar constancia en el expediente de su existencia y dónde quedan depositadas y por quién se custodian en el correspondiente archivo, provisional o definitivo, de la oficina judicial.

En el formato electrónico la constancia de que el proceso se halla íntegro difiere del formato en papel en el que la plenitud o integridad se hacía depender de su foliado. En el expediente judicial electrónico constará un índice electrónico que permita la debida localización y consulta, incluso el escrito principal puede hacer referencia a documentos adicionales, siempre y cuando se cumplan unas exigencias técnicas[12]. Por lo que en el expediente judicial electrónico se incorpora un índice electrónico con todas las actuaciones judiciales que será el que garantice

10 Art. 135.2 LEC, modificado por el art. 103.18 RD-Ley 6/2023: "Cuando la presentación de escritos perentorios dentro de plazo por los medios electrónicos a que se refiere el apartado anterior no sea posible por interrupción no planificada del servicio de comunicaciones telemáticas o electrónicas, siempre que sea posible se dispondrán las medidas para que el usuario resulte informado de esta circunstancia, así como de los efectos de la suspensión, con indicación expresa, en su caso, de la prórroga de los plazos de inminente vencimiento. El remitente podrá proceder, en este caso, a su presentación en la oficina judicial el primer día hábil siguiente acompañando el justificante de dicha interrupción.
En los casos de interrupción planificada deberá anunciarse con la antelación suficiente, informando de los medios alternativos de presentación que en tal caso procedan.
Cuando la presentación de escritos perentorios dentro de plazo se vea impedida por limitaciones, incluso horarias, en el uso de soluciones tecnológicas de la Administración de Justicia, establecidas de conformidad con la normativa que regule el uso de la tecnología en la Administración de Justicia, como regla, el remitente podrá proceder a su presentación el primer día hábil siguiente, justificándolo suficientemente ante la oficina judicial. En el caso de que la imposibilidad de la presentación se deba a la naturaleza del documento a presentar o al tamaño del archivo, el remitente deberá proceder, en este caso, a la presentación del escrito por medios electrónicos y presentar en la oficina judicial dentro del primer día hábil siguiente el documento o documentos que no haya podido adjuntar."

11 Recordemos la literalidad del art. 135.4 LEC: "Sin perjuicio de lo anterior, los escritos y documentos se presentarán en soporte papel cuando los interesados no estén obligados a utilizar los medios telemáticos y no hubieran optado por ello, cuando no sean susceptibles de conversión en formato electrónico y en los demás supuestos previstos en las leyes. Estos documentos, así como los instrumentos o efectos que se acompañen quedarán depositados y custodiados en el archivo, de gestión o definitivo, de la oficina judicial, a disposición de las partes, asignándoseles un número de orden, y dejando constancia en el expediente judicial electrónico de su existencia.
En caso de presentación de escritos y documentos en soporte papel, el funcionario designado para ello estampará en los escritos de iniciación del procedimiento y de cualesquiera otros cuya presentación esté sujeta a plazo perentorio el correspondiente sello en el que se hará constar la oficina judicial ante la que se presenta y el día y hora de la presentación."

12 Este último aspecto es consecuencia de la reforma del apartado 4 del art. 273 por el RD-Ley 6/2023: Los escritos y documentos presentados por vía telemática o electrónica indicarán el tipo y número de expediente y año al que se refieren e irán debidamente referenciados mediante un índice electrónico que permita su debida localización y consulta. El escrito principal deberá incorporar firma electrónica y se adaptará a lo establecido en la Ley reguladora del uso de las tecnologías en la Administración de Justicia.
Si se considera de interés, el escrito principal podrá hacer referencia a los documentos adicionales, siempre y cuando exista una clave que relacione esa referencia de manera unívoca por cada uno de los documentos, y, a su vez, asegure de manera efectiva su integridad.

la integridad del expediente judicial electrónico, i.e., que contiene todas las actuaciones procesales que se han realizado en el proceso.

2. Autenticidad de las actuaciones judiciales.

Este principio se encuentra relacionado con la veracidad de las actuaciones judiciales. Los documentos judiciales tienen el carácter de auténticos si resultan ser un reflejo fiel del contenido de las actuaciones judiciales que se han realizado. En el expediente judicial, en formato en papel, las actuaciones judiciales de las partes son auténticas si están firmadas por las partes o el documento está firmado por los profesionales que lo han confeccionado; y en el caso de resoluciones judiciales se refiere a que las mismas deben estar firmadas por los titulares del órgano judicial. Sólo de esta manera, i.e., si son auténticas, pueden unirse dichas actuaciones al procedimiento.

En el procedimiento judicial digital los documentos inacabados o utilizados como borradores o los documentos erróneos no se deben entender como actuaciones judiciales y deben permanecer al margen del procedimiento. Es necesario que se ponga especial cuidado a la hora de confeccionar los documentos judiciales e ir prestando atención en eliminarlos para evitar un expediente judicial que contenga actuaciones erróneas o documentos judiciales inválidos; se deben incluir sólo documentos judiciales definitivos que son los que tendrán la cualificación de auténticos.

En este sentido el art. 40 RD-Ley 6/2023 dispone lo que debe considerarse documento electrónico, distinguiendo entre original y copias electrónicas. En lo que aquí nos ocupa y de acuerdo con lo dispuesto en el punto 1 del art. 40, tienen la consideración de documento original, cuya autenticidad viene referida a la firma electrónica del documento o resolución judicial, "todos los documentos judiciales electrónicos emanados de los sistemas de gestión procesal y provistos de firma electrónica, así como los correspondientes a los escritos y documentos iniciadores o de trámite presentados por las partes e interesados, una vez hayan sido incorporados al expediente judicial electrónico.

También tendrán la consideración de documentos originales las resoluciones judiciales o administrativas que hubiesen sido firmadas electrónicamente por la autoridad competente para su emisión, a través de cualquiera de los sistemas legalmente establecidos, incluyendo los basados en Código Seguro de Verificación.

No tendrán la consideración de originales, a estos efectos, las copias digitalizadas de otros documentos incorporados al expediente judicial electrónico, salvo que así se declare expresamente."

Por lo tanto, el proceso judicial electrónico está formado por actuaciones judiciales que son definitivas y, por consiguiente, no se pueden modificar. Estamos hablando de las actuaciones habituales en el proceso como la realización de una prueba preconstituída o la celebración de una vista que se ha grabado y firmado electrónicamente, una resolución judicial definitiva y firmada electrónicamente o los escritos de partes presentado y firmado de manera electrónica.

El expediente judicial electrónico se puede seguir y en él se pueden consultar todas las actuaciones judiciales definitivas que estarán ordenadas de manera cronológica, desde la demanda judicial, los escritos de las partes y las resoluciones judiciales hasta la vista, incluso se van mejorando las aplicaciones digitales incorporadas con nuevas funcionalidades[13].

3. Seguridad y transparencia.

Una de las preocupaciones y quizá el mayor reto que se debe afrontar en la implementación de nuevas tecnologías en los órganos judiciales es, precisamente, la seguridad en la transmisión de los datos. Precisamente, esta cuestión está muy presente en el RD-Ley 6/2023 dedicando la Sección Segunda del Capítulo II, Capítulo III y Capítulo IV a la "ciberseguridad judicial" de manera que, junto con otras cuestiones, como la interoperabilidad judicial, la reutilización de aplicaciones y transferencias tecnológicas y la Protección de Datos de carácter personal se pretende garantizar la seguridad de la Administración Judicial en la transmisión de los datos y cuantas otras exigencias cuya competencia corresponde al Comité Técnico estatal de la Administración judicial electrónica (art. 93 RD-Ley 6/2023)[14].

El RD-Ley 6/2023 tiene muy en cuenta esta necesidad de seguridad que es necesario proporcionar en el sistema de gestión procesal, en particular, y en la Administración de Justicia, en general, por lo que establece en el art. 94 una mejora continua del proceso de seguridad, en el art. 95 crea el Subcomité de seguridad en el que se debe apoyar el Comité Técnico estatal de la Administración judicial electrónica y en el art. 96 establece un centro de operaciones de ciberseguridad de la administración de Justicia. Este articulado corrobora la importancia que el RD-Ley 6/2023 otorga a la seguridad de la información de la Administración de justicia.

13 Es el caso del visor de expedientes judiciales Horus 5.2, en territorio Ministerio, versión que "mejora la accesibilidad, visibilidad, comunicación, gestión y control de la información contenida en el Expediente Judicial Electrónico".
Disponible en https://www.mjusticia.gob.es/es/institucional/gabinete-comunicacion/noticias-ministerio/mejoras-horus; acceso el 09/04/2024.

14 Dispone el art. 93 sobre "Política de seguridad de la información de la Administración Judicial Electrónica. 1. Corresponde al Comité técnico estatal de la Administración judicial electrónica la elaboración y actualización de la política de seguridad de la información de la Administración de Justicia, en sus aspectos organizativos, técnicos, físicos y de cumplimiento de la normativa."

Relacionado con la seguridad se encuentra la protección de los datos personales, contemplado en el art. 5 j) RD-Ley 6/2023 como un derecho de la ciudadanía "a la protección de datos de carácter personal y, en particular, a la seguridad y confidencialidad de los datos que sean objeto de tratamiento por la Administración de Justicia, en los términos establecidos en la Ley Orgánica 6/1985, de 1 de julio, y con las especialidades establecidas por esta; en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE; en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales; y en la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, así como los que deriven de leyes procesales."[15]

Se contempla también la seguridad de los archivos electrónicos que contengan los documentos, en el art. 6 e) RD-Ley 6/2023, dentro de los derechos de los y las profesionales que se relacionan con la Administración de Justicia; así derecho : "A la garantía de la seguridad y confidencialidad y disponibilidad en el tratamiento de los datos personales realizado por la Administración de Justicia que figuren en los ficheros, sistemas y aplicaciones de la Administración de Justicia en los términos establecidos en la Ley Orgánica 6/1985, de 1 de julio, y con las especialidades establecidas por esta; en las leyes procesales, en el presente real decreto-ley, en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016; en la Ley Orgánica 3/2018, de 5 de diciembre; y en la Ley Orgánica 7/2021, de 26 de mayo, así como los que deriven de leyes procesales. Corresponderá a la Administración competente cumplir con las responsabilidades que, como administración prestacional, tenga atribuidas en esa materia."

En definitiva, en materia de seguridad el Libro Primero del Título VII, siguiendo la estructura de la derogada Ley 18/2011, aborda la cooperación entre las distintas administraciones con competencias en el ámbito de la Justicia. Asimismo, se establece el marco del Esquema Judicial de Interoperabilidad y Seguridad, junto con otras normativas relacionadas con la seguridad.

Se fortalece el rol del Comité Técnico Estatal de la Administración Judicial Electrónica, como un órgano de cogobernanza en la gestión digital de la Justicia, encargado de impulsar y coordinar la transformación digital en este ámbito. Sus funciones se alinean con las directrices de la Conferencia Sectorial de Justicia.

15 La LOPJ reproduce esta obligatoriedad de seguridad en su art. 230.4: "Los procesos que se tramiten con soporte informático garantizarán la identificación y el ejercicio de la función jurisdiccional por el órgano que la ejerce, así como la confidencialidad, privacidad y seguridad de los datos de carácter personal que contengan en los términos que establezca la ley".

Dentro de este comité, se contempla la creación de un Consejo Consultivo para la Transformación Digital de la Administración de Justicia. Este consejo tiene como objetivo facilitar la colaboración con el sector privado y los grupos interesados en el diseño y desarrollo de sistemas digitales.

Se establece la regulación del Esquema Judicial de Interoperabilidad y Seguridad, con especial énfasis en la interoperabilidad con colegios profesionales y registros relacionados con la Administración de Justicia. Esto incluye registros electrónicos vinculados a propiedades, bienes muebles, registros mercantiles, así como protocolos electrónicos notariales y comunicaciones electrónicas internacionales.

Finalmente, se establecen normas para la formulación y actualización de la política de seguridad de la información en la Administración de Justicia. Además, se prevé la creación de un Subcomité de Seguridad, como un órgano especializado del Comité Técnico Estatal de la Administración Judicial Electrónica, y un Centro de Operaciones de Ciberseguridad de la Administración de Justicia.

La seguridad, por lo tanto, es un tema fundamental en la utilización de los sistemas de información para la tramitación de los procesos judiciales y también prima para el caso de la interoperabilidad judicial.

Por razones obvias, la tramitación digital del expediente judicial proporciona no sólo un acceso más fácil al expediente judicial, sino que proporciona una mayor transparencia de las actuaciones judiciales lo cual está directamente relacionado con el principio de publicidad del proceso. En el contexto digital desaparece la posibilidad física de acudir al órgano jurisdiccional a fin de tener acceso a las actuaciones judiciales[16] depositadas en la Oficina Judicial puesto que el acceso a

16 Art. 234 LOPJ: 1. Los Letrados de la Administración de Justicia y funcionarios competentes de la Oficina judicial facilitarán a los interesados cuanta información soliciten sobre el estado de las actuaciones judiciales, que podrán examinar y conocer, salvo que sean o hubieren sido declaradas secretas o reservadas conforme a la ley.
2. Las partes y cualquier persona que acredite un interés legítimo y directo tendrán derecho a obtener, en la forma dispuesta en las leyes procesales y, en su caso, en la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia, copias simples de los escritos y documentos que consten en los autos, no declarados secretos ni reservados. También tendrán derecho a que se les expidan los testimonios y certificados en los casos y a través del cauce establecido en las leyes procesales.
Art. 235 LOPJ: "Los interesados tendrán acceso a los libros, archivos y registros judiciales que no tengan carácter reservado, mediante las formas de exhibición, testimonio o certificación que establezca la ley."
Artículo 235 bis: "Sin perjuicio de lo establecido en el párrafo segundo del apartado 1 del artículo 236 quinquies y de las restricciones que, en su caso, pudieran establecerse en las leyes procesales, el acceso al texto de las sentencias, o a determinados extremos de las mismas, o a otras resoluciones dictadas en el seno del proceso, sólo podrá llevarse a cabo previa disociación de los datos de carácter personal que los mismos contuvieran y con pleno respeto al derecho a la intimidad, a los derechos de las personas que requieran un especial deber de tutela o a la garantía del anonimato de las víctimas o perjudicados, cuando proceda.
En todo caso se adoptarán las medidas necesarias para evitar que las sentencias y el resto de resoluciones dictadas en el seno del proceso puedan ser usadas con fines contrarios a las leyes.
Art. 454.4 LOPJ: "Facilitarán a las partes interesadas y a cuantos manifiesten y justifiquen un interés legítimo y directo, la información que soliciten sobre el estado de las actuaciones judiciales no declaradas secretas ni reservadas."

expediente judicial se realiza vía telemática y en la Oficina Judicial virtual y no en la física. El acceso de las partes y las personas interesadas a las actuaciones judiciales en el entorno digital debe realizarse con la máxima garantía en la seguridad de transmisión de los datos a fin de impedir que se transmitan de manera masiva y casi al instante datos personales o se vea afectada la intimidad de las personas.

En la actualidad el sistema de acceso de las partes e interesados al contenido de las actuaciones judiciales digitales[17] no está implantado totalmente por lo que no se efectúa ni de manera generalizada ni homogénea en todos los órganos jurisdiccionales; aunque es previsible que, en los próximos años y a medida que se implanten los sistemas procesales de comunicación previstos en la reciente normativa, se desarrollará con habitualidad. Esta previsibilidad inmediata en un futuro próximo hace que se deba proteger, por vía de la regulación procesal, la privacidad de las partes y terceros interesados en el proceso.

4. Principio general de orientación al dato.

Sin duda el principio por excelencia que va a regir el proceso judicial digital es el principio general de orientación al dato[18]. Precisamente, el Título III del Libro Primero se refiere a la tramitación electrónica de los procedimientos judiciales y en el propio preámbulo de la norma analizada se recoge que se trata de "una de las grandes novedades de esta ley". Teniendo en cuenta, como de nuevo establece el preámbulo de la norma, "los datos son clave en las políticas públicas modernas"; así, el principio general de orientación al dato posibilitará la gestión de los datos facilitando "la interoperabilidad de los sistemas, la tramitación electrónica, la búsqueda y análisis de los datos, la anonimización y seudonimización, la elaboración de cuadros de mando, la gestión de documentos y su transformación, la publicación de información en portales de datos abiertos, la producción de actuaciones automatizadas, asistidas y proactivas, la utilización de sistemas de inteligencia artificial para la elaboración de políticas públicas, y la transmisión de los datos conforme a lo que se determine."[19]

El capítulo II del Título III (arts. 35 a 37) regula el principio general de la justicia orientada al dato, según el cual todos los sistemas de información y comunicación que se utilicen en el ámbito de la Administración de Justicia, incluso para finalidades de apoyo a las de carácter gubernativo, asegurarán la entrada, incorporación y tratamiento de la información en forma de metadatos, conforme a esquemas

17 Vid. Mira Ros, C.: *El expediente judicial electrónico*, Dykinson, Madrid, 2010.

18 Sobre el paso de la Justicia digital orientada al documento a la Justicia orientada al dato, vid. Barona Vilar, S.: "Ecosistema digital de Justicia eficiente (De la Justicia digital orientada al documento a la Justicia orientada al dato", *Actualidad Civil*, 2023, núm. 5.

19 Detalla aplicaciones concretas Bueno De Mata, F.: "Diálogos para el futuro judicial. LXXV. Medidas de Eficiencia Digital del Servicio Público de Justicia", *Diario La Ley*, de 6 de febrero de 2024, núm. 10440.

comunes, y en modelos de datos comunes e interoperables. La norma parte, como hemos puesto de manifiesto, de que los datos son clave en las políticas públicas modernas. Por tanto, la gestión sobre los mismos posibilitará o facilitará la interoperabilidad de los sistemas, la tramitación electrónica, la búsqueda y análisis de los datos, la anonimización y seudonimización, la elaboración de cuadros de mando, la gestión de documentos y su transformación, la publicación de información en portales de datos abiertos, la producción de actuaciones automatizadas, asistidas y proactivas, la utilización de sistemas de inteligencia artificial para la elaboración de políticas públicas, y la transmisión de los datos conforme a lo que se determine. Para ello, la norma establece que los sistemas informáticos y de comunicación utilizados en la Administración de Justicia posibilitarán el intercambio de información entre órganos judiciales, así como con las partes o interesados, en formato de datos estructurados.; a través de sistemas de intercambio masivo de información.

Atendiendo al objeto de los datos o a la finalidad de su tratamiento es posible distinguir entre la gestión y su explotación, que puede ayudar en una tramitación judicial más rápida al automatizarse. El análisis y la explotación de los datos puede también ser útil en la toma de decisiones judiciales; sin embargo este último uso debe ser cauteloso porque la utilización conjunta de inteligencia artificial, que se propicia en la norma con motivo de las actuaciones asistidas, puede afectar a principios y garantías procesales de carácter constitucional que incluso tienen incidencia en el ejercicio de la función jurisdiccional si es que se utiliza como sustitutivo de ésta y no como mera herramienta auxiliar.

III. CONCLUSIONES.

En el texto se analizan los principios fundamentales del proceso judicial digital que se establecen con motivo de la reforma legal en virtud del nuevo Real Decreto-Ley 6/2023, que busca modernizar y agilizar el sistema judicial, adaptándolo al entorno tecnológico y digital actual.

La reforma responde a la necesidad de adaptar el sistema judicial español a los avances tecnológicos y digitales. Sin embargo, se debe tener en cuenta que la implementación de tecnología en el ámbito judicial debe realizarse con cautela para garantizar la efectividad y la justicia del sistema. Se busca mejorar la eficiencia procesal y la celeridad en la resolución de casos, aunque es importante considerar si las medidas implementadas realmente lograrán estos objetivos sin comprometer la calidad de las decisiones judiciales.

La digitalización del sistema judicial plantea desafíos en cuanto a la protección de datos y la seguridad jurídica. Es crucial garantizar los principios que rigen el nuevo proceso judicial digital como son la integridad, autenticidad, confidencialidad

y disponibilidad de la información judicial, así como asegurar el cumplimiento de la normativa de protección de datos. Sin duda la utilización de sistemas de inteligencia artificial en el ámbito judicial para la elaboración de políticas públicas y la toma de decisiones judiciales plantea riesgos en términos de imparcialidad, transparencia y garantías procesales. Se debe prestar especial atención para evitar posibles sesgos o discriminaciones en la aplicación de la ley.

Por lo tanto, la implementación de cambios tan profundos en nuestro sistema judicial requiere de un enfoque gradual y cuidadoso, con evaluaciones constantes de su impacto y efectividad. Además, es fundamental contar con la colaboración de todos los actores involucrados, incluyendo la judicatura, letrado/as de la Administración de Justicia, abogacía y ciudadanía, para garantizar una transición exitosa.

En resumen, si bien la reforma busca modernizar y agilizar el sistema judicial español, es fundamental abordar de manera crítica y cuidadosa los desafíos y riesgos asociados con la digitalización e implementar de manera efectiva los nuevos principios que rigen el proceso judicial digital.

BIBLIOGRAFÍA

Barona Vilar, S.: "Ecosistema digital de Justicia eficiente (De la Justicia digital orientada al documento a la Justicia orientada al dato)", *Actualidad Civil*, 2023, núm. 5.

Bueno De Mata, F.: "Diálogos para el futuro judicial. LXXV. Medidas de Eficiencia Digital del Servicio Público de Justicia", *Diario La Ley*, de 6 de febrero de 2024, núm. 10440.

Catalán Chamorro, M. J.: *La justicia digital en España: Retos y desafíos*, Tirant Lo Blanch, Valencia, 2023.

Gómez Colomer, J. L.: "Cuestiones generales del proceso", en *Introducción al Derecho Procesal. Derecho Procesal I*, 3ª ed., Tirant lo Blanch, Valencia, 2023.

Mira Ros, C.: *El expediente judicial electrónico*, Dykinson, Madrid, 2010.

Pérez Estrada, M. J.: *El proceso judicial digital,* Tirant Lo Blanch, Valencia, 2021

Valero Canales, A. L.: "El proceso judicial electrónico. Requisitos para su formación. Comunicaciones y plazos", *Práctica de tribunales: revista de derecho procesal civil y mercantil*, 2018, núm. 131.

A HARMONIZAÇÃO DO DIREITO INTERNACIONAL PRIVADO NA ERA DIGITAL: O GUIA DE BOAS PRÁTICAS EM MATÉRIA DE COOPERAÇÃO JURISDICIONAL PARA AS AMÉRICAS*

THE HARMONIZATION OF PRIVATE INTERNATIONAL LAW IN THE DIGITAL AGE: THE GUIDE TO BEST PRACTICES ON JURISDICTIONAL COOPERATION FOR THE AMERICAS

Actualidad Jurídica Iberoamericana Nº 21, agosto 2024, ISSN: 2386-4567, pp. 240-263

* Artigo elaborado no marco do projeto "Claves para una justicia digital y algorítmica con perspectiva de género", PID2021-123170OB-I00 financiado por MCIN/AEI/10.13039/501100011033.

Valesca Raizer
BORGES
MOSCHEN

ARTÍCULO RECIBIDO: 29 de mayo de 2023
ARTÍCULO APROBADO: 1 de julio de 2024

RESUMEN: As Tecnologias de Informação e Comunicação (TICs) estão cada vez mais presentes no exercício jurisdicional dos Estados. Nas comunicações entre autoridades judiciárias ou administrativas para a execução de atos de um Estado em território de um outro, ou seja, na cooperação jurisdicional, as disparidades normativas, de infraestrutura e os diferentes tratamentos dados à tecnologia colocam em xeque a eficiência da prestação jurisdicional e a consequente tutela de direitos e pessoas. O Comitê Jurídico Interamericano (CJI), com o intuito de promover uma interpretação dinâmica e mais adequada à realidade tecnológica atual dos instrumentos convencionais ou dos direitos autônomos existentes, especialmente, na região, elaborou o "Guia de Boas Práticas em Matéria de Cooperação Judiciária para as Américas". Essa inciativa se inclui nos instrumentos da harmonização do Direito Internacional Privado destinado à promoção do acesso transnacional à justiça. O artigo ora proposto parte da premissa de que o acesso à justiça é um direito fundamental, também na escala global. Assim, busca compreender a sistematização realizada pelo Comitê Jurídico Interamericano, em particular, através do Guia de Boas Práticas em Matéria de Cooperação Jurisdicional Internacional para as Américas, para o desafio da utilização das TICs e a regulação e aplicação da cooperação jurisdicional.

PALABRAS CLAVE: Cooperação jurisdicional internacional; Comitê Jurídico Interamericano; Organização dos Estados Americanos; digitalização da Justiça.

ABSTRACT: *Information and Communication Technologies (ICTs) are increasingly present in the jurisdictional exercise of States. In communications between judicial or administrative authorities for the execution of acts of one State in the territory of another, that is, in judicial cooperation, disparities in regulations, infrastructure, and different treatments given to technology call into question the efficiency of judicial provision and the consequent protection of rights and people. The Inter-American Legal Committee (CJI), to promote a dynamic interpretation that is more appropriate to the current technological reality of existing occasional instruments or alternative rights, especially in the region, has prepared the "Guide of Good Practices in Matters of Judicial Cooperation for as the Americas." This initiative is included in the harmonization instruments of Private International Law aimed at promoting transnational access to justice. The proposed article is based on the proposals that access to justice is a fundamental right, also on a global scale. Thus, we seek to understand the systematization carried out by the Inter-American Legal Committee, in particular, through the Guide of Good Practices in the Matter of International Jurisdictional Cooperation for the Americas, for the challenge of using ICTs and the regulation and application of judicial cooperation.*

KEY WORDS: *International jurisdictional cooperation; Inter-American Juridical Committee; Organization of American States; digitalization of justice.*

I. INTRODUÇÃO.

O incremento da conectividade global, incentivada pelo desenvolvimento das tecnologias de informação e comunicação, propiciaram uma dimensão individual e coletiva nova. A globalização permitiu uma nova configuração do espaço social e alterou a forma como os atores sociais se relacionam[1] – a virtualidade passou a ser uma dimensão fundamental da realidade. Por sua vez, os litígios, nessa nova configuração social, caracterizada pela anulação tecnológica das distâncias temporais e espaciais[2], transcendem, cada vez mais, os limites nacionais ao se caracterizarem a partir de distintos elementos fáticos e/ou jurídicos que remetem a mais de uma realidade nacional, portanto, irredutível a um ordenamento jurídico apenas[3].

A cooperação jurídica internacional, gestora do acesso transnacional à justiça e compreendida, "lato sensu", pelo intercâmbio de medidas administrativas e/ou jurisdicionais entre Estados, não obstante a nova dimensão virtual da realidade, está, por vezes, intermediada por procedimentos e trâmites cartoriais, ministeriais e diplomáticos[4].

O presente artigo parte das premissas de que o acesso à justiça é um direito fundamental, também na escala global, e depende do compromisso da cooperação

1 Sholte, A. J.: *Globalization. A critical introduction*, Red Global Press, London, 2005, p. 46.

2 Bauman, Z.: *Globalização: as consequências humanas*, Zahar, Rio de Janeiro, 2021, p. 25.

3 Moschen, V. y Barbosa, L.: "O processo civil internacional no CPC/2015 e os princípios ALI/UNIDROIT do processo civil transnacional: uma análise de consonância da harmonização processual", *Revista Eletrônica de Direito Processual – REDP,* 2018, ano 12, vol. 19, núm. 2, p. 202.

4 Polido, F.: *Direito internacional privado nas fronteiras do trabalho e tecnologias: ensaios e narrativas na era digital*, Lumen Juris, Rio de Janeiro, 2018, p. 76.

• Valesca Raizer Borges Moschen
Professora Titular de Direito Internacional, Faculdade de Direito, Universidade Federal do Espírito Santo – UFES/Brasil. E-mail: valesca.borges@ufes.com.

jurídica – administrativa e jurisdicional – entre os Estados. Há de se ressaltar que as tecnologias de informação e comunicação que oportunizaram a digitalização desafiam as regulações nacional, internacional e transnacional sobre a cooperação.

A identificação do problema principal aponta a necessidade de conhecer e sistematizar as respostas do movimento de harmonização do direito internacional privado, em matéria de cooperação jurídica internacional, diante do desenvolvimento das tecnologias de informação e comunicação, em particular no contexto americano.

Como hipótese principal, levanta-se a urgência de um novo tratamento do instituto da cooperação jurídica internacional na era digital e sua análise sobre as estruturas codificadoras do direito internacional privado. Adota-se, portanto, a compreensão de que o Direito se constitui no interior de um processo social[5]; e, nesse sentido, são cada vez mais recorrentes instrumentos de harmonização que buscam responder pela segurança jurídica dos operadores internacionais e pela convergência na adequação do exercício jurisdicional. Diante de tal realidade, o texto, inicialmente, trabalhará os aspectos contextuais da harmonização do direito internacional privado nas Américas, referente à cooperação jurisdicional, e as tecnologias de informação e comunicação, para logo se adentrar no seu objeto central, isto é, a análise do Guia de Boas Práticas em Matéria de Cooperação Jurisdicional Internacional para as Américas, aprovado em agosto de 2023 no 103º período ordinário de sessões do Comitê Jurídico Interamericano (CJI) da Organização dos Estados Americanos (OEA).

II. HARMONIZAÇÃO DO DIREITO INTERNACIONAL PRIVADO AMERICANO.

A harmonização das regras de direito internacional privado americano tem a sua origem em diferenciados contextos históricos. Um, inserido ao movimento de promoção de instrumentos universais sobre o direito internacional privado, como exemplificam os Tratados de Montevidéu[6], que representaram um primeiro capítulo na história da codificação mundial do direito internacional privado[7] e cujo legado, para além das inovações convencionadas trazidas, está na sua influência sobre os sucessivos instrumentos convencionais e nas legislações regionais, em

5 Hespanha, A. M.: *Panorama histórico da cultura jurídica européia*, Publicações Europa-América, Lisboa, 1998, p. 25.

6 Sobre os legados das CIDIPs: Belandro, R.: "¿Qué imagen refleja un tratado de 1889 en el espejo del siglo XXI?", en AA.VV.: *130 años de los Tratados de Montevideo: Legado y Futuro de sus soluciones en el concierto Internacional actual* (coord. por Fresnedo de Aguirre, C. y Lorenzo Idiarte, G.), FCU, Montevideo, 2019, p. 64.

7 Lopes, I. y Moschen, V.: "Os papeis da OEA e da ASADIP para construção de uma cultura 'Glocal' de Direito Internacional Privado na América Latina", en AA.VV.: *Desafios do direito internacional privado na sociedade contemporânea* (coord. por Lopes, I. y Moschen, V.), Lumen Juris, Rio de Janeiro, 2020, p. 325.

particular na América Latina[8]. E, em um outro sentido, dentro de um paralelo à iniciativa de Montevidéu, no movimento pan-americanista que deu origem à União Internacional das Repúblicas Americanas, embrião da Organização dos Estados Americanos[9].

A partir dessa iniciativa foram instituídas as Conferências Internacionais Americanas, com a finalidade, especialmente, de articular um sistema compartilhado de normas e instituições regionais[10]. Nesse contexto, e após a constituição da Comissão Internacional de Jurisconsultos, gérmen da atual Comissão Jurídica Interamericana (CJI), elaborou-se e aprovou-se, em 1928, o Código de Direito Internacional Privado, o denominado Código de Bustamante[11], que, ao lado dos Tratados de Montevidéu, representou um segundo sistema de codificação de direito internacional privado na América Latina[12]. Essa dualidade de iniciativas codificadoras gerou, segundo Diego Fernandez Arroyo[13], uma "bipolaridade" na região, que apenas se flexibiliza a partir do aumento gradual da participação da Organização dos Estados Americanos (OEA) enquanto intérprete da harmonização do direito internacional nas Américas.

1. A Organização dos Estados Americanos (OEA) como intérprete da harmonização do direito internacional privado nas Américas.

A OEA, constituída em 1958, através da carta de Bogotá[14], é uma organização intergovernamental que, na atualidade, está composta por 34 (trinta e quatro) Estados-membros[15], o que demonstra sua grande capilaridade regional. Além da manutenção da paz de segurança do continente, como finalidades hão de ser acrescentadas a solução de problemas políticos, jurídicos e econômicos e a cooperação para o desenvolvimento econômico, social e cultural de seus Estados-

8 Fernandez Arroyo, D.: *La Codificación del derecho internacional privado en América Latina*, Eurolex, Madrid, 1994, p. 142.

9 Parra-Aganguren, G.: "La primera etapa de los tratados sobre Derecho Internacional Privado en América (1826-1940)", *Revista de la Facultad de Ciencias Jurídicas y Políticas*, 1996, vol. 41, núm. 98, pp. 62-93.

10 Villalta Vizcarra, A. E.: "Viabilidad de las CIDIPS como órgano de codificación del derecho internacional privado", en AA.VV.: *130 años*, cit., p. 685.

11 O Código de Bustamante consta de 437 artigos sobre regras gerais de direito internacional privado, direito civil internacional, direito mercantil internacional, direito penal internacional e direito processual internacional. Está vigente em 14 Estados da região, entre os quais o Brasil, promulgado pelo Decreto nº 18.871, de 13 de agosto de 1929.

12 Ver Araújo, N.: *Direito Internacional Privado: Teoria e Prática Brasileira,* Revista dos Tribunais, Rio de Janeiro, 2019, p. 73.

13 Fernandez Arroyo, D.: "La Codificación", cit., p. 234.

14 Posteriormente, a Carta Constitutiva da OEA foi reformada pelo "Protocolo de Buenos Aires" (1967), "Protocolo de Cartagena das Índias" (1985), "Protocolo de Washington" (1992), "Protocolo de Manágua" (1993). Ver em: Organização dos Estados Americanos (oea): *Quem Somos*. Disponível em: http://www.oas.org/pt/sobre/quem_somos.asp. Acesso em: 2 abr. 2024.

15 Organização dos Estados Americanos (oea): *Estados Membros*. Disponível em: http://www.oas.org/pt/estados_membros/default.asp. Acesso em: 2 abr. 2024.

membros[16]. Desde seu início, a harmonização do direito internacional, incluindo o privado, esteve presente em sua atuação. Com efeito, em 1975, a Assembleia Geral da OEA aprova a primeira Conferência Interamericana sobre Direito Internacional Privado (CIDIP)[17], dando início a uma frutífera via da harmonização do direito internacional privado.

A) As CIDIPS na harmonização do direito internacional privado americano.

No artigo 122 da Carta da OEA[18], as Conferências Especializadas estão qualificadas como reuniões intergovernamentais através das quais se desenvolvem assuntos específicos da cooperação interamericana, tais como o desenvolvimento do direito internacional privado regional. Muito embora tais reuniões não se restrinjam à matéria do direito internacional privado, as Conferências foram sendo reconhecidas no contexto da harmonização jurídica dessa matéria. As CIDIPs responderam pelo principal "locus" regional da harmonização de um amplo leque temático do direito internacional privado[19]. Como legado, foram gerados 26 instrumentos, entre "hard" e "soft law", dos quais enumeram-se 21 Convenções e dois Protocolos, com mais de 805 ratificações[20]. Quanto aos instrumentos de "soft law", destacam-se a Lei Modelo Interamericana sobre Garantias Imobiliárias[21] e dois Documentos Uniformes, relativos à Documentação Mercantil Uniforme para Transporte Internacional e Lei Aplicável e Jurisdição Internacional Competente em Matéria de Responsabilidade Civil Extracontratual[22].

16 Art. 2 da Carta de Bogotá. Ver em: Organização dos Estados Americanos (oea): *Carta da Organização dos Estados Americanos*. Disponível em: https://www.oas.org/dil/port/tratados_A-41_Carta_da_Organiza%C3%A7%C3%A3o_dos_Estados_Americanos.htm. Acesso em: 2 abr. 2024.

17 Realizada no Panamá, quando foram aprovados seis instrumentos convencionais em temáticas de processo civil e comércio internacional. Ver em: Organização dos Estados Americanos (oea): *Histórico do Processo das Cidips*. Disponível em: https://www.oas.org/dil/PrivateIntLaw-HistCidipProc-port.htm. Acesso em: 2 abr. 2024.

18 Art. 122 da Carta de Bogotá: As Conferências Especializadas são reuniões intergovernamentais destinadas a tratar de assuntos técnicos especiais ou a desenvolver aspectos específicos da cooperação interamericana e são realizadas quando o determine a Assembleia Geral ou a Reunião de Consulta dos Ministros das Relações Exteriores, por iniciativa própria ou a pedido de algum dos Conselhos ou Organismos Especializados. Ver em: Organização dos Estados Americanos (oea): *Carta da Organização dos Estados Americanos*. Disponível em: https://www.oas.org/dil/port/tratados_A-41_Carta_da_Organiza%C3%A7%C3%A3o_dos_Estados_Americanos.htm. Acesso em: 2 abr. 2024.

19 A importância das CIDIPs no contexto do desenvolvimento do direito internacional privado americano está remarcada em: Opertti Badán, D.: "Compatibilidad e interacción de la codificación regional interamericana con los ámbitos de producción jurídica universal y subregional. Balance de los veinte primeros años de las CIDIP", en AA.VV.: *El derecho internacional privado interamericano en el umbral del siglo XXI: sextas jornadas de profesores de derecho internacional privado*, Eurolex, Madrid, 1997, p. 220.

20 Organização dos Estados Americanos (oea): *Histórico do Processo das Cidips*. Disponível em: https://www.oas.org/dil/PrivateIntLaw-HistCidipProc-port.htm. Acesso em: 2 abr. 2024.

21 Aprovada na Sexta Conferência Especializada Interamericana sobre Direito Internacional Privado, em 8 de fevereiro de 2002. Ver em: Organização dos Estados Americanos (oea): *Sixth Inter-American Specialized Conference on Private International Law*. Disponível em: https://www.oas.org/dil/CIDIP-VI-finalact-Port.htm. Acesso em: 2 abr. 2024.

22 Aprovados na Sexta Conferência Especializada Interamericana sobre Direito Internacional Privado, em 8 de fevereiro de 2002. Ver em: Organização dos Estados Americanos (oea): *Sixth Inter-American Specialized Conference on Private International Law*. Disponível em: https://www.oas.org/dil/CIDIP-VI-finalact-Port.htm. Acesso em: 2 abr. 2024.

O mérito das iniciativas harmonizadoras gestadas nas CIDIPs está, sobretudo, no reconhecimento de serem essas Conferências um meio "modernizador"[23] da pauta geral do direito internacional privado, que se manifestam em outros instrumentos de codificação e nas reformas dos sistemas jurídicos, em particular na América Latina. Entretanto esse veículo vem perdendo o seu protagonismo, quiçá pela atual governança plural dos espaços de codificação do direito internacional privado, que se apresenta a partir de uma natureza multifacetária, desterritorializada e impulsionada pela participação cada vez maior de atores especializados fora do eixo estatal/intergovernamental[24]. O que se leva a suscitar a necessidade de reformulação do sistema da Organização dos Estados Americanos, sob pena "de echar al olvido toda posibilidad de que la región siga contribuyendo al desarrollo del derecho internacional privado y beneficiándose del mismo"[25].

B) O resgate do Comitê Jurídico Interamericano (CJI) como veículo da harmonização do direito internacional privado.

As CIDIPs, em função de sua natureza intergovernamental, respondiam "por las necesidades de los Estados negociadas entre estos"[26]. O sistema americano de harmonização do direito internacional privado, nos últimos quarenta anos, se ancorou em reuniões intergovernamentais nas quais os Estados eram os principais partícipes. Como metodologia empregada, estava, sobretudo, a técnica convencional de tratados negociados e sujeitos ao futuro referendo estatal. A dificuldade de manutenção desse modelo permitiu o avanço do protagonismo do Comitê Jurídico Interamericano (CJI)[27].

Por ser um corpo técnico da OEA, a composição do CJI se caracteriza pela especialidade e pela independência. O Comitê reúne onze juristas independentes, indicados pelos Estados-membros. Por sua natureza não governamental, o CJI não corresponde a um espaço de negociações de instrumentos convencionais; diferentemente, a metodologia utilizada refere-se à harmonização jurídica indireta ou informal, que possui como elemento caracterizador o reduzido, ou inexistente, efeito jurídico vinculante[28]. Esse órgão está alinhado a um perfil mais "instrutivo"

23 Fernandez Arroyo, D.: "La Codificación", cit., p. 184.

24 Fernandez Arroyo, D.: "La Codificación", cit., p. 345.

25 Negro Alvarado, D.: "Redefiniendo el rol de las conferencias especializadas interamericanas sobre derecho internacional privado (CIDIPS)", en AA.VV.: *130 años*, cit., p. 731.

26 Opertti Badán, D.: "Compatibilidad", cit., p. 231.

27 O Comitê Jurídico Interamericano se instaura em 1906, na terceira Conferência Internacional Americana, celebrada no Rio de Janeiro, onde mantém a sua sede. Conforme Capítulo XIV, artigos 99 a 105 da carta da OEA, ele serve de corpo "consultivo da Organização em assuntos jurídicos; promove o desenvolvimento progressivo e a codificação do Direito Internacional; e analisa os problemas jurídicos referentes à integração dos países com vistas ao desenvolvimento do Hemisfério". Ver em: Organização dos Estados Americanos (oea): *Comissão Jurídica Internacional*. Disponível em: https://www.oas.org/pt/sobre/comissao_juridica.asp. Acesso em: 4 abr. 2024.

28 Moschen, V. y Barbosa, L.: "O processo", cit., pp. 200-228.

da OEA, que se apresenta nos últimos tempos, com projetos não legislativos, mas com conteúdos mais "didáticos"[29]. Nos últimos dez anos, significantes instrumentos foram aprovados, entre os quais frisam-se: o "Guia prático de aplicação da imunidade de jurisdição das organizações internacionais" (2018); o "Guia sobre o direito aplicável aos contratos comerciais internacionais nas Américas" (2019); o Informe "Autonomia da vontade nos contratos internacionais com partes negociavelmente débil: desafios inerentes e possíveis soluções. Informe e recomendações de boas práticas" (2023); e o "Informe sobre as novas tecnologias e sua relevância para a cooperação jurídica internacional que inclui o Guia de boas práticas em matéria de cooperação jurídica para as Américas" (2023)[30]. Esse último, objeto do presente artigo.

III. TECNOLOGIAS E COOPERAÇÃO JURISDICIONAL NA PAUTA DO COMITÊ JURÍDICO INTERAMERICANO (CJI).

Embora tradicionalmente observada a partir dos interesses dos Estados nacionais, focados em suas governabilidades e numa boa governança internacional, a cooperação jurisdicional, diante das transições do próprio Estado democrático[31], encontra-se em um processo de mudança de lentes. O foco reside, sobretudo, no destinatário final da prestação jurisdicional. O que está em jogo é a tutela de pessoas e direitos.

As tecnologias de comunicação e informação auxiliam no acesso transnacional à justiça, uma vez que permitem maior agilidade e eficiência na prestação jurisdicional e na solução de controvérsias. Essas vantagem somam-se a outras, como a promoção da acessibilidade, vez que o uso das tecnologias promove a diminuição do custo do acesso jurisdicional.

Em 2021, na 98ª sessão ordinária, de 5 a 9 de abril, o Comitê Jurídico Interamericano (CJI) aprova a inclusão em sua agenda de trabalho do tema "As novas tecnologias e sua relevância para a cooperação jurídica internacional"[32]. A proposta foi apresentada pela Dra. Cecilia Fresnedo Aguirre, membro do CJI e responsável pela relatoria do tema, que buscava o desenvolvimento de estudos destinados à análise da atualização dos instrumentos convencionais sobre a matéria

29 Lopes, I. y Moschen, V.: "Os papeis", cit., p. 334.

30 Ver em: Organização dos Estados Americanos (oea): *Temas Culminados (1998-2023)*. Disponível em: http://www.oas.org/es/sla/cji/temas_culminados_recientemente.asp. Acesso em: 4 abr. 2024.

31 Para Haberle, o Estado Constitucional e o Direito Internacional transformam-se em conjunto, criando o Estado Constitucional Cooperativo, que é a resposta interna do Estado Constitucional ocidental livre e democrático à mudança no Direito Internacional (Haberle, P.: *Estado Constitucional Cooperativo*, Renovar, Rio de Janeiro, 2007, p. 132).

32 Fresnedo de Aguirre, C.: *Las nuevas tecnologías y su relevancia para la cooperación jurídica internacional*, Comité Jurídico Interamericano, 2021. Disponível em: https://www.oas.org/es/sla/cji/docs/CJI-doc_637-21.pdf. Acesso em: 2 abr. 2024.

da cooperação aos novos retos da tecnologia, através de um Guia de Princípios. Fresnedo afirma:

"[…] considero que el avance tecnológico es imparable y que no sólo debemos aceptarlo sino utilizarlo con miras a mejorar la cooperación jurisdiccional internacional en todas las materias. Sin perjuicio de avanzar en materia normativa, podemos utilizar mientras – en la medida de lo posible – los instrumentos con que contamos actualmente, como las Convenciones Interamericanas […], aunque actualizándolas en la práctica a través de una Guía, Principios u otro Instrumento que el CJI pueda elaborar"[33].

Como primeiro passo, um estudo foi elaborado com o intuito de se conhecer o estado da arte sobre a legislação, a prática e a doutrina no tema de cooperação jurisdicional e tecnologia. As respostas coletadas no "Cuestionário sobre las nuevas tecnologías y su relevancia para la cooperación jurisdicional internacional" serviram de base para o Guia de Boas Práticas em Matéria de Cooperação Jurisdicional para as Américas[34].

1. Justiça digital e cooperação jurisdicional: o mapeamento do CJI.

A metodologia utilizada para o mapeamento das informações, como mencionado, foi a de realização de um questionário, dividido em três conjuntos de perguntas. Um primeiro, destinado à análise da realidade normativa dos Estados, sobretudo quanto às fontes convencionais – multilaterais, regionais e bilaterais – e autônomas, em matéria de cooperação jurisdicional. A partir das respostas obtidas, permitiu-se identificar as participações dos Estados da região nos instrumentos convencionais interamericanos, multilaterais, "mercosurenhos" e bilaterais[35]. A análise geral do CJI indicou que todos os países que responderam ao questionário são partes de convenções e possuíam normas vigentes em matéria de cooperação.

Um segundo conjunto de perguntas foi direcionado a prática dos tribunais, jurisprudência e atuação das autoridades centrais diante do uso de ferramentas digitais na gestão da cooperação. Foram seis perguntas, destinadas, especialmente,

33 Fresnedo de Aguirre, C.: "Las nuevas", cit., p. 2.

34 Em acordo de cooperação com a ASADIP, o questionário foi distribuído entre especialistas da região. Posteriormente, na reunião de 16 de setembro de 2021 entre a OEA, a Conferência da Haia e os representantes de chancelaria, os Estados-membros da OEA foram convidados a responder o referido questionário. Além dos especialistas de alguns Estados-membros da OEA, como Argentina, Bolívia, Brasil, Colômbia, Cuba, Paraguai e Venezuela, as chancelarias de Canadá, Costa Rica, Equador, Panamá, México e Uruguai também participaram da pesquisa promovida através do questionário. Ver em: Comité Jurídico Interamericano (cji): *Las nuevas tecnologías y su relevancia para la cooperación jurisdiccional internacional*, OEA, Rio de Janeiro, 2023, p. 6. Disponível em: https://www.oas.org/es/sla/cji/docs/CJI-doc_696-23_rev1_ESP.pdf. Acesso em: 2 abr. 2024.

35 Perguntas de "a" a "j". Ver em: Comité Jurídico Interamericano (cji): "Las nuevas", cit., pp. 6-7.

a saber se, no cumprimento das normas convencionais ou autônomas vigentes, a jurisprudência e/ou as autoridades centrais do país utilizam mecanismos tecnológicos[36]. O atual artigo se debruçou nesse grupo de questões, tendo em vista o objetivo de analisar as tecnologias de comunicação e informação na cooperação. A princípio, a utilização de ferramentas tecnológicas é uma realidade em construção na região, assim como a existência de normas autônomas, promotoras da digitalização, como também a utilização de instrumentos digitais por parte dos sistemas judiciários nacionais.

No que tange à doutrina, esta foi analisada nas questões do terceiro grupo. As informações mapeadas pela pesquisa, através do questionário, permitiram uma análise comparada dos argumentos doutrinários sobre os limites e as possibilidades da utilização de tecnologia e de promoção da justiça digital em matéria de cooperação jurisdicional.

Os princípios da imaterialidade e da conexão[37], que se referem, o primeiro, à transformação do processo analógico em digital, e o segundo, à interação judicial e processual com a "web" e demais sistemas de maximização das informações disponíveis na rede, estiveram presentes nas questões relativas aos expedientes e aos documentos eletrônicos. Os princípios da hiper-realidade e da interação[38], que conectam o processo ao mundo virtual, proporcionando maior autenticidade e flexibilidade às partes, também puderam ser observados nas perguntas relativas às notificações, às intimações e às sentenças digitais, assim como nas comunicações entre autoridades judiciárias e/ou autoridades centrais. Conforme a análise realizada pelo CJI, algumas observações comparadas sobre o estado da arte da digitalização processual na região puderam ser apontadas.

A partir do questionário, foi possível delimitar o estado da arte da digitalização e o uso de ferramentais tecnológicas nos sistemas jurídicos e jurisdicionais de Argentina, Bolívia, Brasil, Colômbia, Costa Rica, Cuba, Equador, México, Panamá, Uruguai e Venezuela. As respostas foram elaboradas por profissionais independentes atuantes na área, além de representantes das chancelarias de alguns Estados-membros da OEA[39].

36 Comité Jurídico Interamericano (CJI): "Las nuevas", cit., p. 6.

37 Quanto aos conceitos dos princípios gerais do processo digital, ver Rabelo, T. C.: *Processo judicial eletrônico e digital*, Rideel, São Paulo, 2023, pp. 22-23.

38 Respectivamente conceituados em: Rabelo, T. C.: "Processo judicial", cit., pp. 29 e 31.

39 Na Argentina, os professores Maria Blanca Noodt Taquela e Julio C. Córdoba, além de representantes da chancelaria argentina, foram os que contribuíram com o CJI e responderam às perguntas formuladas. Na Bolívia, as informações foram ministradas, especialmente, pelo Prof. José Manuel Canelas. No Brasil, pela equipe do Grupo de Estudos Labirinto da Codificação do Direito Internacional Privado (LABCODEX), coordenado pelas professoras Valesca Raizer Borges Moschen, Inez Lopes e Martha Olivar Jimenez. Em Cuba, por Taydit Peña Lorenzo. Na Colômbia, por José Luis Marín. Na Costa Rica, participou a Oficina de "Cooperación y Relaciones Internacionales da Área de Derecho Internacional". No México, além dos professores Carlos E. Odriozola e Nuria Gonzáles Martín, a chancelaria daquele país. No Panamá, Sr. Otto A. Escartín Romero, "Director Encargado de Asuntos Jurídicos y Tratados", y Sr. Juan Carlos Arauz

A) Expediente judicial e documentos eletrônicos.

Quanto à existência de processo judicial eletrônico e documentos eletrônicos, aponta-se que, em quase todos os países que responderam à pesquisa, a digitalização dos expedientes processuais passa a ser um fato – com algumas exceções, como na Venezuela, onde não se utiliza o processo eletrônico e os expedientes processuais continuam físicos; entretanto, é possível, naquele sistema, a utilização de documentos eletrônicos em expedientes processuais. No Uruguai, embora haja a previsão legal de expedientes eletrônicos, na atualidade se continua trabalhando com expedientes em formato de papel, sem prejuízo de levar um registro digital deles[40]. Não obstante a prática de processos analógicos, os documentos digitais estão regulados e podem ser utilizados. Por sua vez, no México, o processo eletrônico e a utilização de documentos eletrônicos são utilizados em alguns Estados da Federação, como "Nuevo León", "Estado do México", "Ciudad de México" e no Poder Judicial da Federação[41].

No Brasil, a digitalização do processo judicial já era objeto de estudo e regulação desde 2006, quando da edição da Lei nº 11.419/2006[42]. Quanto aos documentos eletrônicos, são passíveis de serem utilizados como meio de provas, tais como áudios, fotos, conversas eletrônicas e em redes sociais. Os certificados e trâmites processuais realizados, principalmente, pelos secretários notariais são feitos de forma eletrônica, através de um sistema em cada Tribunal de Justiça[43]. Na Argentina, na Bolívia, na Costa Rica e no Panamá, faz-se a previsão normativa de expedientes e documentos eletrônicos, embora sem especificar, explicitamente, sua aplicação para os casos internacionais[44].

B) Assinatura, comunicações e domicílio eletrônicos e digitais.

A assinatura eletrônica e digital, as comunicações eletrônicas e o domicílio digital são utilizados na maioria dos países que participaram do questionário. No México, por exemplo, é possível a utilização de assinatura e comunicações eletrônicas nas regiões onde o processo eletrônico é existente. Na Venezuela, a assinatura eletrônica é passível de utilização, ao passo de não estar permitida

Ramos, "Presidente del Colegio de Abogados de Panamá". No Uruguai, Daniel Trecca e Sr. Marcos Dotta, "Director de Asuntos de Derecho Internacional del Ministerio de Relaciones Exteriores". Finalmente, na Venezuela, María Alejandra Ruiz contribuiu com as informações solicitadas. Ver em: Comité Jurídico Interamericano (cji): "Las nuevas", cit., p. 14.

40 Comité Jurídico Interamericano (cji): "Las nuevas", cit., p. 14.

41 Comité Jurídico Interamericano (cji): "Las nuevas", cit., p. 14.

42 Brasil: *Lei nº 11.419, de 19 de dezembro de 2006*, Diário Oficial da União, Brasília, 2006. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11419.htm. Acesso em: 2 abr. 2024.

43 Comité Jurídico Interamericano (cji): "Las nuevas", cit., p. 14.

44 Comité Jurídico Interamericano (cji): "Las nuevas", cit., p. 15.

a digital. No Uruguai, é cada vez mais frequente que as cartas rogatórias sejam julgadas em formato eletrônico, com firma eletrônica[45].

Quanto às comunicações eletrônicas, na maioria do conjunto de países que participaram do questionário, essas, especificamente, são previstas e utilizadas. Por exemplo, no Panamá, "pueden ser compulsadas como genuinas ante Notario Público pero la información debe ser gestionada y autenticada por un perito informático idóneo dentro de la República de Panamá"[46].

O domicílio digital, entendido como um domicílio eletrônico permanente que concentra todas as comunicações processuais[47], também vem sendo regulado e permitido na região, com exceção de alguns países – o Panamá, por exemplo, não o utiliza; na Venezuela, a previsão do domicílio digital está limitada para efeitos fiscais[48]. No que tange ao domicílio eletrônico contratual constituído no estrangeiro, alguns países, como a Costa Rica, expressamente informam sobre a possibilidade do estabelecimento de um domicílio contratual sempre que seja em uma localidade física dentro ou fora do país, para efeitos de aplicação da Lei de Notificações Judiciais[49]. A Bolívia, em seu Código Processual Civil, informa que as partes "también podrán comunicar a la autoridad judicial el hecho de disponer medios electrónicos (…) como domicilio procesal, a los fines de recibir notificaciones y emplazamientos"[50].

C) Notificações, intimações e sentenças digitais.

Conforme as informações coletadas no questionário, as notificações em geral, incluindo as intimações, são cada vez mais realizadas por via digital. Na Bolívia, por exemplo, o artigo 82 do Código de Processo Civil informa que: "Después de las citaciones con la demanda y la reconvención, las actuaciones judiciales en todas las instancias y fases del proceso deberán ser inmediatamente notificadas a las partes en la secretaria del juzgado o tribunal o por medios electrónicos, conforme a las disposiciones de la presente Sección"[51].

45 Comité Jurídico Interamericano (CJI): "Las nuevas", cit., p. 16.

46 Comité Jurídico Interamericano (CJI): "Las nuevas", cit., p. 17.

47 Art. 3 da Ley de Notificaciones Judiciales, nº 8687, de Costa Rica. Ver em: Costa Rica: *Ley de Notificaciones Judiciales, nº 8687*, Asamblea Legislativa de la República de Costa Rica, San José, 2008. Disponível em: pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=64786&nValor3=75313&strTipM=TC. Acesso em: 2 abril 2024.

48 Comité Jurídico Interamericano (CJI): "Las nuevas", cit., p. 18.

49 Art. 3 da Ley de Notificaciones Judiciales, nº 8687, de Costa Rica. Ver em: Costa Rica: *Ley de Notificaciones Judiciales, nº 8687*, Asamblea Legislativa de la República de Costa Rica, San José, 2008. Disponível em: pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=64786&nValor3=75313&strTipM=TC. Acesso em: 2 abril 2024.

50 Comité Jurídico Interamericano (CJI): "Las nuevas", cit., p. 17.

51 Art. 82 do Código Procesal Civil da Bolívia (Abroga el Código de Procedimiento Civil aprobado por DL 12760 de 06/08/1975). Ver em: Bolívia: *Código Procesal Civil, de 19 de noviembre de 2013*, Órgano Legislativo, 2013. Disponível em: https://bolivia.infoleyes.com/articulo/73268. Acesso em: 2 abr. 2024.

Do mesmo modo, no Brasil, "tanto el Código de Procedimiento Civil como la Ley nº 11.419 establecen la posibilidad de que tanto la citación como la intimación se realicen electrónicamente"[52]. Entretanto, em alguns países, como a Costa Rica, algumas notificações, intimações, resoluções e sentenças requerem a notificação e o cumprimento pessoal, além do domicílio físico[53]. Da análise das respostas do questionário, registra-se que nas regulações nacionais não há, usualmente, distinção para a utilização de meios eletrônicos para os casos de notificação a demandado domiciliado no exterior[54]. As normativas autônomas que regulam o procedimento de uma forma geral e o digital, em especial, não fazem distinção entre casos com ou sem elementos de estrangeria.

Em termos de cooperação jurisdicional, a jurisprudência de alguns países, em particular na época da covid-19, estendeu a possibilidade da realização de notificações e intimações através de ferramentas digitais em casos "pluriconectados". Por exemplo, no Brasil, o veículo para a notificação de parte domiciliada no estrangeiro é a Carta Rogatória. Em abril de 2021, meses antes da promulgação da Lei nº. 14.195/21[55], que alterou o artigo 246 I do Código de Processo Civil[56] – estabelecendo que a principal forma de notificação pessoal será feita preferencialmente por meio eletrônico[57] –, a 7ª Câmara de Direito Privado do Tribunal de Justiça do Estado de São Paulo autorizou, atendendo aos argumentos da parte autora de celeridade e eficiência, que fosse feita a notificação da parte contrária residente no exterior em ação alimentar através do WhatsApp[58].

D) Comunicações entre autoridades judiciais e/ou autoridades centrais.

A comunicação entre autoridades judiciárias e/ou administrativas caracteriza-se pela incorporação das tecnologias de comunicação e de informação, com o fulcro

52 Comité Jurídico Interamericano (cji): "Las nuevas", cit., p. 18.

53 Limitação aplicável, no Brasil, em processos de execução e, na Costa Rica, nos casos de traslado inicial da demanda, imputação de cargos, entre outros. Ver em: Comité Jurídico Interamericano (cji): "Las nuevas", cit., p. 18.

54 Conforme observa-se dos comentários da Profª. Maria Blanca Noodt Taquela e do Profº. Julio C. Córdoba, sobre o Código Procesal Civil y Comercial de la província de Corrientes. Ver em: Comité Jurídico Interamericano (cji): "Las nuevas", cit., p. 18.

55 Brasil: *Lei nº 14.195, de 26 de agosto de 2021*, Diário Oficial da União, Brasília, 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14195.htm. Acesso em: 2 abr. 2024.

56 Brasil: *Lei nº 13.105, de 16 de março de 2015. Código de Processo Civil*, Diário Oficial da União, Brasília, 2015. Disponível em: https://www2.camara.leg.br/legin/fed/lei/2015/lei-13105-16-marco-2015-780273-publicacaooriginal-146341-pl.html. Acesso em: 2 abr. 2024.

57 Parágrafo Primeiro da Lei 14.195, de 26/08/2021, Capítulo X: Da Racionalização Processual, que alterou a redação art. 246 do CPC, que passou a viger da seguinte forma: "Art. 246. A citação será feita preferencialmente por meio eletrônico, no prazo de até 2 (dois) dias úteis, contado da decisão que a determinar, por meio dos endereços eletrônicos indicados pelo citando no banco de dados do Poder Judiciário, conforme regulamento do Conselho Nacional de Justiça". Ver em: Brasil: *Lei nº 14.195, de 26 de agosto de 2021*, Diário Oficial da União, Brasília, 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14195.htm. Acesso em: 2 abr. 2024.

58 Tribunal de Justiça do Estado de São Paulo (tjsp): *Processo nº 2071616-69.2021.8.26.0000,* Foro Unificado da Comarca de São Paulo, São Paulo. Disponível em: https://www.jusbrasil.com.br/processos/387068674/processo-n-207XXXX-6920218260000-do-tjsp. Acesso em: 2 abr. 2024.

de promover maior agilidade e eficiência para a cooperação. Na recompilação das informações ora em análise, pode-se afirmar que, de uma forma geral, os países possuem sistemas de promoção de comunicação eletrônica entre autoridades judiciárias e/ou administrativas na tramitação dos pedidos ativos e passivos da cooperação jurídica internacional.

Na Argentina, por exemplo, conforme informado pelo CJI, a grande maioria das cartas rogatórias diligenciadas pela "Dirección de Asistencia Jurídica Internacional del Ministerio de Relaciones Exteriores, Comercio Internacional y Culto" é recebida através do e-mail institucional cooperacioncivil@mrecic.gov.ar; posteriormente, caso aceitas, as cartas são reemitidas em formato digital às autoridades competentes[59]. Em Cuba, por sua vez, as comunicações se operam por correio eletrônico, via telefônica e, em alguns casos, como o de "Registro de actos de última voluntad", com registros que estão informatizados[60]. No Brasil[61] e no Uruguai[62], a comunicação entre autoridades judiciárias e/ou administrativas na esfera da cooperação é feita, preferencialmente, por meios eletrônicos, sempre que a autoridade central estrangeira assim o permita.

De outro lado, no México, as cartas rogatórias não são usualmente tramitadas por via eletrônica[63]. Na Costa Rica, as comunicações por meios eletrônicos somente se realizam, diretamente, entre autoridades judiciais e consulados e, indiretamente, com autoridades de outros países. Para que se concretize a cooperação, requer-se o envio da solicitude formal através da via diplomática[64]. Estima-se que a elaboração de uma ferramenta, mesmo que não convencional, como o Guia de Boas Práticas, possa auxiliar a transição da justiça analógica para a digital, também na seara da cooperação jurisdicional, a fim de promover o acesso transnacional à justiça de forma ágil e eficiente.

59 Comité Jurídico Interamericano (CJI): "Las nuevas", cit., p. 23.

60 Comité Jurídico Interamericano (CJI): "Las nuevas", cit., p. 24.

61 O Brasil instituiu o sistema COOPERA, que é um programa do Conselho Federal de Justiça, órgão do Superior Tribunal de Justiça, que, em parceria com o Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional, órgão do Ministério da Justiça, busca viabilizar o trâmite eletrônico dos pedidos ativos de cooperação jurídica internacional e a comunicação entre as autoridades judiciárias e as autoridades centrais, a fim de que sejam realizados de forma ágil e simplificada. Ver em: Brasil: *Sistema COOPERA*, Conselho da Justiça Federal. Disponível em: https://www.cjf.jus.br/cjf/CECINT/sistema-coopera-1. Acesso em: 2 abr. 2024.

62 No Uruguai, a autoridade central possui endereços eletrônicos específicos para a cooperação civil e para a cooperação penal, a saber: cooperacioncivil@mec.gub.uy e cooperacionpenal@mec.gub.uy. Ver em: Comité Jurídico Interamericano (CJI): "Las nuevas", cit., p. 24.

63 Comité Jurídico Interamericano (CJI): "Las nuevas", cit., p. 24.

64 Comité Jurídico Interamericano (CJI): "Las nuevas", cit., p. 24.

IV. A JUSTIÇA DIGITAL E O GUIA DE BOAS PRÁTICAS EM MATÉRIA DE COOPERAÇÃO JURISDICIONAL PARA AS AMÉRICAS.

O Guia de Boas Práticas em Matéria de Cooperação Jurisdicional para as Américas, doravante Guia de Boas Práticas, é representativo da harmonização indireta ou informal do direito internacional privado, ou seja, aquela que se desenvolve a partir de mecanismos mais afirmativos e descentralizados[65]. Nasce, como já mencionado, com o intuito de fazer frente aos desafios contemporâneos da virtualidade que atinge o exercício jurisdicional. A dimensão digital da justiça, somada à necessidade de implementação de seu acesso para além das fronteiras dos sistemas jurídicos nacionais, traz para a cooperação uma transição significativa. De um modelo cartorial, a realidade virtual impõe a sua adaptação em prol de sua eficiência e celeridade. A inclusão das tecnologias e a promoção da justiça digital na cooperação promovem uma maior espontaneidade dos atos de cooperação, o que facilita a atuação das autoridades centrais como intermediadoras da cooperação, além de fomentar redes e comunicações diretas entre os sujeitos cooperantes.

O Guia de Boas Práticas possui como objetivo principal instrumentalizar os operadores do direito na utilização das ferramentas tecnológicas e digitais na cooperação jurisdicional. Permite a atualização, quer seja das normas convencionais existentes, quer seja das autônomas dos Estados, sobre cooperação jurisdicional, diante da digitalização da justiça e da inserção das TICs. Embora de caráter regional, vez que concentra as suas soluções às convenções interamericanas e aos instrumentos regionais preexistentes, transcende a esse, já que permite responder às rupturas da cooperação jurisdicional impactada pelas tecnologias de comunicação e informação. Pretende resultar de utilidade para futuros instrumentos ou para a reforma de instrumentos convencionais ou autônomos já existentes. Será aplicado de forma complementária aos Princípios da ASADIP sobre acesso transnacional à justiça (TRANSJUS)[66].

Possui 32 (trinta e duas) regras distribuídas em três conjuntos temáticos: um primeiro, em que estão descritos os seus objetivos; na parte dois do Guia, são estabelecidas regras gerais de interpretação e aplicação das normas convencionais e autônomas vigentes; e na terceira parte, são previstas regras específicas para a cooperação jurisdicional internacional.

65 Glenn, P. H.: "Prospects for Transnational Civil Procedure in America", *Uniform Law Review*, 2003, vol. 1, núm. 2, p. 824.

66 Sobre os Princípios TRANSJUS e seu impacto na harmonização do direito processual civil internacional, ver Moschen, V. y Barbosa, L.: "Hacia el acceso transnacional a la justicia: um análisis de la consonancia entre los princípios TRANSJUS y el Código de Proceso Civil Brasileño CPC/2015", *Revista Jurídica* , 2019, vol. 02, núm. 55, pp. 77-105.

1. Digitalização como vetor de eficiência para a cooperação jurisdicional no Guia de Boas Práticas.

O Guia de Boas Práticas responde aos retos contemporâneos da digitalização processual, ao fazer previsão de regras destinadas – desde a interpretação e a aplicação de normas até a utilização de ferramentas e veículos da cooperação jurisdicional – à busca pela eficiência jurisdicional através do uso de tecnologias na cooperação.

A preocupação com a eficiência está marcada nas regras que exaltam a interpretação ampla e flexível das normas convencionais ou autônomas vigentes[67]; a priorização da finalidade substantiva da norma diante dos formalismos legais, promovendo a espontaneidade de atos[68]; assim como naquelas que fomentam o uso de meios tecnológicos de forma geral – sobretudo para as autuações, audiências e diligências –e a digitalização processual[69] em detrimento de exigências e formalidades presenciais e analógicas. Está observada ainda nas regras promotoras do uso de videoconferência e meios eletrônicos de comunicação para transmissão e recepção de cartas rogatórias, notificações, intimações e outros meios de comunicação[70]; também nas normas que determinam a equiparação na validade e na eficácia de documentos e arquivos eletrônicos ante os analógicos[71].

A eficiência, entretanto, não pode ser vista como um valor em si mesma, mas sim compaginada com os outros valores e garantias processuais para a adequação do exercício jurisdicional. O princípio da eficiência não deve estar acima de outros valores[72], tais como neutralidade, imparcialidade, precisão e acessibilidade. O Guia de Boas Práticas, ao mesmo tempo que proclama pela eficiência, remarca a necessidade de cuidar das garantias processuais no uso da tecnologia e da digitalização na cooperação, como exemplifica a parte final da regra 3 do GBP, que, após indicar a prioridade da interpretação substantiva diante dos formalismos

67 "Regla 1. Interpretación y aplicación de las normas. La interpretación y aplicación de las normas convencionales y autónomas vigentes en cada Estado en materia de cooperación jurisdiccional internacional se hará de forma amplia y flexible […]". Ver em: Comité Jurídico Interamericano (cji): "Las nuevas", cit., p. 42.

68 "Regla 3. Finalidad subjetiva y formalismos legales. […] se priorizará la finalidad sustantiva de las mismas frente a los formalismos legales […]". Ver em: Comité Jurídico Interamericano (cji): "Las nuevas", cit., p. 43.

69 "Regla 5. Utilización de medios tecnológicos. Se utilizarán, en la medida de lo posible, los medios tecnológicos para todas las actuaciones, audiencias y diligencias […] evitando exigir y cumplir formalidades presenciales o similares, que no sean estrictamente necesarias […]". Ver em: Comité Jurídico Interamericano (cji): "Las nuevas", cit., p. 43.

70 Regras 10 e 12 do Guia de Boas Práticas em Matéria de Cooperação Jurisdicional para as Américas. Ver em: Comité Jurídico Interamericano (cji): "Las nuevas", cit., p. 44.

71 "Regla 13. Archivos y documentos electrónicos emitidos por autoridades judiciales y administrativas". Ver em: Comité Jurídico Interamericano (cji): "Las nuevas", cit., p. 46.

72 Sobre o conceito e os parâmetros do princípio da eficiência e sua relação com os valores de justiça, ver Gélinas, F. y Camion, C.: "Efficiency and values in the Constitutional of Civil Procedure", *International Journal of Procedure Law*, 2014, vol. 4, núm. 2, p. 206.

legais, na aplicação das normas convencionais e autônomas, delimita-a diante do respeito das garantias do devido processo legal.

O Guia ainda prevê, na sua Parte 3, regras específicas para a materialização da cooperação jurisdicional internacional a partir da incorporação das tecnologias de comunicação e informação. Nesse apartado, estão previstas regras destinadas, sobretudo, à facilitação da circulação dos veículos da cooperação jurídica, particularmente das cartas rogatórias pela via digital. Propõe-se que o Guia permita a harmonização entre os instrumentos convencionais elaborados, principalmente no processo de harmonização multilateral do tema, e a digitalização da cooperação jurisdicional. Nesse sentido, as regras 23 a 28 destinam-se a guiar os operadores do direito na utilização das cartas rogatórias. Inicialmente, indicam que os Estados utilizem o meio eletrônico para a transmissão dos pedidos de cooperação, qualquer que seja a via de comunicação (judicial, diplomática ou consular ou através de autoridades centrais)[73]. É recomendado que o suporte utilizado para viabilizar a cooperação seja o digital, e, consoante comentários específicos do artigo 24, embora grande parte dos instrumentos convencionais não se refiram ao suporte que deve consignar a carta rogatória, este não deve ser necessariamente em papel. Exorta-se aos Estados que a via digital seja a de praxe[74]. No mesmo sentido, o Guia indica que, com o intuito de promoção da eficiência e da rapidez, os documentos e os requisitos para o cumprimento da cooperação também sejam digitalizados – e, no mesmo sentido, o diligenciamento das cartas rogatórias[75].

Na busca pela eficiência da prestação jurisdicional, o Guia de Boas Práticas requer aos Estados o desenvolvimento, a tecnificação e a utilização das Autoridades Centrais[76] como intermediadoras eficazes da cooperação jurisdicional. Esse movimento de centralização na gestão da cooperação jurídica internacional através das Autoridades Centrais permite maior especialização, sistematização, celeridade, redução de custos e desenvolvimento de uma política pró-cooperativa. As comunicações entre autoridades centrais se caracterizam pela utilização de uma multiplicidade de ferramentas tecnológicas, nomeadamente o correio eletrônico, a videoconferência e outros usos da tecnologia de informação e comunicação. Nesse mesmo sentido, a sistematização da cooperação pela preferência das técnicas de formulários facilita a tramitação de pedidos e promove, em função de sua uniformização, a segurança e a previsibilidade na circulação dos pedidos

73 Regras 23 e 28 do Guia de Boas Práticas em Matéria de Cooperação Jurisdicional para as Américas. Ver em: Comité Jurídico Interamericano (cji): "Las nuevas", cit., pp. 52 e 67.

74 "Regla 24. Soporte en el cual se consigna el exhorto o carta rogatoria. Se recomienda a las autoridades de los Estados la consignación del exhorto en soporte digital". Ver em: Comité Jurídico Interamericano (cji): "Las nuevas", cit., p. 62.

75 Regras 25, 26 e 27 do Guia de Boas Práticas em Matéria de Cooperação Jurisdicional para as Américas. Ver em: Comité Jurídico Interamericano (cji): "Las nuevas", cit., p. 64-65.

76 Conforme as regras 23 e 29 do Guia de Boas Práticas em Matéria de Cooperação Jurisdicional para as Américas. Ver em: Comité Jurídico Interamericano (cji): "Las nuevas", cit., pp. 52 e 70.

de cooperação. O Guia incentiva a utilização desses formulários eletrônicos[77], tendo em vista a contribuição desses para a celeridade processual, através da padronização de pedidos, promovendo uma melhor adequação do acesso à justiça transnacional aos retos da contemporaneidade.

V. O ACESSO TRANSNACIONAL À JUSTIÇA DIGITAL E A CONTRIBUIÇÃO DO GUIA DE BOAS PRÁTICAS: CONSIDERAÇÕES FINAIS.

O acesso transnacional à justiça na era digital impõe aos operadores do direito desafios para além da digitalização dos meios e procedimentos da cooperação jurisdicional transfronteiriça. O Guia de Boas Práticas, ao representar, junto com outros instrumentos de "hard" e "soft law" da harmonização do direito internacional privado, um meio de promoção do acesso adequado e transnacional à justiça, não esgotou suas proposições quanto à utilização das tecnologias de informação e comunicação no campo da cooperação jurisdicional. Diferentemente, buscou, também, consolidar princípios atinentes à relação entre a cooperação jurisdicional e a concretização da cidadania processual transnacional, compreendida como aquela a ser lograda a partir de um exercício jurisdicional "em concreto, com efetividade e segurança jurídica como valores fundamentais[78]".

Nesse sentido, cabe referenciar as regras enumeradas no Guia de Boas Práticas destinadas à interpretação e à aplicação das normas jurídicas convencionais e/ou autônomas e, ao mesmo tempo, aquela destinada ao limite e à extensão da ordem pública ante a cooperação jurisdicional em uma era digital. No primeiro caso, a regra 20 exorta os Estados para que interpretem, de forma evolutiva e progressiva, os instrumentos de "hard" ou "soft law" que regulem aspectos da cooperação jurisdicional que não fizeram menção à utilização de ferramentas tecnológicas por razões cronológicas. A proposta é a de que tais instrumentos possam ser interpretados e, logo, aplicados, de forma dinâmica, com um significado atual, a partir das modificações trazidas pelo impacto da tecnologia de informação e comunicação, em particular na justiça[79]. Por sua vez, a regra 21 proclama aos Estados que desenvolvam, de forma progressiva, sua legislação autônoma que, porventura, seja contrária ou omissa, com o cumprimento de algumas das regras previstas no próprio Guia. A perspectiva é a de que o Guia sirva como um farol na regulação autônoma e/ou advinda da harmonização do direito internacional

77 "Regla 18. Formularios electrónicos. Entre otros instrumentos facilitadores de la celeridad procesal en el ámbito de la cooperación jurisdiccional internacional, se procurará utilizar la técnica de formularios electrónicos modelos". Ver em: Comité Jurídico Interamericano (cji): "Las nuevas", cit., p. 47.

78 Zaneti Jr. H.: *O novo processo civil brasileiro e a constituição. O modelo constitucional da justiça brasileira e o Código de Processo Civil de 2015*, 3. ed., Juspodivum, Salvador, 2016, p. 23.

79 Merece destaque o comentário à regra 20 do Guia de Boas Práticas em Matéria de Cooperação Jurisdicional para as Américas, que afirma que a sugestão estabelecida na referida norma é a de "remediar, precisamente por vía interpretativa, el envejecimiento de los textos normativos". Comité Jurídico Interamericano (cji): "Las nuevas", cit., p. 48.

privado – de origem convencional ou não –, na regulação da cooperação jurisdicional à luz do desenvolvimento tecnológico que, a partir da eficiência, da transparência e da celeridade, permita um adequado, seguro e eficaz acesso à justiça na era digital.

Na parte 3 sobre as regras para a cooperação jurisdicional internacional, o Guia inicia o apartado incitando os Estados à aplicação prioritária da prática mais favorável à cooperação. Essa regra reforça a necessidade do desenvolvimento progressivo da legislação interna permissiva da utilização de ferramentas tecnológicas como meio de eficiência para a cooperação. Sinaliza que as autoridades dos Estados devem priorizar sempre as práticas mais facilitadoras à cooperação jurisdicional e só em circunstâncias excepcionais deixem de aplicá-las[80]. A regra expressa o princípio "in dubio pro cooperationis", também previsto nos Princípios da ASADIP, segundo o qual "as dúvidas que suscitem os conflitos normativos persistentes, se resolverão em favor de uma solução que favoreça a cooperação jurídica internacional[81]".

O Guia finaliza a sua compilação de regras recomendando aos Estados que, especialmente em matéria de cooperação jurisdicional internacional, suas autoridades tenham claro que a utilização de ferramentas tecnológicas não contradiz os princípios fundamentais da ordem pública internacional, uma vez que elas possuem caracteres meramente instrumentais e não afetam aspectos substantivos, desde que se garantam o devido processo legal e a segurança do meio utilizado[82].

As tecnologias de informação e comunicação, ao mesmo tempo que promovem o acesso transnacional à justiça, ainda são utilizadas, como visto na análise do informe do Comitê Jurídico Interamericano (CJI) sobre "Las Nuevas Tecnologías y su Relevancia para la Cooperación Jurisdiccional Internacional", a partir de diferentes percepções e amplitudes pelos sistemas jurídicos nacionais nas Américas. A busca pela promoção de segurança e eficiência no exercício jurisdicional e na tutela de pessoas e direitos, através da cooperação jurisdicional internacional, gestora do acesso transnacional à justiça, levou o CIJ a elaborar um Guia de Boas Práticas em Matéria de Cooperação Jurisdicional para as Américas, ora em análise, que teve como fulcro a convergência entre as necessidades de eficiência e agilidade que a tecnologia proporciona, especialmente diante da promoção da digitalização da justiça, e os instrumentos regulatórios autônomos e/ou convencionais, multilaterais regionais e/ou bilaterais que, em virtude da

80 Regra 23 do Guia de Boas Práticas em Matéria de Cooperação Jurisdicional para as Américas. Ver em: Comité Jurídico Interamericano (cji): "Las nuevas", cit., p. 52.

81 Comentário à regra 22 do Guia de Boas Práticas em Matéria de Cooperação Jurisdicional para as Américas. Principios TRANSJUS: "in dubio pro cooperationes" (art. 1.2b). Ver em: Comité Jurídico Interamericano (cji): "Las nuevas", cit., p. 51.

82 Regra 32 do Guia de Boas Práticas em Matéria de Cooperação Jurisdicional para as Américas. Ver em: Comité Jurídico Interamericano (cji): "Las nuevas", cit., pp. 71-72.

cronologia, não fizeram a previsão da incorporação das ferramentas tecnológicas destinadas à cooperação jurídica internacional. Como visto, trata-se de um instrumento de "soft law" que intenta representar um modelo facilitador do acesso à justiça no âmbito transnacional, diante dos desafios e das facilidades da tecnologia. O Guia recompila regras destinadas à facilitação do uso da tecnologia e do processo de digitalização na promoção da cooperação jurisdicional. Contribui com a possibilidade de interpretação e aplicação, atualizada e dinâmica, de instrumentos convencionais, a partir de suas regras promotoras da eficiência da cooperação jurisdicional, mediante a utilização de ferramentas tecnológicas e da digitalização da justiça. Estima-se a sua utilidade na tutela de direitos e pessoas como vetor de desenvolvimento do "Estado de Direito em âmbito nacional e internacional e da garantia da igualdade de acesso à justiça para todos[83]".

Parafraseando os professores Maria Mercedes Albornoz e Sebastián Paredes[84], não existe um "turning point" para a inclusão das tecnologias de comunicação e informação na cooperação jurisdicional. Cabe assim, como desafio, o aprimoramento dos sistemas jurídicos para que promovam o direito fundamental ao acesso à justiça transnacional e digital. Estima-se que a utilização do Guia de Boas Práticas em Matéria de Cooperação Jurisdicional para as Américas, elaborado pelo Comitê Jurídico Interamericano (CJI), contribua para o avanço do exercício jurisdicional dos Estados nacionais e para o desenvolvimento de novos instrumentos harmonizadores do direito internacional privado, promovendo uma melhor governança na matéria de cooperação jurisdicional nas Américas.

83 Objetivo 16. Promover sociedades pacíficas e inclusivas para o desenvolvimento sustentável, proporcionar o acesso à justiça para todos e construir instituições eficazes, responsáveis e inclusivas em todos os níveis. Ver em: Nações Unidas: *Objetivos de Desenvolvimento Sustentável*, Brasília. Disponível em: https://brasil.un.org/pt-br/sdgs/16. Acesso em: 2 abr. 2024.

84 Albornoz, M. M. y Paredes, S.: "No turning back: information and communication technologies in international cooperation between authorities", *Journal of Private International Law*, 2021, vol. 17, núm. 2, p. 232.

BIBLIOGRAFIA

Albornoz, M. M. y Paredes, S.: "No turning back: information and communication technologies in international cooperation between authorities", *Journal of Private International Law*, 2021, vol. 17, núm. 2, pp. 224-254. Disponível em: https://doi.org/10.1080/17441048.2021.1950332. Acesso em: 2 abr. 2024.

Araújo, N.: *Direito Internacional Privado: Teoria e Prática Brasileira*, 8. ed., Revista dos Tribunais, Rio de Janeiro, 2019.

Bauman, Z.: *Globalização: as consequências humanas*. Tradução: Marcus Penchel. Zahar, Rio de Janeiro, 2021.

Belandro, R.: "¿Qué imagen refleja un tratado de 1889 en el espejo del siglo XXI?", en AA.VV.: *130 años de los Tratados de Montevideo: Legado y Futuro de sus soluciones en el concierto Internacional actual* (coord. por Fresnedo de Aguirre, C. y Lorenzo Idiarte, G.), FCU, Montevideo, 2019.

Bolívia: *Código Procesal Civil, de 19 de noviembre de 2013*, Órgano Legislativo, 2013. Disponível em: https://bolivia.infoleyes.com/articulo/73268. Acesso em: 2 abr. 2024.

Brasil: *Lei nº 11.419, de 19 de dezembro de 2006*, Diário Oficial da União, Brasília, 2006. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11419.htm. Acesso em: 2 abr. 2024.

Brasil: *Lei nº 13.105, de 16 de março de 2015. Código de Processo Civil*, Diário Oficial da União, Brasília, 2015. Disponível em: https://www2.camara.leg.br/legin/fed/lei/2015/lei-13105-16-marco-2015-780273-publicacaooriginal-146341-pl.html. Acesso em: 2 abr. 2024.

Brasil: *Lei nº 14.195, de 26 de agosto de 2021*, Diário Oficial da União, Brasília, 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14195.htm. Acesso em: 2 abr. 2024.

Brasil: *Sistema COOPERA*, Conselho da Justiça Federal. Disponível em: https://www.cjf.jus.br/cjf/CECINT/sistema-coopera-1. Acesso em: 2 abr. 2024.

Castells, M.: *O digital é o novo normal. Virtualidade real na pós-pandemia: um olhar no futuro*, 2020. Disponível em: https://www.fronteiras.com/leia/exibir/o-digital-e-o-novo-normal. Acesso em:2 abr. 2024.

Comité Jurídico Interamericano (cji): *Las nuevas tecnologías y su relevancia para la cooperación jurisdiccional internacional*, OEA, Rio de Janeiro, 2023. Disponível em:

https://www.oas.org/es/sla/cji/docs/CJI-doc_696-23_rev1_ESP.pdf. Acesso em: 2 abr. 2024.

Costa Rica: *Ley de Notificaciones Judiciales, Nº 8687*, Asamblea Legislativa de la República de Costa Rica, San José, 2008. Disponível em: pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=64786&nValor3=75313&strTipM=TC. Acesso em: 2 abril 2024.

Fernandez Arroyo, D.: *La Codificación del derecho internacional privado en América Latina*, Eurolex, Madrid, 1994.

Fresnedo de Aguirre, C.: *Las nuevas tecnologías y su relevancia para la cooperación jurídica internacional*, Comité Jurídico Interamericano, 2021. Disponível em: https://www.oas.org/es/sla/cji/docs/CJI-doc_637-21.pdf. Acesso em: 2 abr. 2024.

Gélinas, F. y Camion, C.: "Efficiency and values in the Constitutional of Civil Procedure", *International Journal of Procedure Law*, 2014, vol. 4, núm. 2.

Glenn, P. H.: "Prospects for Transnational Civil Procedure in America", *Uniform Law Review*, 2003, vol. 1, núm. 2.

Haberle, P.: *Estado Constitucional Cooperativo*, Renovar, Rio de Janeiro, 2007.

Hespanha, A. M.: *Panorama histórico da cultura jurídica européia*, 2. ed., Publicações Europa-América, Lisboa, 1997.

Lopes, I. y Moschen, V.: "Os papeis da OEA e da ASADIP para construção de uma cultura 'Glocal' de Direito Internacional Privado na América Latina", en AA.VV.: *Desafios do direito internacional privado na sociedade contemporânea* (coord. por Lopes, I. y Moschen, V.), Lumen Juris, Rio de Janeiro, 2020.

Moschen, V. y Barbosa, L.: "Hacia el acceso transnacional a la justicia: um análisis de la consonancia entre los princípios TRANSJUS y el Código de Proceso Civil Brasileño CPC/2015", *Revista Jurídica*, 2019, vol. 2, núm. 55, pp.77-105.

Moschen, V. y Barbosa, L.: "O processo civil internacional no CPC/2015 e os princípios ALI/UNIDROIT do processo civil transnacional: uma análise de consonância da harmonização processual", *Revista Eletrônica de Direito Processual – REDP*, 2018, ano 12, vol. 19, núm. 2.

Nações Unidas: *Objetivos de Desenvolvimento Sustentável*, Brasília. Disponível em: https://brasil.un.org/pt-br/sdgs/16. Acesso em: 2 abr. 2024.

Negro Alvarado, D.: "Redefiniendo el rol de las conferencias especializadas interamericanas sobre derecho internacional privado (CIDIPS)", en AA.VV.: *130 años de los Tratados de Montevideo: Legado y Futuro de sus soluciones en el concierto Internacional actual* (coord. por Fresnedo de Aguirre, C. y Lorenzo Idiarte, G.), FCU, Montevideo, 2019.

Opertti Badán, D.: "Compatibilidad e interacción de la codificación regional interamericana con los ámbitos de producción jurídica universal y subregional. Balance de los veinte primeros años de las CIDIP", en AA.VV.: *El derecho internacional privado interamericano en el umbral del siglo XXI: sextas jornadas de profesores de derecho internacional privado*, Eurolex, Madrid, 1997.

Organização dos Estados Americanos (oea): *Carta da Organização dos Estados Americanos*. Disponível em: https://www.oas.org/dil/port/tratados_A-41_Carta_da_Organiza%C3%A7%C3%A3o_dos_Estados_Americanos.htm. Acesso em: 2 abr. 2024.

Organização dos Estados Americanos (oea): *Comissão Jurídica Interamericana*. Disponível em: https://www.oas.org/pt/sobre/comissao_juridica.asp. Acesso em: 4 abr. 2024.

Organização dos Estados Americanos (oea): *Estados Membros*. Disponível em: http://www.oas.org/pt/estados_membros/default.asp. Acesso em: 2 abr. 2024.

Organização dos Estados Americanos (oea): *Histórico do Processo das Cidips*. Disponível em: https://www.oas.org/dil/PrivateIntLaw-HistCidipProc-port.htm. Acesso em: 2 abr. 2024.

Organização dos Estados Americanos (oea): *Quem Somos*. Disponível em: http://www.oas.org/pt/sobre/quem_somos.asp. Acesso em: 2 abr. 2024.

Organização dos Estados Americanos (oea): *Sixth Inter-American Specialized Conference on Private International Law*. Disponível em: https://www.oas.org/dil/CIDIP-VI-finalact-Port.htm. Acesso em: 2 abr. 2024.

Organização dos Estados Americanos (oea): *Temas Culminados (1998-2023)*. Disponível em: http://www.oas.org/es/sla/cji/temas_culminados_recientemente.asp. Acesso em: 4 abr. 2024.

Parra-Aganguren, G.: "La primera etapa de lo tratados sobre Derecho Internacional Privado en América (1826-1940)", *Revista de la Facultad de Ciencias Jurídicas y Políticas*, 1996, vol. 41, núm. 98.

Polido, F.: *Direito internacional privado nas fronteiras do trabalho e tecnologias: ensaios e narrativas na era digital*, Lumen Juris, Rio de Janeiro, 2018.

Rabelo, T. C.: *Processo judicial eletrônico e digital*, Rideel, São Paulo, 2023.

Sholte, A. J.: *Globalization. A critical introduction*, 2. ed., Red Global Press, London, 2005.

Tribunal de Justiça do Estado de São Paulo (tjsp): *Processo nº 2071616-69.2021.8.26.0000,* Foro Unificado da Comarca de São Paulo, São Paulo. Disponível em: https://www.jusbrasil.com.br/processos/387068674/processo-n-207XXXX-6920218260000-do-tjsp. Acesso em: 2 abr. 2024.

Villalta Vizcarra, A. E.: "Viabilidad de las CIDIPS como órgano de codificación del derecho internacional privado", en AA.VV.: *130 años de los Tratados de Montevideo: Legado y Futuro de sus soluciones en el concierto Internacional actual* (coord. por Fresnedo de Aguirre, C. y Lorenzo Idiarte, G.), FCU, Montevideo, 2019.

Zaneti Jr. H.: *O novo processo civil brasileiro e a constituição. O modelo constitucional da justiça brasileira e o Código de Processo Civil de 2015*, 3. ed., Juspodivum, Salvador, 2016.

EL VALOR DEL CONSENTIMIENTO EN LA SOCIEDAD POSMODERNA DE CONSUMO DIGITAL*

THE VALUE OF CONSENT IN THE POSTMODERN DIGITAL CONSUMER SOCIETY

Actualidad Jurídica Iberoamericana Nº 21, agosto 2024, ISSN: 2386-4567, pp. 264-295

* Trabajo realizado en el marco del Proyecto "Los datos como bien patrimonial: uso y protección en el mercado único digital", CIPROM/2022/67, financiado por la Generalitat Valenciana.

Marina
SANCHO
LÓPEZ

ARTÍCULO RECIBIDO: 29 de mayo de 2023
ARTÍCULO APROBADO: 1 de julio de 2024

RESUMEN: La sociedad posmoderna de consumo, decididamente influenciada por la economía digital, ha sufrido notables cambios por lo que respecta a los patrones de consumo y a las lógicas regulatorias tradicionales. Procesos como la datificación social y la comercialización de los datos personales, nos llevan a interrogarnos sobre si el consentimiento, como mecanismo de garantía de la autonomía de la voluntad, ha perdido su significado legitimador, en los términos atribuidos por la dogmática tradicional de los contratos.

PALABRAS CLAVE: Consentimiento; contratos; autonomía de la voluntad; protección de datos; Derecho de consumo.

ABSTRACT: The postmodern consumer society, strongly influenced by the digital economy, has undergone significant changes in terms of consumption patterns and traditional regulatory logics. Processes such as social datification and the commercialization of personal data lead us to question whether consent, as a mechanism for guaranteeing the autonomy of the will, has lost its legitimizing meaning, in the terms attributed by the traditional dogmatics of contracts.

KEY WORDS: Consent; contracts; autonomy of will; data protection; consumer law.

I. INTRODUCCIÓN.

Asumiendo como indiscutible e irretroactivo el cambio imperante en el contexto de consumo de la sociedad moderna y digitalizada, como parte de la deriva capitalista en la que se inserta, partimos pues, de una noción de consumismo que no se limita a las estructuras productivas sino que se extiende a todo el sistema político, económico, social y cultural dominante. Este marco referencial viene perfectamente descrito por Bauman cuando contrapone la noción individual de "consumo" al "consumismo", como atributo de la sociedad misma, como "forma específica de la comunidad humana" alienada de los individuos[1]. Ello se construye mediante la estimulación constante de las personas, a través de todo tipo de técnicas publicitarias, generándoles estímulos y necesidades de consumo bajo la percepción ilusoria de que su satisfacción conducirá a una plenitud y felicidad que, no obstante, jamás se alcanzará por completo en tanto que dichos incentivos se renuevan constantemente y los impulsos son de crecimiento exponencial, al igual que las carencias que intentan suplir y las frustraciones que generan.

Este panorama, ni es nuevo ni revelador aunque sí que lo es el contexto en el que tiene lugar, que ha magnificado el fenómeno, debido al desarrollo de la técnica y las tendencias de consumo digital, no sólo de productos sino también medios, contenidos y servicios. A esto se le une a la velocidad a la que crecen las expectativas y la inmediatez con la que podemos satisfacerlas de forma que, en el bombardeo constante de nuevos productos a consumir, no hay lugar para la reflexión ante el temor de la obsolescencia, lo que altera los ciclos de consumo tradicionales y las pautas de comportamiento. Esto ha sido descrito por el anterior autor como la paradoja de la "perpetua infelicidad" en la que, al mismo tiempo que a los individuos se les promete la satisfacción de todos sus deseos, se les genera constantemente nuevas necesidades que deben satisfacer para alcanzar ese ideal, fruto de los nuevos estándares de productividad y competitividad que tienden a exacerbar los niveles de consumo.

1 Bauman, Z.: *Mundo consumo*, Paidós, Barcelona, 2021, p. 26.

• Marina Sancho López
Profesora Permanente Laboral, Departamento de Derecho civil, Universitat de València.
Correo electrónico: marina.sancho@uv.es

Esta coyuntura debe necesariamente interrelacionarse con el papel de Internet que, junto con las redes sociales, han alterado el patrón consumista tradicional, instaurando estándares de consumo insólitos. Uno de los cambios más significativos del capitalismo digital es la transformación de los individuos en productos de consumo en sí mismos, constituyendo el mayor ejemplo las redes sociales. Lleva tiempo advirtiéndose eso de que "si el producto es gratis, entonces tú eres el producto", y aunque puede que ello sea una visión reduccionista del fenómeno, lo cierto es que en una década hemos pasado del Internet de las cosas al Internet de las corporaciones, donde las cosas somos nosotros y en el que los datos personales son el nuevo producto a comercializar[2].

Partiendo de esta premisa, a continuación se analiza la afectación del nuevo contexto y las herramientas digitales, en especial los algoritmos, a los patrones de consumo y a las lógicas regulatorias tradicionales y de reciente implementación, con la finalidad última de descubrir si el papel del consentimiento, en términos garantistas respecto de la autonomía de la voluntad, ha perdido su significado legitimador, atribuido por las tradicionales teoría de los contratos, en la nueva economía de consumo digital.

II. EL PROCESO DE DATIFICACIÓN SOCIAL.

El cambio de paradigma arriba descrito se yuxtapone a un proceso de datificación social, gracias al desarrollo digital y al uso masivo de sus herramientas, en tanto que el consumismo imperante requiere de la mayor información posible para desplegar su funcionamiento en su máxima extensión. Y en tanto que los individuos, según hemos dicho, son simultáneamente los sujetos destinatarios finales y los objetos a comercializar, esta información que se precisa les concierne en sí mismos, por lo que abarca gran cantidad de datos personales.

El proceso de datificación consiste en procesar información, digitalizándola a través de herramientas tecnológicas para poder clasificarla, almacenarla o tratarla posteriormente, convirtiéndola en datos tangibles y registrables. Es decir, se trata de transformar y cuantificar todos los aspectos de la vida humana a través de información digital que se puede atesorar y reutilizar. En la actualidad, cualquier movimiento cuotidiano puede y es datificado: quienes somos, qué preferencias tenemos, qué decisiones tomamos y/o llevaremos a cabo, etc. Es tan grande la cantidad de datos que generamos a diario, ya sea conscientemente o no, que dicho fenómeno ha recibido el nombre de "Big data" para describir su magnitud.

2 Del Fresno García, M.: "Internet como macromedio: la cohabitación entre medios sociales y medios profesionales", *Revista de Pensamiento sobre Comunicación, Tecnología y Sociedad*, 2014, núm. 99°.

Las ventajas para quienes almacenan estos datos masivos, no reside sólo en la posibilidad de clasificarlos y estructurarlos (tratarlos, en definitiva) en torno a múltiples variables (usos secundarios incluídos) sino en sus posibilidades predictivas, mediante el uso de algoritmos y técnicas de Inteligencia Artificial como el "machine learning". Todo esto sirve a un mismo propósito (por ahora): el consumismo en su máxima extensión. Hablamos en términos económicos, principalmente de marketing personalizado –no sólo de bienes, incluso de ideas[3]– aunque también se aplica a aspectos más nobles pero igualmente controvertidos como ocurre en el ámbito de la biomedicina, y sus aplicaciones futuras están aún por explorar, en tanto que es un campo en continuo desarrollo.

1. Aspectos controvertidos que subyacen al mismo.

La realidad de la datificación da lugar al planteamiento de múltiples cuestiones. Por lo pronto, quién es objeto de datificación y quién queda excluido de dicho proceso. Es decir, si el volumen de extracción o traducción de datos de una persona depende del uso o existencia de su información personal en Internet, es inevitable que ciertos individuos queden al margen de dicho proceso debido a causas diversas (pobreza, geografía, estilo de vida…), por lo que, si el resultado de dicha datificación sirve de base para una influencia o condicionamiento posterior, se estaría distorsionando a favor de las mayorías integradas en el sistema económico y social la lógica que orienta el tratamiento y análisis de los datos masivos[4] y, claro está, la toma de decisiones o su aplicación ulterior.

Por otra parte, el proceso hegemonizador anterior comporta una construcción acrítica del modelo social y económico, cada vez más alejado del libre albedrío, por lo que cabe también preguntarse cuáles son las implicaciones de los procesos de abstracción y fragmentación de las personas a meros datos que, como luego se analizará, comporta una concentración de poder –en manos privadas, además– y nuevas formas de condicionamiento social.

Dejando estos últimos aspectos de lado, así como otras cuestiones consustanciales al fenómeno, como podría ser la vigilancia masiva o la pérdida de la privacidad, y volviendo al hilo inicial, la datificación se trata de un proceso artificial, de abstracción de determinadas realidades, como bien señala Gitelman[5], y por ende, viene precedido de decisiones, intencionalidades o prejuicios.

3 Como expone O'Neil, "nos clasifican y categorizan y nos asignan puntuaciones en cientos de modelos en base a los patrones y preferencias que hemos desvelado. Y esto constituye un poderoso fundamento para muchas campañas publicitarias legítimas, aunque también alimenta a la publicidad depredadora: los anuncios que identifican a las personas con grandes necesidades y les venden promesas falsas o productos a precios excesivos". O'Neil C.: *Armas de destrucción matemática. Cómo el Big data aumenta la desigualdad y amenaza la democracia*, Capitán Swing, Madrid, 2018, p. 89.

4 Lerman, J.: "Big data and its exclusions", *Stanford Law Review,* 2013, núm. 66º.

5 Gitelman, L.: *"Raw data" is an oxymoron*, The MIT Press, Cambridge (Massachusetts), 2013.

En su gran mayoría, esta información personal objeto de datificación viene sometida a un proceso de explotación cuya finalidad última es generar beneficios, como sostienen Mejias & Couldry, la datificación combina dos procesos: la transformación de la vida humana en datos a través de técnicas de cuantificación y la generación de diferentes tipos de valor a partir de los datos[6], "convirtiendo el flujo de la vida social y el significado social en secuencias de números que se pueden contabilizar"[7]. Por otro lado, se trata de un proceso de mercantilización de los datos cuyos beneficios económicos se obtienen por quienes ostentan los mismos, al margen de quienes generan dicha cantidad de información[8].

En este punto, parece ciertamente paradójico que nos encontremos ante un proceso de etiquetaje social, con consecuencias evidentes de desindividualización y que al mismo tiempo, el destino final de dicho proceso, en su mayoría, sea la publicidad personalizada. Como si tuviéramos que desprendernos de nuestra individualidad en pro de una identidad compartida y compatible con otros afines: la individualidad colectiva o transindividual. Esta dicotomía entro lo público y lo privado, en sus múltiples facetas, es una constante en el campo en el que nos encontramos, en tanto que comporta una dimensión íntegra de transformación social, por más que la autonomía privada de las personas juegue un papel central que, como veremos más adelante, a veces es meramente formal.

Sin embargo, uno de los principales obstáculos para garantizar la autonomía de la voluntad y el libre desarrollo de la personalidad, estriba en la dificultad de traducir estos obstáculos privados en problemáticas públicas, y como bien señala Bauman es urgente "galvanizar y condensar los problemas endémicamente privados bajo la forma de intereses públicos que sean mayores que la suma de sus ingredientes individuales"[9].

Y es que estamos hablando de datos personales, cuya protección ha sido intensificada al máximo al conferirle carácter de derecho fundamental y, en este contexto, la voluntad individual deviene presupuesto legitimador para el tratamiento de información privada, del mismo modo que actúa como principio ordenador de la relación entre particulares. La autonomía privada, pues, implica un poder de autodeterminación –o autorregulación jurídica, si se quiere– de toda persona para disponer y ordenar las relaciones jurídicas en las que es o ha

6 Una argumentación similar esgrime ZUBOFF cuando dice que, en el modelo actual, el cual describe como "capitalismo de la vigilancia" se datifica "la experiencia humana, entendiéndola como una materia prima gratuita que puede traducir en datos de comportamiento". Zuboff, S.: *La era del capitalismo de la vigilancia*, Paidós, Barcelona, 2019, p.21.

7 Mejias, U. & Couldy, N.: "Datificación", *Revista Latinoamericana de Economía y Sociedad Digital*, 2022, Julio.

8 Sobre la percepción de beneficios y el funcionamiento del Big data, Vid. Martínez Velencoso, L.M. & Sancho López, M.: "El nuevo concepto de onerosidad en el mercado digital, ¿Realmente es gratis la App?", *InDret*, 2018, Enero.

9 Bauman, Z.: *Modernidad líquida*, Fondo de Cultura Económica, Madrid, 2017, p.21.

de ser parte, en íntima conexión con la libertad y la dignidad personal, derechos inviolables ambos e inherentes al libre desarrollo de la personalidad.

Sin embargo, este poder de disposición de los individuos y la eficacia vinculante que genera el consentimiento prestado, en consecuencia, debe venir precedido de una igualdad material y la libre voluntad de los sujetos, que dote a la autonomía privada de un carácter verdaderamente autónomo, en tanto que la libertad personal deviene fundamento de la autonomía individual[10].

Así las cosas, las preferencias y el consentimiento de una persona para obligarse adquieren una notoriedad indiscutible en este ámbito, así como en la constitución de los negocios jurídicos que dan lugar al tratamiento de datos personales. Es por ello que, a lo largo de estas páginas, nos interrogamos sobre el contexto y las condiciones ambientales en las que se forma y manifiesta el consentimiento para el tratamiento de datos personales, como cristalización de la autonomía de la voluntad en la nueva economía digital.

2. Transparencia algorítmica en el Derecho contractual y de consumo.

Esta nueva sociedad de consumo, para servir al objeto de su causa, requiere de una estratificación de la sociedad en general y los individuos en particular, capaz de identificar las necesidades existentes y catalogar los sujetos destinatarios potenciales. Es por ello que el proceso de datificación social al que antes hacíamos referencia, se asienta sobre el cálculo algorítmico, en tanto que es el mecanismo que permite estructurar los datos y dotarlos de significado, como se observa en el campo de la Inteligencia Artificial, donde los algoritmos de aprendizaje progresivos son consustanciales al funcionamiento mismo de la herramienta.

En este punto, debemos hacer algunas consideraciones. En primer lugar, sobre el funcionamiento mismo del algoritmo, como herramienta de clasificación o etiquetaje –proceso correlativo al desglose efectuado por la datificación–, en tanto que permite procesar los datos en múltiples variables, reconfigurando nuestra identidad –sobre todo cuando hablamos de datos personales– para instrumentalizar los diversos rasgos en los que hemos sido desgranados en base, como veremos luego, a intereses de terceros. Se fomenta así un proceso reduccionista y simplificador de etiquetaje respecto de determinados colectivos, a partir de prácticas discriminatorias de tipo social o económico, que pueden determinar una segregación excluyente de los grupos afectados y cuyo reflejo, afecta también al ámbito de la autonomía privada y la contratación.

10 De hecho, hay quien exige que la nota de alteridad esté presente para que la regla creada por un individual adquiera relevancia jurídica. Vid. Capilla Roncero, F. "Autonomía de la voluntad y Derecho de la persona o la autonomía personal en el Derecho privado", *Diario La Ley*, 2011, núm. 7685º.

Por otra parte, conocer de forma verdaderamente transparente la lógica de funcionamiento del cálculo algorítmico no resulta posible, pues gracias a las políticas de privacidad y la salvaguarda del secreto empresarial, está dotada de gran opacidad. Mientras tanto, los riesgos de legitimar cualquier tipo de decisión basada en los cálculos algorítmicos son evidentes en términos de segmentación, discriminación y exclusión, pero también en términos de libre albedrío porque, al omitir la capacidad crítica, no se dan las garantías para que exista racionalidad decisoria, quedando en entredicho el consentimiento prestado.

Sobre lo anterior, cabría reflexionar acerca de la capacidad del cálculo algorítmico de incidir en el proceso de formación de voluntades pues, como se ha expuesto al inicio, nos encontramos ante dinámicas que constituyen nuevas formas de ordenación de los procesos sociales lo cual, para empezar, resulta difícilmente compatible con el razonamiento crítico. La falta de transparencia inherente a dichos procesos, unida a las técnicas nuevas de marketing personalizado, buscan generar necesidades, condicionar las preferencias de los usuarios –quienes, muchas veces, desconocen las técnicas a las que están siendo sometidos– o modificar subliminalmente su comportamiento, lo que sin duda afecta a sus posibilidades de decisión, restringiendo su capacidad electiva. Como más tarde se abordará, no existe neutralidad en estos procesos como tampoco en el mero almacenamiento de datos y, aunque así fuera, encontramos una discriminación estructural que viene integrada por procesos sociales difusos y sistémicos –al margen de la intencionalidad de las personas individualmente consideradas–, que se reproduce a través de los mismos, en tanto que atraviesan todas las dimensiones de la existencia, de ahí su afectación a la capacidad de toma de decisiones y formación de preferencias[11]. Ahí justo reside el nexo con el principio de autonomía de la voluntad que, aunque sea en abstracto libre, viene preconfigurado por una serie de elementos condicionantes que no pueden ignorarse pues, desconocer u ocultar los patrones de discriminación estructural puede llevar a presentar como una decisión libre algo que, en realidad, es una preferencia adaptativa o una decisión marcada por un estado de necesidad que invalida la presunción de consentir de manera libre e informada.

Teniendo lo anterior en cuenta, debemos cuestionar el alcance de la libertad de elección en estos procesos de formación de las necesidades y la posible alteración que sufre en la cultura consumista actual en la que la minimización del tiempo para formar y materializar una elección deviene inherente a su lógica de funcionamiento. Si relacionamos dichas variables, esto es, tiempo de reflexión y confirmación de la elección, con los procesos de injerencia y alteración de las preferencias y/o necesidades personales, parece oportuno preguntarse acerca de

11 Añón Roig, M.J.: "Transformaciones en el derecho antidiscriminatorio: avances frente a la subordinación", *Revista electrónica del Instituto de Investigaciones Jurídicas y Sociales Ambosio Lucas Gioja*, 2021, núm. 26°, p. 52.

las consecuencias que ello pueda tener en la formación del libre albedrío y la manifestación de la autonomía de la voluntad.

La opacidad de los procesos de tratamiento opera en un sentido amplio, no sólo desde el momento de recabar los datos personales, sino también en los sesgos que impregnan el propio diseño y funcionamiento de los algoritmos, lo que nos lleva a cuestionar la totalidad del modelo y, en lo que aquí nos interesa, arroja grandes dudas acerca de la integridad de la autonomía privada en la formación de los contratos, pues no cabe duda de que el contexto presentado genera influencias desde la emisión de la oferta hasta la propia perfección del contrato, pasando por la manifestación y formación de la voluntad.

A continuación, pues, se rebate la imposición de valores inmutables u ontológicos basados en un conocimiento técnico que, además de obviar los límites de ciertas prácticas que, amparadas en el desarrollo y la innovación, son capaces de vulnerar derechos y libertades y desnaturalizan el significado social de las normas jurídicas. Rechazamos así, la preeminencia algorítmica acrítica, en tanto que facilita sesgos y perpetúa discriminaciones, lo que puede resultar especialmente asfixiante en el ámbito jurídico[12], dónde ni siquiera los derechos humanos pueden concebirse como un fenómeno neutral[13].

3. La paradoja de lo neutro.

Si los procesos de datificación arriba descritos, en apariencia neutrales, no pueden ser considerados como tales en tanto que derivan de situaciones y posiciones intrínsecamente ligadas al poder (quién crea y ostenta la propiedad de las plataformas en las que se propagan los datos, para qué aplican los mismos, la forma en las que se genera la información o el valor monetario atribuido a la misma[14]), tampoco lo es el cálculo algorítmico empleado para el tratamiento de dicha información.

Se trata de procesos selectivos en base a parámetros elegidos y algoritmos diseñados por personas, corporaciones o entidades que, por lo general, nada tienen que ver con causas filantrópicas, de forma que, por ejemplo, la mera

12 Añón Roig va más allá, al afirmar que la inteligencia artificial se desarrolla al margen de los derechos, "de su lógica, de sus principios y de sus criterios interpretativos" hasta el punto de estar "exenta de derechos humanos". Añón Roig, M.J.: "Desigualdades algorítmicas: conductas de alto riesgo para los derechos humanos", *Derechos y Libertades*, 2022, núm. 47º, p. 18.

13 Compartimos la visión de Mayer-Schönberger & Cukier cuando dicen que "en la era de los datos masivos, tendremos que ampliar nuestra visión de la justicia y exigir que incluya salvaguardias para el albedrío humano, del mismo modo que, en la actualidad, velamos por la imparcialidad procesal. Sin esas salvaguardias, la idea misma de la justicia podría debilitarse por completo". Mayer-Schönberger, V. & Cukier, K.: *Big data. La revolución de los datos masivos*, Turner, Madrid, 2015, p. 216.

14 Un ejemplo sobre los efectos negativos de la estratificación económica de distintos grupos sociales lo encontramos en Fourcade, M. & Healy, K.: "Classification situations: Life-chances in the neoliberal era", *Accounting, Organizations and Society*, 2013, núm. 38º.

intención de maximizar los beneficios económicos está dotada de significado e impregna todo el proceso de tratamiento, que no deviene en absoluto objetivo, por más que se trate de una finalidad enteramente legítima.

De hecho, las conductas de acopio de datos de forma masiva evidencian una lógica capitalista[15] en tanto que, o bien directamente se les confiere el valor de mercancía, o bien son considerados un factor de producción en términos de capitalización[16], siendo ambos supuestos una forma de incrementar los ingresos económicos a través del comercio de información personal, motivo por el cual Zuboff lo considera el ejemplo más palmario de capitalismo[17].

Hay que tener presente que, por mucho que los algoritmos puedan responder a razonamientos matemáticos ciertos, fruto de una lógica científico-numérica, ello no obsta para que presenten determinados sesgos o limitaciones cuando traspasan el ámbito acrítico ideal, propio del pensamiento científico, para aplicarse en el *ámbito* conflictivo de los procesos sociales. De acuerdo con O'Neil, "las aplicaciones fundamentadas en las matemáticas que alimentaban la economía de los datos se basaban en decisiones tomadas por seres humanos que no eran infalibles. Seguro que algunas de esas decisiones se tomaban con la mejor de las intenciones, pero muchos de estos modelos programaban los prejuicios, las equivocaciones y los sesgos humanos en unos sistemas informáticos que dirigían cada vez más nuestras vidas"[18].

Así pues, no puede despreciarse el riesgo de que los parámetros que orientan el cálculo algorítmico puedan establecer una serie de desigualdades en el tratamiento de las realidades a las que se dirijan. Por ejemplo, piénsese en la posibilidad de establecer variables relacionadas, con el nivel económico o la procedencia social de los sujetos destinatarios del cálculo algorítmico. Si bien puede presentarse como un criterio técnico, sin ningún ánimo discriminatorio respecto de sus destinatarios, resultan innegables los riesgos de que este tipo de prácticas puedan terminar en

15 Como señala Monasterio Astobiza, tanto el cálculo algorítmico como el Big data en el que opera, no son realidades sociales neutras, en tanto que, pese a revestir un carácter científico-técnico, la forma de orientar esta evolución, por ejemplo, respecto al valor monetario atribuido a los datos masivos, muestra una opción ideológica concreta. Monasterio Astobiza, A.: "*Ética algorítmica: implicaciones éticas de una sociedad cada vez más gobernada por algoritmos*", *Dilemata*, 2018, núm. 24°.

16 Otros autores como Sadowski o Gregory equiparan directamente los "datos" al "capital", encontrando paralelismos tanto teóricos como financieros. *Vid.* Sadowski.: "When data is capital: Datafication, accumulation and extraction", *Big Data & Society*, 2019, vol. 6. Gregory, K.: "Big data, like Soylent Green, is made of people", *CUNY*, 2014.

17 Y como argumento, añade: "Aunque algunos de dichos datos se utilizan para mejorar productos o servicios, el resto es considerado como un excedente conductual privativo («propiedad»)". Zuboff, S.: *La era del capitalismo de la vigilancia*, cit., p.21.

18 O'Neil, C.: *Armas de destrucción matemática. Cómo el Big data aumenta la desigualdad y amenaza la democracia*, cit., p. 11.

un mero proceso simplificador y reduccionista de etiquetaje de la ciudadanía en función de su acceso a los recursos[19].

Sobre la premisa anterior, mucho más significativo deviene el posterior procesamiento de datos pues, si su mera recopilación puede evidenciar ciertos sesgos, estos se incrementan exponencialmente conforme se van sistematizando, sometiendo a métodos analíticos, reestructurando, interpretando sus resultados o reciclando los mismos.

Así, la consumación usual de estos procesos da lugar, según ciertos autores, a la creación de una "sociedad de clases digital"[20] que, en casos extremos, pueden producir la exclusión o la creación de colectivos silenciados –como se apuntaba al inicio–, en tanto que no se atiende a sus preferencias o comportamientos para la oferta de bienes y servicios por el Mercado –ni siquiera por parte de los poderes públicos que, al desestimarlos, podrían excluirlos de sus políticas asistenciales–. Y es que, generalmente los algoritmos se emplean para tomar decisiones, en lo que se ha denominado "automated decision-making," así como para la elaboración de perfiles. Y aquí residen las reticencias a dichos procesos, fundamentalmente por la opacidad y los peligros inherentes a los mismos, pues los individuos no ostentan ningún control sobre el conocimiento que se está obteniendo a través de su información personal, alterando gravemente las expectativas de las personas y afectando a la noción misma de la autonomía de la voluntad, y con innegable incidencia en los procesos de formación y manifestación del consentimiento.

III. LA EVOLUCIÓN DE LA AUTONOMÍA PRIVADA EN EL MARCO REGULATORIO.

Los fenómenos arriba esbozados no resultan ajenos al legislador, que da cuenta de ellos en las diversas normas sectoriales que tratan alguna de estas cuestiones, desde el Reglamento de Servicios Digitales[21] hasta la nueva normativa de Inteligencia Artificial[22] pasando, como no, por el Reglamento europeo de protección de datos personales (RGPD)[23]. A través de su análisis, en lo que concierne al objeto de este estudio, puede apreciarse una evolución del tratamiento y conceptualización del

19 Por ejemplo, en el ámbito de la contratación, donde podrían darse supuestos de discriminación genética al denegar coberturas o incrementar los precios de las pólizas de seguros de vida, en base a la predisposición genética a sufrir determinadas enfermedades.

20 Han, B.: *Psicopolítica*, Herder, Barcelona, 2014, p. 99.

21 Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022 relativo a un mercado único de servicios digitales.

22 Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial, al escribir estas líneas, pendiente de aprobación por la Eurocámara.

23 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

consentimiento en tanto que es el mecanismo a través del cual la persona titular autoriza a terceros al tratamiento de su información más personal.

Como luego se incidirá, el consentimiento resulta parte indispensable en la teoría del negocio jurídico y, trasladado al campo de la protección de datos, se erige en la figura cardinal a través de la cual se produce una afectación al derecho fundamental de privacidad. Es decir, el Ordenamiento jurídico permite que, mediante el consentimiento, una persona autorice a que se produzcan interferencias en su esfera privada que, en su ausencia, devendrían ilegítimas. Es por ello que la declaración de voluntad de una persona puede constituir en sí misma un negocio jurídico debido a que se ejercita, con ello, su autonomía de la voluntad en lo que Perez Luño define como la "paulatina, pero, decisiva decantación desde la esfera de la personalidad al ámbito patrimonial"[24].

Así pues, el consentimiento viene reconocido, tradicionalmente, como una causa legitimadora de la intromisión en determinados derechos y libertades, como se puede apreciar en múltiples normativas reguladoras de distintas materias –desde la LO 1/82 de protección civil del derecho al honor, la intimidad personal y familiar y la propia imagen, hasta la Ley 14/2007, de Investigación biomédica–. Este consentimiento, para que sea válido, debe venir precedido de la información previa necesaria para que sea formado un juicio de valor con todos los elementos y, en consecuencia, su manifestación sea libre y auténtica. Surge así el concepto de "consentimiento informado", que exige a quienes recauden información personal que expliciten a las personas interesadas cómo y para qué van a ser usados sus datos, de forma que puedan comprender y hacerse un juicio de valor previo acerca de lo que van a consentir y las implicaciones que pueden dimanarse.

A este consentimiento informado, respecto de la materia que nos ocupa, se le ha venido reconociendo y exigiendo la concurrencia de requisitos adicionales: especificidad, necesidad de transparencia y un poder de disposición sobre la información personal. La especificidad, unida al carácter inequívoco del consentimiento, exige poner en conocimiento de la persona interesada toda la información necesaria para que la manifestación de su voluntad se adecúe a la finalidad concreta para la que presta su beneplácito, eliminando toda sospecha de ambigüedad y no siendo extensible a otras realidades. Esto queda patente en el art. 8 de la Carta de los derechos fundamentales de la Unión Europea que exige, para el tratamiento de los datos personales, un consentimiento previo de la persona afectada, obtenido de forma leal y para fines concretos. Ello se extendió,

24 Pérez Luño, A.E.: "Principios de la protección de datos: consentimiento del afectado. El consentimiento de los menores", en AA.VV.: *Comentario a la ley Orgánica de Protección de Datos de Carácter Personal* (dir. por Troncoso Reigada), Civitas, València, 2010, p. 483.

posteriormente, en la derogada Directiva 95/46/CE de protección de datos[25] a la identidad de la persona responsable y los fines de tratamiento, de forma que la autorización dada por el sujeto venga precedida de una comprensión integral de los hechos e implicaciones a los que da lugar.

Esto viene intrínsecamente relacionado con la noción de transparencia, desarrollada posteriormente para enfatizar la exigencia de dotar de información previa sobre todos y cada uno de los aspectos que puedan comprometer la prestación del consentimiento, desde un punto de vista tanto subjetivo como sustantivo. El propio Reglamento de protección de datos establece el contenido mínimo de información que debe suministrarse previamente al interesado para que pueda prestar un consentimiento informado sobre sus datos, ampliado respecto de la normativa anterior[26]. Además, la prestación informada, específica, afirmativa e indubitada del consentimiento, debe venir acompañada de una serie de garantías que orbitan sobre todo el proceso material de formación y prestación del consentimiento. Es decir, la transparencia se proyecta no sólo sobre la información proporcionada sino en el cómo se proporciona la misma y su calidad: de forma accesible, en un formato apropiado, legible, comprensible y adaptada a cada destinatario[27]. Así, por ejemplo, debe emplearse un lenguaje claro y sencillo para informar al sujeto interesado de todos los pormenores que entrañan el almacenamiento o tratamiento de sus datos personales, con el objeto de conseguir unas condiciones materiales idóneas de formación de la voluntad. Además, esta transparencia no se limita al estado previo a la prestación del consentimiento, sino que se extiende al tiempo durante el que se realice el tratamiento y después de una solicitud del interesado de acceder a sus propios datos[28].

Por último, viene reconocida también una esfera de libertad personal en sentido amplio, permitiendo a la persona interesada ejercitar un control efectivo sobre sus datos y garantizándole un poder de disposición sobre su información privada. Conocido como "habeas data", se trata de enfatizar la dimensión volitiva de la política de protección de datos, directamente intrincada con el derecho a

25 Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

26 Esto es, la identidad y datos de contacto del responsable y del delegado de protección de datos, los fines de tratamiento y su base jurídica, los destinatarios de los mismos y si son o no susceptibles de transferirse a terceros así como la existencia de decisiones automatizadas (incluida la elaboración de perfiles), el plazo de conservación, la existencia de los derechos de acceso, rectificación, supresión y retirada del consentimiento, así como a presentar una reclamación ante una autoridad de control y la existencia de decisiones automatizadas (art. 13 RGPD).

27 Considerando 39 RGPD: "Todo tratamiento de datos personales debe ser lícito y leal. Para las personas físicas debe quedar totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales que les conciernen, así como la medida en que dichos datos son o serán tratados. El principio de transparencia exige que toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro".

28 "Opinion 2/2017 on data processing at work", Article 29 Working Party, p.22.

la autodeterminación informativa. De este modo, se pone de relieve la vertiente positiva del derecho de protección de datos, en su manifestación más amplia de la libertad personal, a través de la cual se garantiza la igualdad y el trato no discriminatorio en su máxima extensión[29].

En definitiva, la normativa reguladora, consciente de los cambios en el modelo que produce el avance de la técnica y los riesgos que de ello se derivan para los derechos y libertades fundamentales, viene tratando de incrementar el poder de control de la ciudadanía sobre sus datos personales, mediante la exigencia de una mayor transparencia y reforzando el papel del consentimiento informado. Sin embargo, ello no ha venido acompañado de una mayor garantía material de los derechos y libertades, de hecho, queda patente en la propia normativa la existencia de grietas en el sistema de protección.

Un ejemplo lo encontramos en materia de transferencia internacional de datos, pues el Reglamento europeo –también la normativa anterior–, establece una prohibición general en cuanto a la cesión de datos personales de ciudadanos europeos a terceros países que no cuenten con ciertos estándares de protección[30]. Entre estos, encontramos a los Estados Unidos, territorio hacia el cual se ha ido produciendo un éxodo masivo de las empresas tecnológicas de datos debido a que, la laxitud de su legislación, deviene más favorable para sus intereses económicos. Pues bien, pese a la prohibición general de transferir datos a terceros países con menores estándares de protección, se han venido materializando acuerdos entre la Unión Europea y los Estados Unidos en pro del intercambio comercial de datos, como ocurrió, en primera instancia, con el Safe Harbor –declarado invalido por la Sentencia del TJUE de 2015 en el caso Schrems I[31]–, el posterior Privacy Shield que lo sustituyó –y que también se declaró nulo en 2020 por el caso Schrems II[32]– y el actual EU-U.S. Data Privacy Framework (DPF)[33]. Es decir, de facto, por la vía de los acuerdos de adecuación y las cláusulas tipo contractuales, se viene permitiendo a las grandes corporaciones del Big data especular con los datos personales de los ciudadanos europeos con cierta impunidad, sorteando los principios inherentes a

29 Ello se observa, por ejemplo, en el reconocimiento del derecho de supresión (art.17 RGPD) que, más allá de reconocer un ámbito de privacidad frente a la intromisión ajena, estipula la potestad de reaccionar frente a una situación de vulneración, concediendo a los interesados la posibilidad de obtener del responsable la supresión de sus datos personales y, en caso de incumplimiento, acceder a una indemnización por daños y perjuicios.

30 Arts. 23 y 44 RGPD.

31 STJUE de 6 de octubre de 2015, asunto C-362/14.

32 STJUE de 16 de julio de 2020, asunto C-311/18.

33 Aprobado el 10 de Julio de 2023 por el Parlamento Europeo y la Comisión Europea, disponible en: https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf

la normativa europea de protección de datos, pese a la limitada seguridad jurídica que éstos ofrecen como mecanismo efectivo de control[34].

Por otro lado, el art. 6.4 del Reglamento permite de facto la reutilización de aquellos datos personales que, pese a no contar con el consentimiento de la persona interesada, exista una compatibilidad entre el fin para el que se recogió la información y la finalidad a la que ahora se pretenda destinar, cuando "constituya una medida necesaria y proporcional en una sociedad democrática". Incluso se prevé la posibilidad de prescindir de la compatibilidad de los fines "si el interesado dio su consentimiento o el tratamiento se basa en el Derecho de la Unión o de los Estados miembros que constituye una medida necesaria y proporcionada en una sociedad democrática para salvaguardar, en particular, objetivos importantes de interés público general" (considerando 50 RGPD).

Un paso más allá da el Reglamento de Gobernanza de Datos[35], aplicable desde septiembre de 2023, que tiene por objeto de reutilización de determinadas categorías de datos dentro del sector público, con el objeto de fomentar la circulación, el intercambio y la disponibilidad de los datos protegidos del sector público, también datos personales, para su reutilización. Esta normativa parte de la premisa de que los datos son elementos centrales de la transformación económica y social, por lo que, su cesión y reutilización no sólo deviene inevitable en el escenario actual sino que resulta deseable desde el punto de vista del avance socioeconómico[36]. Así, con la finalidad de conseguir un "régimen horizontal" para la reutilización de determinadas categorías de datos protegidos en poder de organismos del sector público y la prestación de servicios de intermediación de datos y de servicios basados en la cesión altruista de datos, se fomenta el intercambio de datos en el mercado interior, mediante la creación de un marco armonizado para el intercambios de datos entre los Estados miembros, con el objetivo desarrollar en mayor medida el mercado interior digital sin fronteras y una sociedad y economía de los datos "centradas en el ser humano, fiables y seguras". Se evidencia pues, un cambio de criterio respecto de lo dispuesto en el RGPD, aparentemente basado en la limitación del almacenamiento, uso e intercambio de los datos personales, como elementos inherentes a la condición humana e

34 Ello viene señalándose reiteradamente por el GT29. Vid. Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision, 2016. Disponible en: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf

35 Reglamento (UE) 2022/868 del Parlamento europeo y del Consejo, de 30 de mayo de 2022, relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724.

36 Así se esgrime en los primeros considerandos de la norma "la innovación basada en los datos reportará enormes beneficios tanto a los ciudadanos de la Unión como a la economía […] La economía de los datos se tiene que desarrollar de manera que permita prosperar a las empresas, especialmente las microempresas y las pequeñas y medianas empresas (pymes), tal como se definen en el anexo de la Recomendación 2003/361/CE de la Comisión y a las empresas emergentes, garantizando la neutralidad en el acceso a los datos y su portabilidad e interoperabilidad, y evitando los efectos de dependencia".

intrínsecamente relacionados con los derechos de la personalidad, mutando hacia una concepción de los datos como bienes comunes, de interés general.

Por otro lado, la propuesta de Reglamento de Inteligencia Artificial[37] pivota sobre el reconocimiento del impacto que la Inteligencia Artificial (IA) puede generar en los derechos y libertades, dando lugar "a nuevos riesgos o consecuencias negativas para personas concretas o la sociedad en su conjunto", muestra de ello, es la disposición de una lista de prácticas de IA prohibidas, entre las cuales se contempla cualquiera que impida a las personas decidir libremente ser sometidas o no a sistemas de IA (art. 5), por lo que podría pensarse que, de facto, impone la necesidad de contar con un consentimiento informado. Nada más lejos de la realidad. La noción de transparencia que contempla este texto normativo difiere notablemente del comprendido en el RGPD pues parece limitarse a advertir a los sujetos que están interactuando con un sistema de IA pero no dice nada sobre que sean informados de la lógica inherente al mismo, ni de los riesgos existentes, los fines de tratamiento, los derechos que pueden ejercitar, la claridad en la información suministrada o las garantías que se aplican para salvaguardar sus derechos. Es decir, ambos reglamentos imponen obligaciones distintas, a distintos sujetos y respecto de distintas categorías de información por lo que, podría dar lugar a que, proporcionando a una persona interesada la información elaborada sobre la noción de transparencia del Reglamento de IA, no se cumplan los deberes de transparencia en los términos del RGPD. Y es que, el grueso de la normativa destaca reiteradamente los beneficios económicos y sociales que esta nueva tecnología puede suponer "en todos los sectores y las actividades sociales", justificando como base jurídica del texto no ralentizar la adopción de la IA por parte del Mercado. Así, al mismo tiempo que afirma los peligros inherentes a estas técnicas en términos de igualdad, dispone previsiones que pueden alterar los principios generales de protección de datos[38].

Procede también señalar la Ley 15/2022 de 12 de julio integral para la igualdad de trato y la no discriminación, la cual hace referencia expresa por primera vez en nuestra legislación, a las consecuencias discriminatorias que pueden provocarse mediante el uso de la inteligencia artificial y la gestión masiva de datos por parte de las administraciones públicas y las empresas privadas. Sin embargo, respecto de lo aquí tratado, sólo dispone principios programáticos para las administraciones públicas, en términos de buena fe y transparencia[39].

37 Disponible en: https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0008.02/DOC_1&format=PDF

38 Un ejemplo se observa en su artículo 10, a través del cual se contempla una excepción a la prohibición de tratar categorías especiales de datos establecida, entre otras normas, por el artículo 9 del RGPD, y que viene justificada por las categorías sospechosas de producir discriminación.

39 "Las administraciones públicas favorecerán la puesta en marcha de mecanismos para que los algoritmos involucrados en la toma de decisiones que se utilicen en las administraciones públicas tengan en cuenta criterios de minimización de sesgos, transparencia y rendición de cuentas, siempre que sea factible

En la misma línea procede la Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital, del 23 de enero de 2023 que, en manifestaciones comunes del Parlamento Europeo, el Consejo y la Comisión europea, reconoce el carácter lesivo de la nueva coyuntura digital –en especial, los sistemas algorítmicos y la inteligencia artificial– para la autonomía de la voluntad, sin proponer ni contener cambios políticos o jurídicos capaces de revertir las tendencias actuales[40].

En definitiva, si bien encontramos textos reguladores que hacen referencia a algunas realidades aquí expuestas, estos son escasos y tibios en sus pronunciamientos, sobre todo teniendo en cuenta la magnitud de los procesos a los que nos referimos y el alcance material de sus consecuencias. Así, la garantía integral a la autonomía de la voluntad no está salvaguardada, en tanto que, por ejemplo, la transparencia algorítmica ni se garantiza ni puede reclamarse por ningún medio legal, quedando todo ello a merced de los principios de buena fe y responsabilidad proactiva de los operadores jurídicos, lo cual deviene claramente insuficiente cuando hablamos de derechos fundamentales.

IV. EL VALOR DEL CONSENTIMIENTO EN LA TRANSFORMACIÓN DEL CONTEXTO.

El consentimiento, así pues, se erige como manifestación formal de la autonomía de la voluntad y constituye la base legitimadora del tratamiento de datos personales en los términos arriba expuestos. Sin embargo, es lógico pensar que el cambio de paradigma económico y la transformación social y cultural que ha acontecido recientemente y que queda patente en fenómenos como la datificación o la automatización del procesamiento antes esbozados, ha infligido algunos cambios en la conceptualización del consentimiento.

Para ello, a continuación se examinan algunos fenómenos recientes que han tenido un notable impacto en materia contractual y de consumo, con el objeto de verificar si también producen alteraciones en la dogmática clásica del consentimiento y si, de haberlas, invalidan por sí mismas el modelo existente.

técnicamente. En estos mecanismos se incluirán su diseño y datos de entrenamiento, y abordarán su potencial impacto discriminatorio. Para lograr este fin, se promoverá la realización de evaluaciones de impacto que determinen el posible sesgo discriminatorio" (art.23).

40 Entre otros, la Declaración dispone que "Toda persona debería estar empoderada para beneficiarse de las ventajas de los sistemas algorítmicos y de inteligencia artificial, especialmente a fin de tomar sus propias decisiones en el entorno digital con conocimiento de causa, así como estar protegida frente a los riesgos y daños a su salud, su seguridad y sus derechos fundamentales" (9°) y "Toda persona debería poder elegir de manera efectiva y libre qué servicios digitales utiliza sobre la base de información objetiva, transparente, fácilmente accesible y fiable" (11°).

1. La teoría de los contratos en la economía digital.

El Ordenamiento jurídico dota de eficacia vinculante a ciertas reglas creadas por los individuales en el ejercicio de su autonomía privada, por lo que se les reconoce fuerza obligatoria y eficacia legal[41]. Ahí es donde reside la trascendencia del consentimiento y la autonomía de la voluntad, pues establece los presupuestos para que ciertas realidades sean dispositivas para los sujetos que, en el ejercicio de su libertad contractual y a través de la autonomía privada, pueden autorregular sus relaciones jurídicas (y consecuencias jurídicas)[42].

Por ello es tan importante que la autonomía individual aparezca exteriorizada por una voluntad para obligarse, que sea libre y no venga impuesta ni condicionada por otros, así como que exista una igualdad entre quienes suscriben tal pacto pues, de lo contrario, se invalidaría la misma. Dado que la libertad personal es el fundamento de la autonomía individual, esta potestad presupone la igualdad de las partes al negociar, estipulando libremente los términos y efectos de sus obligaciones jurídicas, sin necesidad de otras interferencias legislativas.

En primer lugar, ello nos obliga a preguntarnos si, en el contexto arriba descrito, existe una igualdad entre actores o si, por el contrario, nos encontramos ante una situación de desequilibrio entre los ciudadanos –usuarios, si se prefiere en este contexto– y las corporaciones de Big data, los propietarios de dominios web o los encargados del tratamiento de datos personales; cuestión que más tarde se abordará. Así, si se constata la posición dominante en el Mercado de ciertas compañías tecnológicas, no se darían las condiciones efectivas para la igualdad real, al quedar patente el "desequilibro claro entre el interesado y el responsable del tratamiento" y, con ello, no se producirían las condiciones para que el consentimiento fuese libre, de conformidad con la propia normativa de protección de datos[43].

En segundo lugar, conviene señalar que existen ciertas cortapisas al ejercicio pleno de la autonomía de la voluntad, en determinados supuestos y circunstancias, basados en el ejercicio efectivo de los derechos y libertades y que constituyen las fronteras del Derecho, traspasadas las cuales no se reconocerá el ejercicio legítimo del mismo[44]. Así, aunque se pueda renunciar a determinadas facultades

41 En efecto, el artículo 1.091 del Código civil establece que "las obligaciones que nacen de los contratos tienen fuerza de ley entre las partes contratantes y deben cumplirse a tenor de los mismos" pues, si bien la principal fuente de obligaciones es la Ley, los contratos también lo son en la medida que ésta autoriza a las personas llevar a cabo negocios jurídicos a través de los contratos.

42 Ello viene justificado por el contexto histórico en el que tenían lugar tradicionalmente las negociaciones inter partes que, a priori y debido al tipo de intercambios de bienes y servicios, se sustentaban en una economía individualizada

43 Considerando 43 del RGPD.

44 Estas limitaciones, hibridan entre el carácter intrínseco de las mismas, como son la Ley, la moral y el orden público, límites por antonomasia de la libertad contractual –al amparo del artículo 1.255 CC–; y los límites

o actuaciones, hay derechos enteramente irrenunciables –como ocurre con la mayoría de los derechos de la personalidad–, en cuyo caso las cortapisas a la autonomía privada son mucho mayores.

En tercer lugar, siguiendo la tesis de la "unmittelbare Drittwirkung", el ejercicio de la autonomía de la voluntad debe ponerse en relación con el contexto histórico y constitucional y las circunstancias concretas de orden socio-económico en el que se desarrollan las relaciones jurídico privadas, es decir, el negocio jurídico debe concebirse al albur de un determinado estado de cosas. Como señala Bercovitz, incluso en el ámbito estricto de las relaciones privadas, interviene el límite del principio de igualdad, puesto que el mismo adquiere la dimensión de orden público en aquellos casos en los que dicha actividad ostenta trascendencia pública o social, lo cual, en el contexto arriba descrito deviene incontestable[45].

Bajo esta premisa, y teniendo en cuenta que la contratación es un elemento ordenador y que el contexto socio-económico, como se verá a continuación, interviene decisivamente en la conformación de la voluntad, las cortapisas a la autonomía privada vienen justificadas, para que ésta se efectúe en su máxima extensión, evitando abusos o lucros indebidos a particulares, precisamente, porque la libertad contractual tiene su fundamento en propia configuración de un Estado social y democrático de Derecho[46].

2. La contratación en la posmoderna sociedad de consumo.

La teoría clásica de formación de los contratos, arriba descrito, se fundamentaba en el consentimiento libre y autónomo entre dos o más partes perfectamente identificadas, las cuales participaban colaborativamente en la confección del contrato. Sin embargo, en la actualidad, la libertad contractual viene fuertemente restringida por la proliferación de la contratación en masa, a distancia, las condiciones generales de la contratación o las cláusulas de adhesión; constriñendo hasta su mínima expresión la negociación inter partes y, en consecuencia, el contenido de la autonomía privada.

Así, la lógica contractual tradicional basada en la idea de que las relaciones privadas quedan sometidas a la iniciativa particular ha sido sacudida por los cambios en el modelo económico y en las pautas sociales de interrelación, en lo

extrínsecos, en tanto que todo negocio jurídico surge al albur de un contexto legal preexistente que le da virtualidad jurídica, que lo completa y al cual supedita su vigencia.

45 Bercovitz Rodríguez-Cano, R.: "Principio de igualdad y Derecho privado", *Anuario de Derecho Civil*, 1990, vol. 43, núm. 2º, p. 416.

46 Como señala Ferrajoli, "el garantismo opera como doctrina jurídica de legitimación y sobre todo de deslegitimación interna" por lo que el autor defiende la subordinación de la legitimidad del ordenamiento jurídico al aseguramiento de las condiciones efectivas de disfrute de los derechos fundamentales. Ferrajoli, L.: *Derecho y razón. Teoría del garantismo penal*, Trotta, Madrid, 2009, p. 852.

que Díez Picazo ha definido como "la transformación de la teoría contractual"[47]. Y es que, la realidad actual de la contratación responde a las necesidades de la sociedad de consumo y se formaliza en contratos en serie –sin negociación inter partes–, constituyendo en su mayoría, un clausulado de adhesión[48], desprendiendo al contrato del carácter dispositivo que se le presume en abstracto.

Ello comporta, en lo que aquí nos interesa, una asimetría en las relaciones jurídicas en tanto que se despersonaliza a los proveedores de productos y servicios, quienes ostentan una posición dominante, y la negociación en la contratación viene sustituida por contratos de adhesión con cláusulas predispuestas y condiciones generales de contratación, en aras de abaratar los costes de transacción. La autonomía de la voluntad, además, plantea retos adicionales en las relaciones jurídicas formalizadas por medios telemáticos o automáticos, teniendo en cuenta el incremento exponencial de la contratación online donde las partes intervinientes ni se detienen a negociar ni muchas veces a revisar el propio contenido del contrato electrónico, a menudo sometido a la inmediatez.

Estos cambios en la contratación suponen una restricción de los derechos comprendidos bajo el principio de autonomía de la voluntad y tienen aparejados posibles riesgos de lesionar intereses jurídicos o menoscabar garantías legales en términos de igualdad entre las partes, información precontractual o cláusulas transparentes y, en última instancia, de seguridad jurídica. Por ello, ante la asimetría constatada entre contratantes, donde los consumidores ostentan una posición en el tráfico jurídico de desigualdad frente a empresarios o profesionales y merecen un mecanismo corrector, surge, bajo el Derecho de consumo, una protección específica para las nuevas relaciones jurídicas que nacen, destacando: el deber de información, el principio de transparencia, la vinculación jurídica de las declaraciones publicitarias, la atribución legal del derecho de desistimiento del consumidor, la nulidad de las cláusulas abusivas, etc. Todo ello con el objeto de salvaguardar la autonomía privada y el libre albedrío de los sujetos en el ámbito contractual[49].

47 Díez Picazo, L. & Ponce De León, L.: "La autonomía privada en la nueva Ley de Arrendamientos Urbanos", *Anuario de Derecho Civil*, 1956, p. 1551.

48 Así, la parte adherente sólo puede manifestar su voluntad o no de formalizar dicho negocio jurídico (libertad de contratar) pero no de discutir o determinar su contenido (libertad contractual) en tanto que es la predisponente la que unilateralmente elabora el contenido del contrato.

49 García Vicente señala muy bien cuál es el propósito de la legislación especial de protección de consumidores, en lo que a sus relaciones contractuales atañe: "procurar la libertad y conciencia del consumidor, su libertad contractual, esto es, que se halle libre de coacciones, seducciones, engaños o errores y razonablemente informado sobre las diversas circunstancias y elementos que influyen típicamente en la decisión de contratar. Pero tal libertad y consciencia no se ciñe sólo al tiempo de contratar, sino que abarca, igualmente, el cumplimiento o ejecución del contrato, así como sus eventuales modificaciones". García Vicente, J.R.: "La contratación con consumidores", en AA.VV.: *Tratado de contratos* (dir. por Bercovitz Rodríguez-Cano), Tirant lo Blanch, València, 2022, p. 1842.

La nueva coyuntura económica y tecnológica supone una vuelta de tuerca para la dogmática clásica en materia de obligaciones y contratos, pues las corporaciones de Big data, posicionadas en una clara situación de oligopolio, tienen un poder absoluto en el Mercado y condicionan a los usuarios a quienes imponen sus condiciones contractuales, por lo general abusivas –piénsese, por ejemplo, en las políticas de privacidad "take it or leave it"–. Por otra parte, cabe examinar el valor del consentimiento, como materialización de la autonomía privada, en este nuevo estado de cosas, lo que lleva a preguntarse, por ejemplo, qué grado de diligencia puede exigírsele al contratante en el entorno online, en función de sus conocimientos tecnológicos previos[50].

Con todo, surge preocupación, entre otras muchas cuestiones, por la reducción de la esfera del principio de autonomía privada en el sentido de determinar como de autónoma es esa voluntad individual, debiendo reflexionar acerca de las injerencias o limitaciones en la autonomía privada y, en consecuencia, el valor efectivo del consentimiento.

3. ¿Nos sirve ahora la doctrina clásica del consentimiento?

Como se ha expuesto arriba, partimos de la base de que la autonomía de la voluntad es el presupuesto indispensable para llevar a cabo negocios jurídicos y, por tanto, el consentimiento de una persona es el elemento sobre el que pivota la eficacia de los actos con trascendencia jurídica, las obligaciones contraídas y los contratos de los que forme parte. Para ello, deben darse condiciones de igualdad –partiendo de una posición jurídica equivalente–, y libertad material, en tanto que, como ya se ha expuesto, la libertad personal es el fundamento de la autonomía individual. Cabría preguntarse pues, si el consentimiento puede tener límites difusos o, al menos, si en el contexto arriba descrito, puede reconocérsele a la autonomía de la voluntad, cierto margen de ambigüedad y, en consecuencia, si ello afecta a su valor como mecanismo legitimador, desde el punto de vista jurídico.

El consentimiento viene ligado desde el Derecho romano a la figura del contrato y, como se acaba de exponer, la teoría clásica de formación del contrato, aún vigente, presupone la igualdad entre partes para formalizar relaciones civiles libremente. Es por eso que, teniendo en cuenta las circunstancias actuales, esta

50 El Tribunal Supremo dispuso a este respecto, en su STS 14 junio 2021 (RAJ 2021, 839) que dentro del consumidor digital cabe hablar de diversas categorías, atendiendo al grado de conocimiento de las nuevas tecnologías, lo que deviene clave en materia de información precontractual pues, el Alto Tribunal estima que "aun encontrándose las condiciones generales publicadas en internet (como también exige el art. 12.1, segundo párrafo de la Carta de derechos del usuario de los servicios de comunicaciones electrónicas) o informándose de las mismas por teléfono en el momento de la contratación, pueden existir usuarios que carezcan de medios o habilidad para acceder a tales condiciones publicadas de manera telemática o para comprender de manera adecuada las condiciones explicadas por teléfono, por ello, para garantizar también sus derechos, se contempla que puedan solicitar la remisión de las condiciones generales de contratación por escrito y han de serles entregadas antes de contratar, pues solo así se garantiza que pueda celebrar el contrato con pleno conocimiento de las condiciones que lo rigen" [FJ 3º].

doctrina del consentimiento adopta también un cariz antagónico porque, al ignorar las estructuras de desigualdad vigentes, las relaciones de dominio o el poder de condicionamiento de la parte predisponente sobre el titular de los datos se invalida el valor del consentimiento como garantía del ejercicio autónomo de la voluntad privada. Y es que, aunque el consentimiento sea en abstracto libre, viene preconfigurado por una serie de elementos condicionantes que no pueden ignorarse, pues desconocer u ocultar los patrones estructurales puede llevar a presentar como una decisión libre algo que, en realidad, es una preferencia adaptativa o una decisión marcada por un estado de necesidad que invalida la presunción de consentir de manera libre e informada[51].

Por otra parte, también desde una perspectiva civilista, hay que remarcar que, asimismo, los contratos que dan lugar a la casuística arriba expuesta, operan con reglas nuevas que muchas veces resultan ajenas a la propia dogmática contractual en tanto que, por ejemplo, permiten disponer de ciertos derechos fundamentales involucrados –recordemos, de nuevo, que el derecho a la protección de datos ha sido reconocido como un derecho fundamental y autónomo[52]– o admiten la posibilidad de revocar el consentimiento prestado en un contrato sinalagmático. Como ejemplo, los contratos sobre contenidos o servicios digitales donde suele exigirse la cesión de datos personales del usuario por parte de los prestadores de un servicio a cambio del mismo, abarcando el intercambio de información, no sólo en el momento de celebración del contrato, sino que dicho suministro de información personal abarca la entera ejecución del contrato. Si bien a este respecto, el art. 6.1 c) del RGPD exige que se produzca una separación clara entre el consentimiento necesario para la perfección del contrato y el consentimiento que legitima el tratamiento de datos personales, lo cierto es que deviene sumamente difícil deslindar tales circunstancias, más aún, si tenemos en cuenta las engorrosas políticas de privacidad –sin entrar, como luego haremos, en la lectura y comprensión asertiva de las mismas–, en las que quedan subsumidas tales circunstancias así como la información preceptiva para la obtención del consentimiento informado.

Asimismo, en esta tipología de contractual, el contrato no es la causa que legitima el tratamiento de los datos personales en el sentido del art. 6.1 c) del RGPD, en tanto que la persona consumidora accede a la cesión de datos que en nada afectan ni se exigen para el cumplimiento de dicho contrato. Como señala Martínez Velencoso, en estos casos existe un evidente solapamiento entre la normativa de protección de datos personales, en la esfera de la protección de los

51 Barrère, M.A. & Morondo, D.: "Subordinación y discriminación interseccional: elementos para una teoría del derecho antidiscriminatorio", *Anales Cátedra Francisco Suárez*, 45, 2011, p. 145.

52 STS 30 de noviembre (RAJ 2000, 292).

derechos fundamentales, y la normativa de protección de consumidores[53], que reconoce y atiende al valor económico de los datos. Y, sobre esta premisa, resulta del todo dudoso que, en la esfera de los derechos de la personalidad, el titular de un derecho sobre su información personal, pueda transmitirlo en su totalidad incluso en su completa titularidad, debido a los límites dispositivos intrínsecos a dicha categoría de derechos fundamentales[54].

En definitiva, la transformación cualitativa de los esquemas teóricos del contrato por negociación es incontestable, por lo que el valor del consentimiento, en tanto que autonomía de la voluntad, ya no responde a las nuevas relaciones contractuales ni tampoco a las necesidades del nuevo estado de cosas, siendo necesario repensar el marco jurídico regulador, de conformidad con la función adaptativa del Derecho y su vocación de acabar con las desigualdades más profundas[55]. De lo contrario, nos aferraríamos a una doblez contradictoria y paradójica acerca del consentimiento que, al mismo tiempo que se asienta sobre la convicción de que es el mecanismo indispensable para validar cualquier ejercicio de autonomía privada, se sabe en peligro por la nueva coyuntura digital, motivo por el cual se vienen introduciendo reformas legislativas encaminadas a lograr una transparencia referencial que mine la abusividad y oscuridad a la que viene sucumbido y que, de facto, reconocen su inoperancia o funcionamiento anormal. Porque, no habiendo libertad real para el ejercicio de la autonomía privada, en lugar de "prestar" el consentimiento, se estaría "cediendo" el mismo. Del mismo modo que, sobreviniendo una situación de subordinación y condicionamiento del titular de los datos personales frente a las TECH tecnologies, en lugar de ser un acto libre, el mismo se convertiría en forzoso.

Por otra parte, conviene interrogarse acerca del interés que pueda tener esta parte predisponente en la vigencia actual del modelo de consentimiento en tanto que, desde esta óptica, la exigencia del consentimiento puede resultar perniciosa pues, al poner la regulación el foco en el consentimiento de la persona interesada, se instala en ella la responsabilidad, individualizando la culpa. Es decir, el responsable del tratamiento, quedará exonerado de cualquier sospecha cuando demuestre que formalmente ha dado cumplimiento a los estándares exigidos por

53 Se añade, asimismo, la interacción de la Directiva (UE) 2019/770 del Parlamento Europeo y del Consejo de 20 de mayo de 2019 relativa a determinados aspectos de los contratos de suministro de contenidos y servicios digitales.

54 Martínez Velencoso, L.M.: "El impacto del big data y el Internet de la cosas en la normativa de protección de datos", en AA.VV.: *Retos normativos del mercado único digital europeo* (coord. por Martínez Velencoso), Tirant lo Blanch, València, 2022, p. 293.

55 Así lo justificaba De Castro cuando decía que "es misión de los juristas el enfrentarse con la realidad económico-social y la necesidad de valorar esa realidad con criterios de justicia" y como sobre ellos pese la obligación de velar para que las circunstancias del momento no nos hagan olvidar que "lo jurídico pierde esta condición al apartarse de la Justicia" cuando se configura una realidad social como instrumento de opresión y causa de desigualdad jurídica para los contratantes, pudiendo se producir una desconexión entre la ley positiva y la justicia. De Castro Y Bravo, F.: "Las condiciones generales de los contratos y la eficacia de las leyes", *Anuario de Derecho Civil*, 1961, p. 8.

la normativa, sin que ello, muchas veces, comporte una actuación lícita, real y transparente[56]. De este modo, el hecho de consentir viene oscurecido de manera constante por las circunstancias en las que tiene lugar, las cuales dejan muy poco margen para oponerse, introducir matices o conocer realmente las implicaciones de lo consentido. Así, resulta pertinente cuestionar la autonomía de esta voluntad materializada en forma de consentimiento, pues consentir sin saber, permite poner en duda la voluntad manifestada, que no es informada ni debería ser válida, en tanto que carece de la libertad material necesaria, condicionada por la desigualdad estructural y la innegable correlación de fuerzas.

Así las cosas, evidenciamos como las diversas aristas de la coyuntura actual deterioran el modelo clásico del consentimiento que, aplicado a la realidad vigente, pervierte su significado y garantías hasta hacerlo, incluso en algunas ocasiones, inválido por completo. Por ello, deviene imprescindible repensar los mecanismos jurídicos para adaptarlos al estado de cosas, con el objeto de preservar las garantías de autonomía y libertad que deben venir acompañando al ejercicio de la autonomía de la voluntad. Con dicho propósito, continuación se exponen algunas claves sobre las que convendría reflexionar a la hora de adaptar el modelo jurídico al marco existente.

V. CLAVES PARA REPENSAR EL CONTEXTO NORMATIVO.

Teniendo en cuenta lo anterior, queda patente la existencia de disfunciones en el modelo de formación de la autonomía de la voluntad, de prestación del consentimiento y de celebración de contratos en determinadas circunstancias del consumo digital, con especial riesgo para la protección de los datos personales y el libre albedrío de sus titulares. En consecuencia, el marco regulador debe hacer frente a la realidad imperante y disponer mecanismos que garanticen la protección de intereses jurídicos, derechos y libertades de los individuos, en plena consonancia con las circunstancias concomitantes de la nueva economía digital, pese a que ello suponga alterar la doctrina clásica del consentimiento, precisamente, con el objeto de preservar su autonomía y libertad.

Para ello, debe partirse de la existencia de un cambio de escenario respecto de los datos personales, que han pasado de ser subproductos de los fines para los que fueron recopilados –es decir, consecuencias inherentes a la contratación de ciertos productos o servicios–, a constituir los productos en sí mismos, con

56 Así, la denominada "accountability" o responsabilidad proactiva, exige a los responsables del tratamiento poner en conocimiento de las personas interesadas, de forma clara, sencilla y comprensible –extendiéndose todas las garantías exigibles al consentimiento informado– las finalidades, técnicas y usos a los que van a destinar sus datos así como las garantías a los que van a quedar sometidos. Sin embargo, teniendo en cuenta los factores antes examinados, y aunque se sobrentiende que todo ello debe hacerse con la debida transparencia, no queda asegurado el cumplimiento de todos los estándares garantistas.

las consecuencias que de ello se derivan para la finalidad de tratamiento y el desarrollo y uso posterior de tal información. En este sentido, la transformación del modelo es innegable, pues si bien en un inicio, el almacenamiento de la información era consustancial a la contratación o prestación de ciertos servicios, en la actualidad, el almacenamiento de datos constituye un fin en sí mismo, sin que pueda conocerse apriorísticamente el uso o procesamiento posterior al que se someterán los mismos.

Tampoco se generan en muchos casos las condiciones idóneas para que el consentimiento sea libre, requisito indispensable para su licitud, como ya se ha visto. En este sentido suscitan dudas, desde la propia conformación de la voluntad y sus vicios –en la medida en la que el modelo actual merma la capacidad electiva de los usuarios, que vienen orientados en sus conductas de consumo–, la capacidad de coaccionar o condicionar sobremanera al usuario para obtener su consentimiento hasta el punto de privarle de capacidad real para oponerse o retirarlo –al menos, no sin perjuicio–, o la formalización de aquellos contratos mediante los cuales los titulares se comprometen a ceder sus datos personales a modo de contraprestación de un servicio –lo que deviene cuestionable a tenor del art. 7.4 RGPD–.

En relación con lo anterior, no puede perderse de vista la asimetría informativa y el desequilibrio que, en este sentido, surge entre las partes contratantes. Incluso en aquellos casos en los que la información previa sea debidamente prestada –sin incurrir en patrones oscuros, cláusulas abusivas ni políticas de privacidad intrincadas–, las cuestiones técnicas y las políticas de tratamiento son tan complejas y están sujetas a tantas imprecisiones que, leyéndolas detenidamente puede que el interesado no acabe de comprender enteramente sus pormenores –piénsese, por ejemplo, en la falta de transparencia algorítmica o del funcionamiento de la IA– y, pese a ello, se acepten dichas cláusulas predispuestas en tanto que ello es preceptivo para llegar a disfrutar de un determinado bien o servicio. Es más, la prestación del consentimiento se ha convertido en un acto mecánico para el acceso a ciertos bienes o servicios, desvirtuando su asertividad y las implicaciones que deberían desplegarse de un consentimiento verdaderamente informado. En consecuencia, ni el cumplimiento formal del deber de información por parte del responsable del tratamiento a través de la política de privacidad ni la aceptación del titular de los datos de la misma, resultan garantes de la presencia de un consentimiento informado y libre, en los términos legales aquí examinados.

A todo lo anterior debe sumársele la datificación social a la que hacíamos referencia al inicio que, en la práctica, implica la existencia de datos observados, derivados o incluso inferidos, generados al margen de la voluntad de la persona afectada y con su total desconocimiento, lo que deviene sumamente cuestionable

en términos de consentimiento, transparencia y licitud. Dejando al margen la posición de dominio y el poder de condicionamiento de las TECH companies, sus meras dinámicas de funcionamiento hacen muy difícil –si no imposible– ser conscientes de qué datos se tienen sobre nosotros, por quienes, cuáles de estos datos son tangibles y cuáles se han inferido, en qué categorías se han clasificados, etc. Y, en consecuencia, desconociendo lo anterior no podemos hacer valer los derechos de rectificar, borrar, bloquear u oponernos a su uso, cesión, reutilización o a ser objeto de tratamiento automatizado. Es imposible ejercitar derechos que tenemos reconocidos si no se dan las garantías para obtener la información previa que sirva de presupuesto para accionarlos. Así, por ejemplo, el RGPD habilita a los individuos a conocer la existencia de decisiones automatizadas, incluida la elaboración de perfiles y a conocer la lógica aplicada en dicho tratamiento (art. 13.2 f)), sin embargo, si como hemos visto anteriormente nos encontramos con lógicas algorítmicas de autoaprendizaje (machine learning), en la práctica, el ejercicio de tal potestad deviene irrealizable o estéril incluso para el responsable de tratamiento –cuestión aparte sería el nivel de transparencia que debe tener dicha explicación la para lograr una comprensión integral por parte de la persona interesada–.

Al hilo de lo anterior, debería asimismo reflexionarse sobre el rol de la persona afectada para la protección de sus derechos e intereses pues, ante un incumplimiento de la normativa arriba expuesta, es ella quien debe ejercitar proactivamente los mismos para lograr su protección y reparación. Además de los conocimientos técnicos y la dedicación personal que se le pueda exigir, ello consagra una lógica radicalmente diferente a la propia del Estado de Derecho –piénsese, por ejemplo, en materia de libertades expresivas–, dejando un gran poder de iniciativa a la ciudadanía sobre sus datos personales, siendo poco deseable en una democracia constitucional que se transfiera la responsabilidad de la protección de los derechos fundamentales a las propias personas interesadas –usuarios, además, de productos y servicios que no vienen preconfigurados de modo garantista–.

Teniendo lo anterior presente, así como otros fenómenos correlativos como la imposibilidad de lograr una trazabilidad real de determinados algoritmos de machine learning o la pasividad de la ciudadanía frente a la pérdida progresiva de su privacidad deben buscarse mecanismos capaces de aplacar los riesgos existentes y afrontar la realidad con mayor seguridad jurídica. Es decir, hay que implementar medidas que apliquen, desde el origen, las garantías legales y el respeto a la ética en el uso de los datos, como puede ser el "legal-tech" o la "privacy by design" para que, de forma generalizada, todo el engranaje funcione de forma transparente, permitiendo a los interesados un control completo sobre sus datos personales y asegurando la supervivencia de las libertades colectivas e individuales. Se trata, en definitiva, de originar apriorísticamente una cultura de protección de datos y

prohibición de discriminaciones de forma que los principios éticos y legales queden implementados no sólo en la forma en la que vienen almacenados y tratados los datos, sino también en la lógica empresarial, en los códigos de software y en la propia economía de Mercado, previniendo un uso pernicioso de la tecnología y una paulatina pérdida de garantías a medida en que los datos van cambiando de mano y van destinándose a usos secundarios.

A la luz de lo expuesto, sobran los motivos para reclamar medidas legislativas decididas, que actúen como imperativos extrínsecos al negocio contractual en pro de equilibrar la igualdad inter partes, garantizando el principio de transparencia y la autonomía de la voluntad, reafirmando el valor del consentimiento, como mecanismo legitimador de la potestad concedida por el habeas data, y materializando la libertad contractual en su máxima extensión. Así, desde el punto de vista de la dogmática contractual, se exige un cambio de modelo a la hora de contratar de forma que las cláusulas contractuales, además de los intereses particulares del predisponente, tengan en cuenta la realización de otros bienes o intereses generales del orden público, como son la protección o tutela de la parte contractual más débil y la calidad y competencia de la contratación bajo condiciones generales.

No debe olvidarse que la autonomía privada es un valor jurídico que constituye la base del propio Estado social y democrático de Derecho, debido al doble carácter de los derechos fundamentales, en tanto que derechos subjetivos y valores objetivos del orden constitucional[57]. Así, desde un punto de vista integral, este principio de transparencia actuaría como eje vertebrador de la sociedad democrática, en estrecha conexión con el principio de legalidad y seguridad jurídica, en la medida en que dichos conceptos actúan como catalizadores del ideal democrático, junto con la idea de la "accountability", en un sentido de responsabilidad o rendición de cuentas, posibilitando una forma de control social frente a las extralimitaciones en las que pueden incurrir quienes ostentan una posición de dominio, limitando las prácticas de dudosa legalidad e incrementando la legitimidad social, máxime cuando nos encontramos en el ámbito de los derechos fundamentales[58].

57 Los derechos fundamentales son "elementos esenciales de un ordenamiento objetivo de la comunidad nacional, en cuanto ésta se configura como marco de una convivencia humana justa y pacífica, plasmada históricamente en el Estado de Derecho y, más tarde, en el Estado Social y Democrático de Derecho, según la fórmula de nuestra Constitución", STC 25/1981, de 14 de julio (RTC 1981, 25).

58 Orduña Moreno dispone que "la transparencia, junto con el equilibrio de las prestaciones, se ha erigido como un principio jurídico del control social establecido" y defiende la necesidad de extender dicho principio jurídico a todo contratante –ya sea consumidor o no– que, como adherente, tenga que recurrir a este modo de contratar bajo condiciones generales, sin posibilidad real de negociación y con una clara posición de inferioridad y asimetría en dicha relación jurídica. Orduña Moreno, F.J. & Sánchez Martín, C.: *La transparencia como valor del cambio social: su alcance constitucional y normativo. Concreción técnica de la figura y doctrina jurisprudencial aplicable en el ámbito de la contratación*, Aranzadi, Navarra, 2018, p. 37.

VI. CONCLUSIONES.

La situación actual, y su evolución anterior al albur de la digitalización, evidencian un cambio substancial en las dinámicas de producción y consumo hasta el punto de impregnar al conjunto político, económico, social y cultural, en lo que ha sido descrito como una "sociedad de consumidores". En este proceso de transformación, ha tenido un papel esencial el almacenamiento y tratamiento masivo de datos personales, erigiendo a los individuos, además de en sujetos destinatarios finales, en bienes de cambio –es decir, en productos en sí mismos–.

En este sentido, hemos asistido a una paulatina datificación social, esto es, una digitalización masiva de la toda aquella información que una persona puede generar –información real pero también deducible y predecible–, convirtiéndola en datos tangibles y rastreables, con el objeto de clasificarla, almacenarla o tratarla. Este proceso, ha venido coadyuvado por su automatización y el cálculo algorítmico, fundamental para la explotación a gran escala todo este volumen de datos, los cuales llevan aparejados riesgos serios de estratificación social, hegemonización, discriminación o vulneración de derechos y libertades.

Se constata, pues, un escenario de insaciabilidad exponencial de información personal, con fines mercantilistas legítimos, pero a través de procesos que siembran dudas sobre la pervivencia de ciertas garantías jurídicas. En concreto, al aplicar las lógicas normativas tradicionales al nuevo estado de cosas, se cuestiona su impacto en la dogmática clásica de los contratos, en concreto, sobre la afectación que ello podría tener para la autonomía de la voluntad, en un sentido amplio: sobre la extensión de la formación de necesidades, la libertad de elección, la igualdad material inter partes, etc.

Se pone en entredicho el valor del consentimiento como catalizador de la autonomía privada debido, principalmente, al desequilibrio inter partes, como se observa en la posición de dominio de las TECH tecnologies en el Mercado, su capacidad de condicionamiento en los usuarios o la predisposición de las cláusulas de adhesión de los contratos seriados. Si bien la desigualdad de poder entre las partes no tiene por qué invalidar el consentimiento prestado en todos los casos, lo cierto es que sí le da un contexto que lo pone bajo sospecha. Es decir, si en las circunstancias concomitantes, la autonomía privada, queda prácticamente reducida a la libertad de contratar o no, entonces la dogmática clásica del consentimiento debe rechazarse en tanto que deviene estéril a la realidad social, privatizando responsabilidades al dejar fuera a las dinámicas de poder. La lógica tradicional, basada en la idea de que las relaciones privadas dependen de la iniciativa particular, no puede aplicarse al marco actual, supeditado a relaciones asimétricas de dominio, estructuras de desigualdad y una falta de libertad material, lo que invalida el valor del consentimiento como garantía del ejercicio autónomo de la voluntad privada.

Es aquí cuando debemos cuestionar el modelo –de un modo global, más allá de lo puramente legal– y, en consecuencia, ello nos lleva a problematizar el consentimiento y reconocer sus limitaciones, en tanto que no sirve para abordar el fenómeno de forma integral ni con perspectiva crítica, por el contrario, su pervivencia sin reconvención alguna aboca al mantenimiento del orden hegemónico, resultando las personas adherentes, usuarias e interesadas, las mayores perjudicadas.

Así, la solución no pasa por recabar el consentimiento de toda persona interesada con el fin de demostrar que la autonomía de la voluntad ha tenido lugar en dicha transacción de un modo formal, sino de garantizar las condiciones materiales para que esa libertad de elección sea real. El consentimiento es un concepto complejo y paradójico y aun así irrenunciable, no es la única solución al problema porque, según se mire, puede instrumentalizarse para legitimar actuaciones desleales, convirtiéndose en una treta que deberíamos impugnar.

En este estado de cosas, se hace del todo necesaria una verdadera discusión pública y transparente, no sólo sobre los límites de la mercantilización de la información privada o la aplicación indiscriminada de procesos automatizados o algorítmicos, sino, esencialmente, de aquéllas cuestiones que puedan limitar el libre desarrollo de la personalidad de la ciudadanía, pues los riesgos de legitimar cualquier tipo de decisión basada en una voluntad privada adulterada, nos privan de autonomía y son perceptibles a todos los niveles, en tanto que impregnan el marco político, económico y social.

No se pretende la impugnación completa del modelo, sino su adaptación a la realidad imperante, a las necesidades presentes y futuras, con la finalidad de preservar las garantías de autonomía y libertad que deben acompañar el ejercicio de la voluntad privada. Ello pasa, necesariamente, por la transformación cualitativa de los esquemas teóricos del contrato por negociación, pues muchas relaciones contractuales actuales operan con reglas que escapan a la dogmática clásica, y aplicar medidas obsoletas, sin tener en cuenta el contexto histórico, los procesos sociales y los patrones de dominación y discriminación, podría vulnerar el propio principio de igualdad. Con ello, se busca reafirmar el valor del consentimiento, en tanto que mecanismo de garantía de la libertad contractual, y acabar con situaciones que, o bien pueden legitimar la abusividad u oscuridad, o perpetuar situaciones de desigualad o irresponsabilidad, o bien lesionan directamente derechos y libertades. Y no podemos olvidar que la autonomía privada, en última instancia, es un valor jurídico que constituye la base del propio Estado social y democrático de Derecho.

BIBLIOGRAFÍA

Añón Roig, M.J.: "Desigualdades algorítmicas: conductas de alto riesgo para los derechos humanos", *Derechos y Libertades*, 2022, núm. 47º.

Añón Roig, M.J.: "Transformaciones en el derecho antidiscriminatorio: avances frente a la subordinación", *Revista electrónica del Instituto de Investigaciones Jurídicas y Sociales Ambosio Lucas Gioja*, 2021, núm. 26º.

Bauman, Z.: *Mundo consumo*, Paidós, Barcelona, 2021.

Bauman, Z.: *Modernidad líquida*, Fondo de Cultura Económica, Madrid, 2017.

Barrère, M.A. & Morondo, D.: "Subordinación y discriminación interseccional: elementos para una teoría del derecho antidiscriminatorio", *Anales Cátedra Francisco Suárez*, 45º, 2011.

Bercovitz Rodríguez-Cano, R.: "Principio de igualdad y Derecho privado", *Anuario de Derecho Civil*, 1990, vol. 43, núm. 2º.

Capilla Roncero, F.: "Autonomía de la voluntad y Derecho de la persona o la autonomía personal en el Derecho privado", *Diario La Ley*, 2011, núm. 7685º.

De Castro Y Bravo, F.: "Las condiciones generales de los contratos y la eficacia de las leyes", *Anuario de Derecho Civil*, 1961.

Díez Picazo, L. & Ponce De León, L.: "La autonomía privada en la nueva Ley de Arrendamientos Urbanos", *Anuario de Derecho Civil*, 1956.

Ferrajoli, L.: *Derecho y razón. Teoría del garantismo penal*, Trotta, Madrid, 2009.

Fourcade, M. & Healy, K.: "Classification situations: Life-chances in the neoliberal era", *Accounting, Organizations and Society*, 2013, núm. 38º.

García Vicente, J.R.: "La contratación con consumidores", en AA.VV.: *Tratado de contratos* (dir. por Bercovitz Rodríguez-Cano), Tirant lo Blanch, València, 2022.

Gitelman, L.: *"Raw data" is an oxymoron*, The MIT Press, Cambridge (Massachusetts), 2013.

Gregory, K.: "Big data, like Soylent Green, is made of people", *CUNY*, 2014.

Han, B.: *Psicopolítica*, Herder, Barcelona, 2014.

Lerman, J.: "Big data and its exclusions", *Stanford Law Review,* 2013, núm. 66º.

MARTÍNEZ VELENCOSO, L.M.: "El impacto del big data y el Internet de la cosas en la normativa de protección de datos", en AA.VV.: *Retos normativos del mercado único digital europeo* (coord. por MARTÍNEZ VELENCOSO), Tirant lo Blanch, València, 2022.

MARTÍNEZ VELENCOSO, L.M. & SANCHO LÓPEZ, M.: "El nuevo concepto de onerosidad en el mercado digital, ¿Realmente es gratis la App?", *InDret*, Enero, 2018.

MAYER-SCHÖNBERGER, V. & CUKIER, K.: *Big data. La revolución de los datos masivos*, Turner, Madrid, 2015.

MEJIAS, U. & COULDY, N. "Datificación", *Revista Latinoamericana de Economía y Sociedad Digital*, Julio, 2022.

MONASTERIO ASTOBIZA, A.: "*Ética algorítmica: implicaciones éticas de una sociedad cada vez más gobernada por algoritmos*", *Dilemata*, 2018, núm. 24º.

O'NEIL C.: *Armas de destrucción matemática. Cómo el Big data aumenta la desigualdad y amenaza la democracia*, Capitán Swing, Madrid, 2018.

ORDUÑA MORENO, F.J. & SÁNCHEZ MARTÍN, C.: *La transparencia como valor del cambio social: su alcance constitucional y normativo. Concreción técnica de la figura y doctrina jurisprudencial aplicable en el ámbito de la contratación*, Aranzadi, Navarra, 2018.

PÉREZ LUÑO, A.E.: "Principios de la protección de datos: consentimiento del afectado. El consentimiento de los menores", en AA.VV.: *Comentario a la ley Orgánica de Protección de Datos de Carácter Personal* (dir. por TRONCOSO REIGADA), Civitas, València, 2010.

SADOWSKI.: "When data is capital: Datafication, accumulation and extraction", *Big Data & Society*, 2019, vol. 6.

ZUBOFF, S.: *La era del capitalismo de la vigilancia*, Paidós, Barcelona, 2019.

PARTE II:

ALGORITMIZACIÓN DE LA JUSTICIA E INTELIGENCIA ARTIFICIAL

TECNOLOGÍA BIOMÉTRICA Y DATOS BIOMÉTRICOS. BONDADES Y PELIGROS. NO TODO VALE

BIOMETRIC TECHNOLOGY AND BIOMETRIC DATA. BENEFITS AND DANGERS. NOT EVERYTHING IS FAIR

Actualidad Jurídica Iberoamericana Nº 21, agosto 2024, ISSN: 2386-4567, pp. 298-331

Silvia BARONA VILAR

ARTÍCULO RECIBIDO: 29 de mayo de 2023
ARTÍCULO APROBADO: 1 de julio de 2024

RESUMEN: El desarrollo volcánico de la tecnología biométrica y la proliferación de técnicas de tratamiento de datos biométricos genera numerosos dilemas en el mundo jurídico. Los datos biométricos sirven para reconocer a las personas de acuerdo con sus características físicas, fisiológicas y parámetros conductuales y pueden ser explotados, manipulados y empleados para tomar decisiones en el sector privado, público y empresarial. Y no son infalibles, en absoluto. Es importante delimitar normas, fijar condiciones de determinación de su finalidad, de su necesidad y de su proporcionalidad. La investigación ahonda en supuestos que orillean las condiciones de legalidad y de ética y ponen en alerta ante su posible manipulación.

PALABRAS CLAVE: Sistemas biométricos; datos biométricos; protección de datos biométricos.

ABSTRACT: Many dilemmas arise in the legal world as a result of the volcanic development of biometric technology and the proliferation of biometric data processing techniques. Used to identify individuals by their physical, physiological and behavioural characteristics, biometric data can be exploited, manipulated and used to make decisions in the private, public and business sectors. And they are not infallible. It is important to delimit standards, to set conditions for determining their purpose, necessity and proportionality. This research examines in depth and critically the assumptions that circumvent the conditions of legality and ethics and alerts us to their possible manipulation.

KEY WORDS: Biometric systems; biometric data; biometric data protection.

SUMARIO.- I. LA APARICIÓN DE LA BIOMETRÍA COMO SISTEMA AUTOMATIZADO DE RECONOCIMIENTO.- II. LOS DATOS BIOMÉTRICOS.- 1. Noción, usos y aplicaciones.- 2. Tipología de las técnicas biométricas y su incidencia en el mundo jurídico.- *A) Huellas dactilares.- B) Reconocimiento del iris y escáner biométrico de la retina.- C) Geometría del árbol de venas del dedo o de las muñecas.- D) Reconocimiento de firma.- E) Reconocimiento de escritura de teclado o biometría del tecleo.- F) Reconocimiento de voz.- G) Análisis biométrico de movimientos corporales.- H) Reconocimiento biométrico de la palma de la mano.- I) Reconocimiento biométrico de orejas (otograma).- J) Biometría por ADN o huella genética.- K) Reconocimiento facial.*- III. AHORA BIEN...NO TODO VALE.- 1. Punto de partida: Protección jurídica de los datos biométricos.- 2. La teoría nos la sabemos, pero qué sucede en la práctica.- *A) Seguridad frente a la sofisticada criminalidad, derivada de la globalización.- B) Algunos Proyectos nacionales e internacionales en marcha con datos biométricos. Dudas.- C) "Worldcoin", el proyecto de escaneo del iris a cambio de criptomonedas; un negocio redondo a costa de datos biométricos.- D) Utilización biométrica en entradas y salidas empresariales y otros fines laborales.*

I. LA APARICIÓN DE LA BIOMETRÍA COMO SISTEMA AUTOMATIZADO DE RECONOCIMIENTO.

La biometría incluye medidas biológicas o características físicas que se pueden emplear para identificar a las personas, y se incardina en el nuevo paradigma algorítmico en el que vivimos; una sociedad con la hipervaloración de los datos, favoreciendo su obtención y explotación. Esta situación amerita regular la protección de los datos personales. Esta volcánica emergencia, como consecuencia en gran medida de la irrupción del dato como valor, como moneda de cambio, como petróleo del siglo XXI[1], como riqueza a la postre, ha encontrado un desarrollo perfecto en la biometría, al generar información especial, obtenida mediante estudios mensurativos o estadísticos de los fenómenos o procesos biológicos[2], que, aun cuando aplicable a otras especies, nos vamos a centrar en la diversidad de los datos biométricos que pueden extraerse de una sola persona humana.

Datos biométricos que están ofreciendo una multiplicidad de posibilidades de usabilidad, favoreciendo la construcción de la sociedad del control y de la vigilancia[3], especialmente a través de los sistemas de reconocimiento automatizado mediante sistemas biométricos; sistemas que han adquirido una valorización espectacular

1 Esta frase se reitera *como si se tratara de un mantra*, tal como apunta Desireé Jaimovich, en la entrevista con Infobae que realizó a Juan Carlos Gutiérrez, director de IBM Storage para América Latina, https://www.infobae.com/america/tecno/2018/07/13/juan-carlos-gutierrez-los-datos-se-estan-convirtiendo-en-el-nuevo-petroleo-de-las-empresas/.

2 Abs, M.: "Biometrik", en *Historisches Wörterbuch der Philosophie,* online version, (ed. por J. Ritter, J.; K Gründer.; G. Schwabe,), AG Verlag, Basel, 1971, pp. 945-946. Y en el mismo sentido, Real academia española de la lengua, que considera que bajo el término "Biometría" se entiende "el estudio mensurativo o estadístico de los fenómenos o procesos biológicos".

3 Barona Vilar,baroBbb S.: *Algoritmización del derecho y de la justicia: de la Inteligencia Artificial a la Smart Justice*, Tirant lo Blanch, Valencia, 2021, especialmente pp. 235-248.

• Silvia Barona Vilar
Catedrática de Derecho Procesal, Universitat de València.
Correo electrónico: silvia.barona@uv.es

en momentos en que la globalización abrió fronteras, se difuminaron, se permitió flujos de población, la movilidad comercial, personal, laboral, con efectos positivos, pero también negativos.

La irrupción de los sistemas tecnológicos favoreció un nuevo modelo de frontera, exigible ante el flujo humano, económico y laboral, incorporando medios que permitieran garantizar la seguridad nacional e internacional. No debe olvidarse que el modelo de "frontera" como delimitadora geográfica respondía a la fijación de la zona territorial en sentido político y administrativo, integrando cuestiones como soberanía (que incide en lindes, titularidades, propiedades y explotaciones de tierra, agua y aire) y que llevó a que fueran materializadas con un sistema de control especialmente en puertos y aeropuertos, con exigencias de pasaportes y visados o documentos identificatorios, para la entrada y salida del país. Este modelo ha permitido, como apunta Escajedo San Epifanio[4], soluciones frente al crecimiento de manipulaciones (robos y usurpaciones de identidad), de terrorismo internacional, de delincuencia organizada y las amenazas a la salud pública. El interés que despierta esta aparición de la biometría en el mundo jurídico se debe esencialmente al desarrollo que la misma ha propulsado en la aparición de los denominados sistemas automatizados de reconocimiento e identificación de seres humanos.

Se ha venido sosteniendo que el origen de la biometría como ciencia se debe fundamentalmente a Francis Galton[5] (aun considerándose que anteriormente hubo quien empleó este *nomen iuris*), quien, junto a Karl Pearson, fundaron la revista "Biometrika" (su primer número en 1901). En ella confluyen aportes de las matemáticas, estadística, antropología, zoología, botánica, estadística económica, etc.., dirigida a la búsqueda del conocimiento biológico por medios cuantitativos, independientemente de los fines - biomédicos, biocientíficos o de otra naturaleza[6]-. Se creó en 1947 la Sociedad internacional de Biometría, cuyo objetivo ha sido promover el "desarrollo y aplicación de la teoría y los métodos matemáticos y estadísticos a las Biociencias, incluyendo la agricultura, las ciencias biomédicas y la salud pública, la ecología, las ciencias ambientales forestales y disciplinas afines"[7].

Sus desarrollos posteriores han alcanzado al Derecho, siendo aceptadas con fascinación en ciertos sectores y con poca mirada crítica. En el siglo XIX se

4 Escajedo San Epifanio, L.: *Reconocimiento e Identificación de las personas mediante Biometrías estáticas y dinámicas,* Tesis Doctoral, Alicante, diciembre 2015, *open access*, p. 40, quien explica los diversos sistemas de registro de los habitantes y los documentos de identificación que se emitían especialmente a lo largo del siglo XX con la movilidad fronteriza y cómo se ha impulsado el sistema automatizado de reconocimiento biométrico en estos últimos tiempos, en gran medida favorecidos por el crecimiento poblacional y la movilidad.

5 Galton, F.: " Spirit of Biometrika", editorial del número primero de la Revista *Biometrika*, 1901.

6 Stigler, S.M.: "The Problematic Unity of Biometrics", Revista *Biometrics*, 2000, p. 654.

7 http://www.biometricsociety.org/about/

vinculó la biometría con las características psíquicas de las personas, el carácter y la capacidad con el cerebro (craneoscopia o frenología), con determinaciones referidas a las facultades mentales y morales derivadas de la estructura del cráneo. Fundamentaron las teorías de Lombroso, que fueron seguidas por Garofalo y Ferri, acerca de la vinculación de la delincuencia con los rasgos biológicos y psíquicos[8], esto es, considerando que el delincuente nace como tal, no se hace, de modo que defendían el determinismo biológico criminal. Posición doctrinal afortunadamente superada, pero que permitió su manipulación por gobiernos totalitarios para fundamentar crímenes contra la humanidad.

En la actualidad la biometría se vincula a los sistemas automatizados de identificación -entendida como el proceso de reconocimiento de un individuo particular entre un grupo- y autenticación -el proceso de probar que es cierta la identidad reclamada por el individuo-[9]. Estos sistemas pueden servir para identificar colectividades, en atención a rasgos identitarios de grupos, o referirse tan solo a datos biométricos de personas individualmente consideradas, siendo esta última la que ha impulsado especialmente los desarrollos biométricos informáticos, desde los que se trabaja con los datos almacenados en soporte informático para ofrecer respuestas de reconocimiento e identificación individual.

II. LOS DATOS BIOMÉTRICOS.

Los datos biométricos en la actualidad se utilizan en procedimientos automatizados de autenticación, comprobación e identificación. Inicialmente, el uso de la biometría se limitó al ADN y a la comprobación de las huellas digitales, especialmente en materia criminal, con una enorme incidencia en la investigación (penal y civil) y en la prueba. La proliferación de adquisición de estos datos ha emergido, ante una suerte de inconsciencia acrítica inicial en torno a los riesgos que supone la conservación de los datos ante la ausencia de protección jurídica de su tratamiento. En las últimas décadas se ha impulsado la legislacion para la protección de datos biométricos, nacional y supranacionalmente.

1. Noción, usos y aplicaciones.

Los datos biométricos sirven para reconocer a las personas de acuerdo con sus características físicas, fisiológicas o parámetros conductuales[10]. Estos datos

8 Garófalo, R.: *La criminología. Estudio sobre el delito y sobre la teoría de la represión,* Analecta editorial, 1900, pp. 142 y siguientes; Ferri, E.: *Principios de Derecho Criminal,* Ed. Reus, Madrid, 1933, pp. 45 y siguientes.

9 Agencia española de protección de datos: *14 equívocos en relación con la identificación y autenticación biométrica,* 2020, https://www.aepd.es/guias/nota-equivocos-biometria.pdf.

10 El artículo 3. 34) del Reglamento de Inteligencia Artificial, en virtud de la Resolución del Parlamento Europeo, de 13 de marzo de 2024, sobre la propuesta de Reglamento (P9_TA (2024)0138, dispone que son "datos biométricos", "los datos personales obtenidos a partir de un tratamiento técnico específico,

biométricos que se obtienen pueden ser el resultado del análisis de un elemento biométrico de naturaleza universal, a saber, que existe en todas las personas, o bien algo identitario y distintivo de la persona, de forma permanente o temporal. No todos los elementos biométricos son equivalentes y el índice de diferenciación de una persona frente a otra es diverso en función del tipo de biometría utilizada. Así, de acuerdo con el objetivo de los sistemas biométricos (identificar o reconocer, oautenticar o verificar las personas a partir de algunas características fisiológicas o morfológicas) se utiliza el sistema más adecuado[11]. En este sentido, los sistemas biométricos de reconocimiento utilizan un dato y lo comparan con una lista o base de datos, como sucede con las bases de datos criminales, mientras que los sistemas biométricos de verificación sólo utilizan un dato comparándolo con el mismo dato previamente almacenado, como es el caso de las bases migratorias[12]. Cada vez más se emplean sistemas biométricos de reconocimiento o autenticación con dos o más datos biométricos, que se denominan "sistemas de combinación biométrica", en los que pueden valorarse el peso, la altura, el tipo de sangre, factor sanguíneo, etc..

Si bien inicialmente las técnicas biométricas funcionaban a través de la instalación de sensores en edificios o salas, su desarrollo y polimorfa multifuncionalidad ha permitido que se integren sensores biométricos en los ordenadores corporativos, para gestionar la identificación con reconocimiento y autenticidad a las personas, a través de sistemas y aplicaciones con tecnologías biométricas. Se trabaja con la biometría bimodal, combinando factores de identificación de quién o cómo es y de lo que se sabe o se tiene[13]. Podemos considerar que a través de estos sistemas se puede[14]:

1.- Llevar a cabo el control de presencia, registrando horarios de trabajo (llegada y salida de los trabajadores), pudiendo emplearse la huella dactilar o la planta o la geometría de la mano, entre otras, siempre con el consentimiento de estos, en relación con la usabilidad de los datos biométricos.

relativos a las características físicas, fisiológicas o conductuales de una persona física, como imágenes faciales o datos dactiloscópicos".

11 Boulgouris, N. V. et al.: *Biometrics, Theory, Methods, and Applications*, IEEE and WILEY, Estados Unidos, 2010.

12 Díaz Rodríguez, V.: "Sistemas biométricos en materia criminal: un estudio comparado", *Revista IUS vol. 7, núm. 31*, Puebla, enero-junio 2013, en http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-21472013000100003.

13 Instituto nacional de ciberseguridad (incibe): *Tecnologías biométricas aplicadas a la ciberseguridad. Una guía de aproximación para el empresario,* 2016, en https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_tecnologias_biometricas_aplicadas_ciberseguridad_metad.pdf, p. 14.

14 Instituto nacional de ciberseguridad (incibe): *Tecnologías biométricas aplicadas a la ciberseguridad*, cit., pp. 14-15.

2.- Permite ser un instrumento de lucha contra el fraude, especialmente en el sector bancario (por ejemplo, para realizar transferencias bancarias) o en el ámbito del fraude a otras entidades privadas o incluso la Administración Pública.

3.- Conformar centros de atención de llamadas, esto es, los *Call-centers*, incorporando técnicas biométricas de reconocimiento de la voz, por ejemplo, otorgando mayor seguridad y eficiencia al comprobar la identidad del cliente interlocutor de forma más segura y con menos tiempo.

4.- Pueden igualmente favorecer el control de navegación como vía para acceder o negar redes sociales o a determinados sitios web, filtrar contenidos, etc.

5.- Para realizar vigilancia general o predictiva policial, ganando protagonismo el reconocimiento facial y el reconocimiento de la manera de andar (movimientos). Esta función está siendo contestada en el seno de la UE, y son numerosos los instrumentos que la limitan; recientemente, el texto de futuro Reglamento de Inteligencia Artificial UE (Artificial Intelligence Act).

6.- En los últimos años se ha venido empleando la denominada combinación biométrica con NFC, a saber, un sistema que permite proteger determinadas aplicaciones, autenticarse, realizar pagos o gestionar contraseñas en el ejercicio de las funciones de los dispositivos móviles. Ejemplo más común es la tecnología *Near Field Communication (NFC)* en los móviles, que permite realizar pagos desde el móvil con un sistema que permite identificar al usuario antes de validar la operación.

Si bien la aplicación general de estos sistemas biométricos es la de identificar a una persona, deben considerarse otras aplicaciones, de manera que es posible hablar: 1º) de medio de autenticación o verificación biométrica, comparando plantillas biométricas (que están en fichero) que pertenecen supuestamente a la misma persona para determinar que la persona es la misma en ambas, lo que el art. 3.36) del Reglamento IA considera como "verificación automatizada y uno-a-uno, incluida la autenticación, de la identidad de las personas físicas mediante la comparación de sus datos biométricos con los datos biométricos facilitados previamente"; 2º) de medio de identificación biométrica (art. 3. 35): "el reconocimiento automatizado de características humanas de tipo físico, fisiológico, conductual o psicológico para determinar la identidad de una persona física comparando sus datos biométricos con los datos biométricos de personas almacenados en una base de datos") ; y 3º) de medio de categorización o segregación biométrica, cuya finalidad no es identificar o verificar a la persona, sino categorizarla (por edad, sexo, raza...), exigiéndose en el Reglamento IA de la UE, de forma conjunta con los sistemas de reconocimiento de emociones, normas armonizadas de transparencia aplicables, de manera que se informe del

funcionamiento del sistema a las personas expuestas a este. Esta última modalidad es altamente riesgosa, dado que puede generar efectos discriminatorios que están proscritos por el art. 21 de la Carta de Derechos de la UE[15].

2. Tipología de las técnicas biométricas y su incidencia en el mundo jurídico.

Estas técnicas biométricas variarán según sean fisiológicas, comportamentales o ambas, y según se utilicen datos estáticos o datos dinámicos sobre el comportamiento[16]. Por un lado, entre las técnicas que inciden en los aspectos físicos y fisiológicos caracterizadores de una persona se hallan: huellas dactilares, análisis de la imagen del dedo, reconocimiento del iris, análisis de la retina, geometría de las manos, otogramas de las orejas, reconocimiento facial, de la voz, análisis de ADN, análisis de poros de la piel o incluso detección de olor corporal. Por otro lado, es posible trabajar con técnicas que analizan el comportamiento de una persona a través de la comprobación de la firma (figura, trazo, presión, velocidad, etc.), el análisis de la pulsación de las teclas, análisis de movimientos o forma de caminar, etc.. Y, además, la integración de ambos sistemas, a saber, aquellos que combinan las características biométricas del usuario con otras tecnologías de identificación o autenticación (contraseña y número de identificación personal, o huella dactilar, por ejemplo); es lo que se denomina la biometría multimodal o de segunda generación[17].

Los avances en biometría no cesan, presentándose como una respuesta a los peligros y riesgos que se están generando cada vez más en materia de ciberseguridad, de modo que frente a las contraseñas tradicionales -punto débil de los sistemas de seguridad desde hace tiempo- la biometría se presenta como la vía de garantía de la ciberseguridad, al combinar elementos identitarios corpóreos con patrones de comportamiento, otorgando una gran versatilidad al poder ser empleados en múltiples áreas y para una enorme multifuncionalidad. Vamos a referenciar algunas de estas modalidades.

A) Huellas dactilares.

Las huellas dactilares son los datos biométricos más usados, en gran medida por su sencillo acondicionamiento (podemos pensar que en la actualidad está siendo usada en dispositivos móviles y portátiles, como vía de autenticación sencilla de

15 En el mismo sentido, Etxeberría Guridi, J.F.: "Sistemas biométricos (el reconocimiento facial en particular) y sus aplicaciones", AAVV.: *Inteligencia Artificial y Administración de Justicia*, (dir. por S. Calaza López y M. Llorente Sánchez-Arjona), Thomson Reuters-Aranzadi, Cizur Menor (Navarra), 2022, pp. 170-171.

16 Grupo de trabajo de protección de las personas en lo que respecta al tratamiento de datos personales (markt/12168/02/es wp 80): *Documento de trabajo sobre biometría*, adoptado el 1 de agosto de 2003, https://www.informatica-juridica.com/documento-trabajo/documento-trabajo-biometria/

17 Grupo de trabajo de protección de las personas en lo que respecta al tratamiento de datos personales: Agencia espanola de protección de datos, *Dictamen 3/2012 sobre la evolución de las tecnologías biométricas* de 27 de abril de 2012 (WP193), https://www.aepd.es/documento/wp193_es.pdf.

los usuarios), que se integran fácilmente, amén de su bajo coste y su consideración de alta precisión[18]. Fue a finales del siglo XX cuando se desarrollaron los sistemas de reconocimiento mediante huellas dactilares, aun cuando la ficha decadactilar se creó en 1891 por el croata Iván Vucetich.

Puede haber dos maneras de recoger las huellas dactilares, bien a través del "basado de minucias", que consiste en identificar formas de la huella dactilar y su posición dentro de la misma; o bien a través del denominado "basado en correlación", o análisis de la huella dactilar de forma global. La huella dactilar ya fue desde hace tiempo un análisis que se realizaba y al que se otorgaba una importante validez en determinados sectores, inclusive permitía sustituirla por la firma cuando no se supiera escribir. Ahora bien en la última década se ha investigado que, aun cuando es difícil, no resulta imposible falsificar huellas dactilares, pudiendo defraudar a través de la entrada en espacios virtuales; inicialmente, estas falsificaciones permitieron desbloquear candados inteligencias y unidades USB protegidas con sensores de huellas dactilares, lo que constata su falibilidad.

B) Reconocimiento del iris y escáner biométrico de la retina.

El reconocimiento del iris se materializa a través de una cámara de infrarrojos, que realiza una fotografía del ojo, y permite identificar a la persona, en cuanto la información referida al iris no es variable (al menos no lo es hasta el momento). Son numerosas las aplicaciones que se realizan en la actualidad con este medio, tanto como medio de acceso propio a instrumentos personales (como el móvil o la Tablet), como para acceso colectivo (para entrar en un lugar de trabajo o para entrar en un país a través de la aduana electrónica, por ejemplo). Existen proyectos dudosos de escaneo de iris, como el "Worldcoin", al que nos referimos *infra*.

Igualmente es posible hacer referencia al escáner biométrico de la retina, que se basa en la utilización del patrón de los vasos sanguíneos contenidos en la misma; se considera una técnica idónea para entornos de alta seguridad por su alto grado de fiabilidad, si bien se requiere que el usuario voluntariamente acepte que se le realice la muestra, manteniéndose inmóvil y muy cerca del sensor durante la captura de la imagen[19], lo que se presenta como inconveniente.

C) Geometría del árbol de venas del dedo o de las muñecas.

El reconocimiento vascular es un dato biométrico que permite el estudio de la geometría del árbol de venas del dedo o de las muñecas. Es probablemente

18 Ferrer, C.: "¿Cómo cumplir el RGPD si manejas datos biométricos?", en *https://protecciódatos-lopd.com/empresas/datos-biometricos-rgpd/,* 9 de julio 2018. Puede verse igualmente, Instituto nacional de ciberseguridad (incibe): *Tecnologías biométricas aplicadas a la ciberseguridad,* p. 8.

19 Instituto nacional de ciberseguridad (incibe): *Tecnologías...*, cit., p. 9.

menos conocido que otros. Se capta, como si fuere una cámara de circuito cerrado de televisión para visualizar ambientes sin luz visible, lo que se denomina la "transmitancia" en la imagen, un proceso que permite diferenciar entre tejido muscular y lo que son venas y capilares, por tanto, el formato de las venas a través de la biometría vascular. Su incorporación a la Biometría arroja mejores resultados que la huella digital (que puede fallar en ciertos casos por falta de impresión en personas con diabetes o de edad avanzada o en quienes manejan productos químicos, o bien por suciedad en la impresión por polvo, cremas, etc, o incluso por cambios en la impresión debido, por ejemplo, a cortes, quemaduras, etc). Se considera, por tanto, que es un sistema biométrico de mayor fiabilidad y que surge como mecanismo de mejora de la biometría digital[20].

D) Reconocimiento biométrico de la palma de la mano.

El reconocimiento biométrico de la palma de la mano gracias a la aplicación de diversos algoritmos, como método de identificación. Fue Samsung quien patentó esta técnica, en la que se conjugan aprendizaje profundo, tecnología de visión computadora y redes neuronales, para reconocer las venas y los patrones de impresión de la palma de la mano, que singularizan las persona, obstaculizando posibles duplicidades. Funciona como una suerte de escaneo de la palma y comenzó inicialmente a emplearse para facilitar a las personas la recuperación de credenciales, ante la complicación que existe en muchos casos de tener que llamar a operadoras, utilizar el correo electrónico, etc. Una manera mucho más sencilla de conseguir el desbloqueo de algunos de nuestros instrumentos cotidianos personales y profesionales.

E) Reconocimiento de firma.

El reconocimiento de firma se presenta como otro de los parámetros biométricos de identificación de la persona. Es una forma de asociar la identidad del que firma un documento electrónico, gracias a la captación de datos biométricos asociados a la firma manuscrita sobre dispositivos electrónicos adecuados. Los datos biométricos que se capturan en la firma son la presión del instrumento con el que se firma (lápiz, bolígrafo), la velocidad de la escritura y la aceleración. Son de gran utilidad como sistemas de identificación en las gestiones bancarias, o en el ámbito laboral. Es una técnica diversa al reconocimiento de la firma manuscrita tradicional, dado que en ésta lo que importa es la firma en sí, las características de la misma, mientras que en la firma biométrica lo que importa es el cómo se realizó la firma para fijar criterios conductuales.

20 Puede verse más detalles en "Biometría vascular: ¿es el futuro?", en https://www.anixter.com/es_la/about-us/news-and-events/news/vascular-biometrics-is-it-the-future.html.

Igualmente, el del reconocimiento del escrito, que se realizará a través de un reconocimiento óptico de los caracteres del texto por medio de un software específicamente determinado.

F) Reconocimiento de escritura de teclado o biometría del tecleo.

El reconocimiento de escritura de teclado es un sistema que incide en un componente conductual - manera de escribir en un teclado-. Se denomina biometría del tecleo, y se analiza la manera y los tiempos en que una persona presiona una tecla y la suelta cuando escribe en una computadora. Aun cuando es técnica moderna, tiene antecedentes en el trabajo que la inteligencia militar en la II Guerra Mundial realizaba con el sistema de valoración de ritmos de transmisión de mensajes emitidos a través del "código morse", según la forma, ritmo de teclear, valorando cómo introducían puntos, comas, guiones en el mensaje, para detectar quienes eran amigos y quienes enemigos.

En la actualidad se trabaja a través de algoritmos, que crean patrones de dinámicas de escritura para efectuar las autentificaciones en su caso. Básicamente los parámetros que se emplean para llevar a cabo la medición, entre otros, son la fuerza con la que se teclea, el tiempo de pulsación y el plazo transcurrido entre las pulsaciones de teclado.

G) Reconocimiento de voz.

En el desarrollo de la investigación penal puede emplearse el reconocimiento de voz a través de aplicaciones algorítmicas que realizan una medición de muestras de voz y devuelven el resultado con la identificación o no de la persona. La voz es una de las características que singularizan a las personas de manera que con escuchar alguna palabra es posible distinguir e identificarla. Hay, empero, factores que pueden alterar la exteriorización de la voz, como el momento del día o alteraciones debido a catarro, faringitis, afonía, etc. Estos elementos permiten afirmar que la biometría de voz es más compleja que la de la huella dactilar, por ejemplo. Se trabaja sobre la parte de la voz que siempre es fija, como las ondas sonoras que se exteriorizan y vienen condicionadas por determinados parámetros fisiológicos como la posición de los dientes o la longitud del cuello entre otras, lo que permite la singularidad de la voz.

La biometría de la voz se despliega a través de varias etapas: por un lado, el registro que permite tomar varias muestras de voz de la persona (por ejemplo, diciendo un código o una frase), configurando la huella vocal; y en segundo lugar, en la fase de test se compara la huella vocal con la voz de quien habla, verificando

si corresponden o no a la misma persona[21]. En cualquier caso, se considera que pueden incidir factores externos que alteren el resultado, como la posible existencia de ruido de fondo que impidiera realizar de forma fiable esa identificación.

Recientemente, están surgiendo herramientas de audio capaces de clonar las voces humanas, a partir de una muestra de 15 segundos para desarrollar su creación. Un ejemplo de ello es el modelo "Voice Engine de Open AI", que utiliza texto y muestra de los 15 segundos para generar un habla natural que se asemeja mucho al hablante original, inclusive en otro idioma diverso al original. De momento es un ensayo, si bien genera no pocas dudas acerca de los riesgos de suplantación de identidad que pueden provocarse como consecuencia de estos resultados algorítmicos[22].

H) Análisis biométrico de movimientos corporales.

Como componente conductual de las personas también existe el análisis biométrico respecto de los movimientos de la persona o forma de caminar. Utilizar el andar humano como característica biométrica es algo relativamente novedoso, aun cuando su estudio ciertamente ha cobrado un enorme interés especialmente por su aplicación al ámbito de la vigilancia y seguridad. Cada persona tiene una manera diferente de caminar.

Lo que se pretende con la biometría es tomar este lenguaje corporal y traducirlo a un conjunto de datos que puede ser interpretado por una computadora. La diferencia con otros sistemas biométricos es que se puede realizar a distancia o incluso con imágenes de baja resolución, de manera que no depende de factores como el color, la textura o la iluminación. En este reconocimiento del andar humano se procesan imágenes extraídas de un video para obtener datos que permitan reconocer al sujeto que está caminando[23]. Su uso en la actualidad es extenso, en bancos, instalaciones militares, hoteles, aeropuertos, estaciones de tren, donde se justifica la posible existente de amenazas, siendo éste un medio para detectarlas de forma rápida[24].

21 "¿Cómo funciona la biometría de voz?", 8 de diciembre de 2015, en https://biometricvox.com/blog/biometria-de-voz/como-funciona-la-biometria-de-voz/.

22 Jiménez, M.: "Open AI lanza una herramienta de audio capaz de clonar las voces humanas", El País 30 de marzo de 2024.

23 Romero Moreno, M.: *Reconocimiento del Andar Humano basado en ensamble de clasificadores utilizando silueta y contorno*, Tesis de Maestría, Instituto Nacional de Astrofísica, Óptica y Electrónica, Tonantzinla, Puebla, 2008, en https://inaoe.repositorioinstitucional.mx/jspui/bitstream/1009/558/1/RomeroMM.pdf, pp. 2-3.

24 Ruane Dawson, M.: *Gait Recognition. Final Report,* Department of Computing Imperial College of Science, Technology and Medicine, Londres, 2002, 4-25.

l) Reconocimiento biométrico de orejas (otograma).

El reconocimiento biométrico de las orejas es el modelo avanzado de lo que históricamente se empleó hace ya algún tiempo en el campo forense, a los efectos de su utilización para la identificación de sospechosos. Era lo que se denominaba como otograma, otohuella o huella auricular[25], una prueba antropomórfica.

Se considera que el análisis del pabellón auricular es uno de los rasgos más fiables y significativos en el reconocimiento biométrico, dado su carácter individualizante y que, a diferencia de las huellas dactilares, no suele tener cambios a lo largo de la vida de la persona. Alphonse Bertillon fue el primer autor que consideró que la oreja era una de los elementos más importantes en la descripción de una persona, manteniendo que es casi imposible que dos orejas sean idénticas. Este autor desarrolló lo que se denominó la "fotografía métrica", en la que se estandarizaban las fotografías de identificación e imágenes visuales de las escenas de crímenes, aplicándolas en la ciencia forense[26]. Todo ello sin olvidar que este discurso permitió trabajar con la genética a Lombroso y sus discípulos creando su teoría antropológica criminal[27]. Ahora bien, si la irrupción de estas ideas se gestó en el Siglo XIX, fue en 1964 cuando el policía californiano Alfred Victor Lannarelli confirmó que en ese momento la huella dactilar y la oreja humana debían considerarse como los medios más adecuados para identificar a una persona[28].

La utilización de la oreja como característica biométrica del individuo viene marcada por ciertas ventajas: por un lado, las orejas son parte del cuerpo visible, elementos externos corpóreos y, por otro, es más sencillo llevar a cabo un reconocimiento biométrico teóricamente sin la percepción ni el consentimiento del sujeto pasivo. Incluso, se ha afirmado por González Sánchez[29], la biometría de la oreja también se puede utilizar para acentuar la efectividad de otras biometrías como la voz, geometría de la mano o identificación de rostros, favoreciendo con ello la implementación de sistemas biométricos multimodales o híbridos.

25 Gargantilla, P.: "Puedes acabar en la cárcel por la huella de tu oreja", publicado el 26 de mayo de 2019 en https://www.abc.es/ciencia/abci-puedes-acabar-carcel-huella-oreja-201905260149_noticia.html, quien explica: "el pabellón auricular está constituido por un esqueleto cartilaginoso, que se pliega sobre sí mismo formando relieves y depresiones, que en su conjunto configuran al pabellón una forma característica. La otohuella es la representación bidimensional del pabellón auricular".

26 "Bertillon system", en http://www.britannica.com/EBchecked/topic/62832/Bertillon-system.

27 Clouston, T. S.: "The Developmental Aspects of Criminal Anthropology", *The Journal of the Antropological Institute of Great Britain and Ireland*, vol. 23, pp. 215-225.

28 Gargantilla, P.: "Puedes acabar en la cárcel por la huella de tu oreja", cit., quien atribuye a Iannarelli el empleo de una denominación que se refiere al reconocimiento de la oreja, *Earology.*

29 González Sánchez, M.E.: *Análisis biométrico de las orejas,* Tesis Doctoral, Departamento de Informática y Sistemas, Universidad de Las Palmas de Gran Canaria, 2008, p. 6, en https://accedacris.ulpgc.es/bitstream/10553/3435/1/Analisis_biometrico_orejas.pdf. Esta autora insiste en la necesidad de aplicar un método robusto de extracción de características, a partir de las imágenes tomadas de la oreja, que se pueda usar para determinar la identidad de algunos individuos.

J) Biometría por ADN o huella genética.

Existe, igualmente, la biometría por ADN o huella genética (son datos genéticos[30]). La técnica atiende a una premisa: dos seres humanos tienen una gran parte de su secuencia de ADN en común y para distinguir a dos individuos se puede explotar la repetición de secuencias altamente variables llamada "microsatélites". Será poco probable que dos seres humanos no relacionados tengan el mismo número de microsatélites en un determinado locus; de ahí que es factible establecer una selección que raramente ha surgido por casualidad, salvo en el caso de gemelos idénticos, que tendrán idénticos perfiles genéticos pero no las huellas dactilares[31].

Esta técnica comenzó en la década de los años ochenta mediante la comparación de muestras genéticas con los perfiles genéticos que obran en las diversas bases de datos, y que puede llevar tanto a la identificación de posibles delincuentes como a la exculpación de quien ha quedado afectado a un proceso penal. Desde la década de los años ochenta hasta la actualidad la inteligencia artificial ha permitido perfeccionar lo que se denominan "Modelos de Inteligencia Forense" que se dirigen a la investigación criminal, empero tratar de equilibrarse en el marco de los derechos y las garantías de quienes son objeto de investigación[32].

Esta técnica de identificación de la huella genética se ha venido utilizando en las investigaciones criminales para identificar a los sospechosos con muestras de sangre, cabello, saliva o semen, o para fundamentar una absolución. Igualmente se utiliza en aplicaciones como la identificación de los restos humanos, pruebas de paternidad, la compatibilidad en la donación de órganos, el estudio de las poblaciones de animales silvestres, y el establecimiento del origen o la composición de alimentos. También se ha utilizado para generar hipótesis sobre las migraciones de los seres humanos en la prehistoria[33].

Para realizar un análisis genético de obtención de un perfil de ADN se requiere de la existencia de material biológico, que puede obtenerse de dos maneras diversas: por un lado, sin intervención corporal alguna, recogiendo dicho material, o bien mediante la intervención corporal para obtener las muestras o vestigios que permitan obtener el perfil de ADN. La injerencia en una serie de derechos

30 El Reglamento de Protección de Datos y la Directiva 2016/680 consideran los datos genéticos como una categoría autónoma y diversa respecto de los datos biométricos, si bien los diversos documentos de trabajo sobre biometría de la Agencia de Protección de Datos (WP80 y GT29) han venido a pronunciarse acerca de las técnicas de elaboración de perfiles de ADN, considerando una posibilidad de su usabilidad para generar sistemas de autenticación o identificación biométrica del ADN.

31 Ecured: "Biometría por ADN", en https://www.ecured.cu/Biometr%C3%ADa_por_ADN.

32 Caneppele, S., Ribeaux, O.: "Forensic intelligence", *"The Routledge International Handbook of Forensic Intelligence and Criminology",* Routledge, 2017, pp. 136-148.

33 Ecured: "Biometría por ADN", en https://www.ecured.cu/Biometr%C3%ADa_por_ADN.

fundamentales se traduce en que la práctica de las intervenciones corporales deberá efectuarse con el debido respeto a un régimen de garantías, máxime cuando estos resultados alcanzados puedan tener una influencia en la persecución de hechos delictivos[34].

K) Reconocimiento facial.

La técnica del reconocimiento facial permite el tratamiento automático de imágenes digitales que contienen las caras de personas con fines de identificación, autenticación o verificación y categorización de las personas empleando algoritmos, a través de "búsqueda de la apariencia". Este sistema algorítmico analiza las facciones del rostro de la persona y las compara con el resto de personas que se hallan incluidas en la base de datos; no es una mera captación de imágenes. Son cada vez más numerosas y más sofisticadas las aplicaciones y programas que permiten identificar a una persona por los rasgos de su cara. Se afirma que el rostro es la identidad visual más importante de un ser humano[35].

El reconocimiento facial se ha convertido en una herramienta efectiva y de gran usabilidad en los últimos tiempos, tanto en ámbitos públicos como privados, basada en un desarrollo tecnológico de *deep learning*, que ha logrado que el sistema computacional interprete con gran acierto la imagen, tras una acumulación masiva de datos biométricos faciales. Gobiernos[36] y empresas se han lanzado a trabajar con estas técnicas de reconocimiento facial, que permiten una vigilancia y seguridad de lugares de trabajo, de aeropuertos, de centros comerciales, de colegios, universidades[37], etc.

Pese a las posibles mermas de capacidad identificadora de los modelos concurrentes, debido a circunstancias como el ángulo de la cámara, el cambio de tono de piel o por cambios estéticos de la cara, en los últimos tiempos las empresas destinadas al diseño y perfeccionamiento de estos softwares han incorporado tecnología de última generación, saltando obstáculos. Los avances en esta técnica biométrica han sido espectaculares, debido a los desarrollos algorítmicos, a la cada

34 Etxeberría guridi, J.F.: "Obtención de perfiles de ADN a la luz de la nueva Orden Europea de Investigación (OEI): diversas alternativas", AAVV.: *Claves de la Justicia Penal. Feminización, Inteligencia Artificial, Supranacionalidad y Seguridad*, (ed. por S. Barona Vilar). Tirant lo Blanch, Valencia, 2019, p. 379.

35 Prasanthi Jasmine, K.; Naga Prakash, K.: *Reconocimiento de emociones humanas a partir de imágenes de rostros*, Ed. Nuestro Conocimiento, 2021, p. 6.

36 Fue EEUU en la década de los noventa cuando desarrolló algunos programas de reconocimiento automatizado de rostros (FERET -*Face Recognition Technmology*-, FRVT -*Face Recognition Vendor Test*-), conm una fiabilidad diversa en función del entorno controlado o no. Puede verse, Escajedo San Epifanio, L.: *Reconocimiento e Identificación de las personas mediante Biometrías estáticas y dinámicas,* cit., p. 90.

37 Con motivo de la realización de pruebas de evaluación on line de estudiantes, ante la situación de crisis sanitaria del COVID-19, la Agencia Española de Protección de Datos (AEDP) realizó un Informe sobre el posible uso del reconocimiento facial a los alumnos que realizan los exámenes universitarios, debiendo concurrir consentimiento libre del afectado, y legitimándose en la existencia de un interés público que debe ser "esencial" para que pueda ser legítimo, que debería justificarse en una norma con rango de ley, que no existía, https://www.aepd.es/es/documento/2020-0036.pdf.

vez mayor disponibilidad de grandes bases de datos de imágenes faciales y método para evaluar el rendimiento y la fiabilidad de los algoritmos de reconocimiento facial[38]. Paradigmático fue la identificación a través de estos datos biométricos del rostro a una persona aun cuando esté usando mascarilla por causa del COVID-19. La tecnología se renovó y se aceleró el entrenamiento de algoritmos para identificar a personas con mascarillas[39].

La experiencia del empleo de las técnicas biométricas de reconocimiento facial en China, Japón, Corea del Sur, Singapur, en parte de EEUU, es larga. Los condicionantes en cada país y sus límites legales son diversos. Si bien es cierto que su empleo en el control de acceso a determinados espacios físicos o virtuales se ha generalizado, en Europa sigue manteniéndose una posición resistente, por los falsos positivos o negativos producidos, que han cobrado especial relevancia, sobre todo cuando se usa como sistema de identificación remota en la prevención, la investigación, el enjuiciamiento y la ejecución de infracciones penales, dada la afectación de derechos fundamentales.

En Europa en general se cuestiona su fiabilidad, su funcionalidad, planteando cuestiones éticas y de afectación de derechos fundamentales, y muy especialmente también del derecho de protección de datos, que tan celosamente ha querido tutelarse por las instituciones europeas. Pese a esta resistencia, hay ya diversas manifestaciones, refiriéndonos a algunos proyectos piloto[40].

En España, a título de ejemplo, Marbella, Ceuta, La Nucía, Las Rozas o Vaciamadrid poseen cámaras que incorporan la técnica biométrica del reconocimiento facial, en la lucha contra determinada delincuencia. La potencia del software marbellí busca por apariencia, que incluye rasgos del rostro, color de ropa, edad, género, color de pelo y aspecto. Frente a los detractores de estos sistemas, se argumenta que se trata de un modelo de inteligencia artificial capaz de observar miles de horas de video para acelerar o concentrar las búsquedas, permitiendo hallar personas y objetos, por ejemplo, automóviles[41]. Y se presenta como la tensión cada vez más íntima o carnal entre las anatomías humanas y los objetos técnicos[42]. No obstante,

38 Prasanthi Jasmine, K.; Naga Prakash, K.: *Reconocimiento de emociones humanas* …, cit., p. 7.

39 García, J.G.: "El reconocimiento facial aprende a identificar mascarillas", *Retina, El País Economía,* mayo 2020. Este autor se refiere precisamente a HERTA, compañía dedicada a conseguir estos avances de forma acelerada.

40 Barona Vilar, S.: *Algoritmización del derecho y de la justicia,* cit., pp. 489-490.

41 A través del software se pretende hacer seguimiento del vehículo, dado que precisamente en Marbella el robo de coches de alta gama se da con mucha asiduidad. Pérez Colomé, J.: "Marbella, el mayor laboratorio de videovigilancia de España", *El País, 22 de noviembre de 2019*, https://elpais.com/tecnologia/2019/11/21/actualidad/1574348695_231540.html, considera que el gran peligro es avanzar poco a poco este software de reconocimiento facial, permitiéndose la búsqueda indiscriminada de la cara de algún sospechoso. La situación no está exenta de dudas, y prueba de ello son las sanciones desde la UE, como la impuesta por empleo de reconocimiento facial en un colegio sueco, pese a tener el consentimiento de los alumnos; y la otra, en Londres, que en la zona de King's Cross estuvo usando durante dos años esta tecnología.

42 Sadin, E.: *La humanidad aumentada,* Ed Caja Negra, 2017, p. 82.

amén de los falsos positivos y negativos, concurre todavía la posibilidad de incurrir en discriminación, en parte por los sesgos y en parte por la calidad de los datos. Precisamente, la Agencia de los Derechos Fundamentales de la Unión Europea (FRA European Union Agency for Fundamentals Rights), refiriéndose a la calidad de los datos, apunta la necesidad de que el software de reconocimiento facial sea alimentado de grandes cantidades de imágenes faciales (debe entenderse, representativas de los diferentes grupos étnicos y de género), dado que, a mayor cantidad de imágenes, mayor precisión en las predicciones[43].

De hecho, cada vez más asistimos a una evolución de esta técnica, combinando características físicas con psicológicas que entroncan con origen, emociones y bienestar y cada vez más están comenzando a emplearse para detectar si las personas mienten o dicen la verdad (inclusive en el ámbito laboral a efectos de productividad). Esto va más allá de la mera identificación.

Así, el Reglamento de la IA (AI Act, P9_TA(2024)0138)[44] incorpora la referencia a los "sistemas de reconocimiento de emociones", entendiendo que se trata de un "sistema de IA destinado a detectar o deducir las emociones o las intenciones de personas físicas a partir de sus datos biométricos" (art. 3.34). Ejemplo de este sistema de reconocimiento de emociones fue el Proyecto iBorderCtrl que se establece en la UE para la detección de mentiras en las fronteras, en el que intervenían Luxemburgo, Chipre, Reino Unido, Polonia, España, Hungría, Alemania y Letonia[45], que provocó reacciones en contra, como el Informe de 13 de julio de 2021 de la Comisión de Libertades Civiles, Justicia y Asuntos de Interior del Parlamento Europeo (A9-0232/2021), que insta a la Comisión para que deje de financiar investigaciones, aplicaciones o programas biométricos que puedan concluir probablemente en una vigilancia masiva e indiscriminada en espacios públicos. El Parlamento Europeo se ha mostrado muy preocupado, especialmente por los efectos de la utilización de los sistemas de reconocimiento facial en sectores como la prevención, investigación, enjuiciamiento y ejecución en materia penal, si bien se recogen como posibles en el texto del reglamento IA.

En algunos países europeos se han dado situaciones específicas con respuestas *ad hoc*. Francia, a través de su regulador de la privacidad en internet (CNIL) propone distinguir cuándo un reconocimiento facial es necesario y cuándo no, para evitar la situación desmedida en una sociedad que se asienta en el reconocimiento de los derechos y las libertades de las personas. Por su parte, Suecia, a través de su Agencia de Protección de Datos, ha multado con 18.500 euros a una escuela secundaria de Skelleftea por adoptar la tecnología de reconocimiento facial para

43 *Facial recognition technology: fundamental rights considerations in the context of law enforcement (2020)*, p. 27.

44 https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_ES.pdf.

45 https://ec.europa.eu/research/infocentre/article_en.cfm?artid=49726.

controlar la asistencia de los alumnos al aula, entendiendo que este proyecto vulnera varios artículos del Reglamento de Protección de Datos, de obligado cumplimiento para empresas y ciudadanos. Fuera de Europa, San Francisco fue la primera ciudad en EEUU que prohibió el uso de la tecnología de reconocimiento facial –debido al movimiento de las organizaciones pro derechos humanos que se manifestaron en contra-, a las que han seguido Oakland, Berkley (California) y Somerville (Massachusetts), en las que se consideró la posible prohibición de la vigilancia facial por el Gobierno. Ahora bien, Nueva York, Chicago, Detroit y Washington tienen programas piloto para implementar estos sistemas. En Gran Bretaña la policía de Gales del Sur lo probó como sistema de vigilancia y en Londres (Scotland Yard), un sistema de cámaras de reconocimiento facial en vivo (LFR), con el objetivo de identificar delincuentes en las calles de la ciudad. Es un sistema capaz de hacer identificación de caras a través del procesamiento de imágenes de caras de gente que pasa por la calle, de forma indiscriminada, detectando si alguna coincide con la lista almacenada de personas sospechosas de haber cometido un hecho delictivo. Durante tres años se han venido realizando pruebas preliminares, arrojando un resultado que para la policía es satisfactorio, en cuanto el sistema ha registrado aciertos en un 70 por cien de los casos (lo que es altamente peligroso si pensamos en el 30% restante), con voces críticas que han presentado un estudio independiente de la policía en el que se demostró un 81% de falsos positivos, lo que incitó que organizaciones civiles (como *Big Brother Watch*) se posicionaran contra su uso de forma indiscriminada[46], considerando que supone un ataque a los derechos de las personas[47].

La posición cautelosa de la UE ha sido constante, por los riesgos e injerencias desmedidas en los derechos fundamentales de las personas. El Reglamento IA (2024) establece en el artículo 5 las prácticas prohibidas de IA, refiriéndose en la letra h) a los sistemas de identificación biométrica remota "en tiempo real" en espacios de acceso público con fines de aplicación de la ley, salvo y en la medida en que dicho uso sea estrictamente necesario para alcanzar algunos de los tres objetivos que se exponen, como excepción a la prohibición: 1°) cuando se trate de una búsqueda selectiva de víctimas concretas de secuestro, trata de seres humanos o explotación sexual de seres humanos, así como la búsqueda de personas desaparecidas; 2°) para la prevención de una amenaza específica, importante e inminente para la vida o la seguridad física de las personas físicas o de una amenaza real y actual o real y previsible de un atentado terrorista; y 3°) para localizar o identificar a una persona sospechosa de haber cometido una infracción penal, con fines de investigación o enjuiciamiento penales o de ejecución de una sanción penal por alguno de los delitos (anexo II) que el Estado castigue con una

46 Barona Vilar, S.: *Algoritmización del derecho y de la justicia,* cit., pp. 491-492.

47 De Miguel, R.; Victoria, M.; Nadal, S.: "Londres instalará cámaras de reconocimiento facial", en El País, sábado 25 de enero de 2020, p. 3.

pena o una medida de seguridad privativas de libertad cuya duración máxima sea de al menos cuatro años.

Se exige en el Reglamento que solo se emplee para los fines expuestos, y bajo las siguientes condiciones: a) la naturaleza de la situación que permite su uso (gravedad, probabilidad y magnitud del perjuicio que se produciría de no utilizarse el sistema); b) las consecuencias que tendría en los derechos y libertades de las personas implicadas y, en particular, la gravedad, probabilidad y magnitud de dichas consecuencias. Además, se exige que se realice en condiciones de necesidad y proporcionalidad, de acuerdo con la legislación nacional que lo autorice, y si la autoridad encargada de la aplicación de la ley ha completado una evaluación de impacto relativa a los derechos fundamentales (en casos de urgencia cabe la utilización de estos sistemas sin registro en la base de datos de la UE, si bien se llevará a cabo sin demora). El uso de estos sistemas de identificación biométrica remota en tiempo real estará supeditado a la concesión de una autorización previa por parte de la autoridad judicial o administrativa independiente, salvo urgencia justificada, solicitándola sin demora debida, a más tardar en un plazo de 24 horas. Rechazada la autorización, se producirá la interrupción de inmediato desechándose todos los datos.

En numerosos países asiáticos[48] se ha acometido un desarrollo tecnológico para favorecer este control a través del reconocimiento facial masivo. Se dice que China es el principal banco de pruebas de esta tecnología, no solo para controlar criminales, sino para llevar a cabo una monitorización (laboral, en las escuelas, universidades, etc), para vigilar a minorías étnicas o para efectuar seguimiento de disidentes políticos. En suma, se muestra como un cauce para implementar un sistema de vigilancia policial predictiva, una monitorización de los ciudadanos, de dónde van, con quién van, qué compran, con quién hablan, si hacen deporte, si viajan mucho, y un largo etcétera. Así, con la tecnología biométrica de identificación facial se permite realizar, como ha sucedido en China, una clasificación ciudadana que, allende la funcionalidad de seguridad ciudadana, convierte a las personas en un número, un color, se le cosifica, y todo ello con ineludibles consecuencias jurídicas.

Uno de los proyectos pioneros fue el desplegado en la región china de Xinjang, en la ciudad de Tumxuk, donde los funcionarios han recogido sin consentimiento muestras de sangre de cientos de uigures como parte de una campaña de recolección masiva de ADN, siendo el objetivo de ello crear imágenes faciales exactas con la información de las muestras de ADN, una tecnología que podría emplearse contra la minoría uigur –son cerca de 11 millones de uigures los que viven en la citada región china y son una minoría predominantemente

48 Barona Vilar, S.: *Algoritmización del derecho y de la justicia,* cit., p. 493.

musulmana- así como respecto de opositores disidentes políticos. El desarrollo tecnológico se realiza en laboratorios dependientes del Ministerio de Sanidad chino con la intervención de dos científicos chinos del Ministerio financiados por la Max-Planck Society y la Erasmus University Medical Center de Holanda. Ha provocado campañas de represión gubernamental contra esta y otras minorías de la provincia, con detenciones masivas, con argumentos de lucha preventiva terrorista y del extremismo islámico. Con el sistema tecnológico chino se aúnan las bases de datos de ADN (la más grande del mundo, con más de 80 perfiles, según medios chinos), que podrían alimentar los sistemas de vigilancia masiva y reconocimiento facial simultáneamente, de manera que se mantendría un férreo control sobre la sociedad civil al permitir no solo rastrear a delincuentes, sino también a manifestantes o a disidentes, con el fin de garantizar las políticas de segregación.

La cuestión es, en suma, para qué el uso de este software que permite etiquetar a las personas, máxime cuando existe el riesgo de que el mismo sistema computacional venga inoculado de sesgos, con niveles de error que ya han sido constatados, como la confusión de 28 congresistas con sospechosos de la policía por un reconocimiento facial hecho por Amazón en 2018[49], lo que cuestiona su fiabilidad[50].

III. AHORA BIEN...NO TODO VALE.

Los desarrollos científicos y tecnológicos y su aplicación a los sistemas biométricos están empleándose en espacios privados y públicos con consecuencias más que palmarias en los derechos y libertades fundamentales. La obtención masiva de datos (excepcional o sin excepción, según el espacio geográfico del planeta), la identificación, la autenticación, la explotación de la información conductual, la clasificación o perfiles que se crean, están permitiendo construir un mundo en el que la manipulación está presente, favoreciendo la alteración de comportamientos de las personas (por ejemplo, en la toma de decisión en las elecciones políticas, en el consumo, en la cultura, etc.), la adopción de políticas represivas frente a minorías, o grupos raciales, o para pervertir políticas igualitarias, a emplear los datos alcanzados para ofrecer respuestas predictivas de riesgos (cometerá delito o reincidirá), para interferir en emociones en el lugar de trabajo, para clasificar y etiquetar a las personas -perfiles- (por raza, sexo, ideología, etc)... Son numerosas

49 Rubio, I.: "Reconocimiento facial: la tecnología que lo sabe todo", en *El País, 25 de mayo de 2019, https://elpais.com/tecnologia/2019/05/21/actualidad/1558455279_966010.html?rel=mas*. Por ejemplo, en EEUU, Amazon ensaya una aplicación de reparto que obliga al mensajero a hacerse una foto cuando entrega el paquete para cotejarla con un programa de reconocimiento facial.

50 Un estudio del Centro de Georgetown para la Privacidad y la Tecnología asegura que el reconocimiento facial utilizado por varios departamentos norteamericanos tiene mucho más margen de error con afroamericanos. Rubio, I.: "Reconocimiento facial: la tecnología que lo sabe todo", en *El País, 25 de mayo de 2019, https://elpais.com/tecnologia/2019/05/21/actualidad/1558455279_966010.html?rel=mas*.

las situaciones que van propulsando lo que Byung-Chul Han denomina como *psicopolítica digital*, que se apodera de la conducta social de las masas, o dicho de otro modo, la sociedad de la vigilancia digital, como le llama este autor, tiene acceso al inconsciente colectivo, controla y manipula posibles futuros comportamientos sociales, lo que irrefutablemente nos está llevando a sistemas totalitarios, en cuanto somos programados y controlados por una ideología que nos viene impuesta, tanto política como social[51]. Es por ello que considera que "el mercado de vigilancia en el Estado democrático se acerca peligrosamente al estado de vigilancia digital". En él vigilancia y control son una parte de la comunicación digital, si bien ese *Big Brother* lleva a que no solo sea el servicio secreto del Estado el que vigile, sino que Facebook, Apple, Amazon, Google, Huawei, los bancos, etc., actúen de espías de sus trabajadores, de sus usuarios, de sus consumidores[52]. Y mientras tanto, los habitantes del panóptico benthiano digital que somos todos vivimos con la ilusión de alimentar con más y más información, renunciando a nuestra esfera privada e íntima y exponiéndola a cambio de una ilusión de seguridad que desde luego no existe[53]. Muy probablemente concurre una suerte de inconsciencia que nos lleva a regalar datos, con un coste impredecible en los momentos en que vivimos.

Ante esta real y perturbadora situación, estamos asistiendo, por un lado, a la necesidad de un marco normativo que permita fijar límites de actuación (qué se puede hacer, hasta dónde llegar y por qué), que exige una reflexión sobre el equilibrio entre la realidad y el deseo, entre qué se puede, por qué se puede y en qué condiciones. El Reglamento de IA, en su última versión de 2024, es el que nos ofrece esa búsqueda del equilibrio entre lo prohibido y lo permitido, siempre con el debido respeto al equilibrio con los derechos y libertades fundamentales. Por otro lado, la importante labor jurisprudencial, que proviene de los tribunales (tanto el TJUE como los tribunales nacionales), así como de las autoridades administrativas de control (agencias de protección de datos en particular) está permitiendo, en tiempos de tránsito en una sociedad digital que cabalga velozmente hacia desarrollos cada vez más disruptivos, responder ante situaciones de "exceso" que truncan los límites de un modelo jurídico de derechos.

1. Punto de partida: Protección jurídica de los datos biométricos.

La necesidad de determinar que no todo vale es lo que llevó a la Unión Europea a preocuparse por establecer normativamente el equilibrio entre la seguridad y los derechos, y muy especialmente la privacidad de las personas. Así, el art. 8 de la Carta de Derechos Fundamentales de la Unión Europea (2000/C364/01) de 18 de diciembre, otorga ese reconocimiento de derecho fundamental a la protección de

51 Han, B-CH: *En el enjambre*, Herder, 2014, pp. 108-109.

52 Han, B-CH: *En el enjambre*, cit., pp. 100-101.

53 Barona Vilar, S.: *Algoritmización del derecho y de la justicia,* cit., p. 495.

datos personales; e igualmente, el art. 16 del Tratado de Lisboa (de Funcionamiento de la UE, TFUE), defendiendo a las personas frente a posibles amenazas de la era digital, fruto de los avances científicos y tecnológicos[54]. El camino tuitivo de protección de datos proviene de la Directiva 95/46/CE, de 24 de octubre, sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, así como en la Decisión Marco 2008/977/JAI, de noviembre de 2008, para la protección de datos personales en la cooperación policial y judicial en materia penal; derogados por el Reglamento (UE) 2016/679, de 27 de abril de 2016, sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DOUE, de 4 de mayo de 2016), que introduce reglas generales uniformes en el Derecho de la Unión[55] y la Directiva (UE) 2016/680, que rige para la protección de datos en relación con la cooperación policial y judicial al prevenir, investigar, detectar o enjuiciar delitos[56]. Sin perjuicio de otras normas que los complementan, así como la jurisprudencia del TJUE, verdadero impulsor e interpretador fundamental del derecho a la protección de datos[57], la UE garantiza el derecho a la protección de los datos personales en la UE.

Si bien inicialmente el tratamiento jurídico de los datos biométricos era el mismo que el de datos de carácter personal, la situación cambia con el Reglamento Europeo de Protección de Datos 2016/679, de 27 de abril, que los considera como "datos de carácter sensible". El art. 4.14 define los datos biométricos como "datos personales obtenidos a partir de un tratamiento técnico específico, relativo a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirme la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos". Además, los datos no personales se regulan por el Reglamento 2018/1807, relativo al marco para la libre circulación de datos no personales en la UE, aplicable desde 28 de mayo de 2018, que habrá que considerar en todo caso, máxime con difuminación entre datos personales y los no personales, debido a los

54 Sobre la incidencia de estos desarrollos puede verse: Barona Vilar,baroBbb S.: *Algoritmización del derecho y de la justicia*, cit., pp. 42-76, así como Planchadell Gargallo, A.: "Inteligencia Artificial y medidas cautelares", AAVV, *Justicia algorítmica y neuroderecho: una mirada multidisciplinar*, (ed. por S. Barona Vilar), Tirant lo Blanch, Valencia, 2021, pp. 389-419.

55 Este Reglamento deroga la Directiva 95/46/CE (RGPD) y propulsó la promulgación española de la L.O 3/2018, de 5 de diciembre, de Protección de Datos personales y garantías de los y garantía de los derechos digitales.

56 Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo (DOUE, de 4 de mayo de 2016).

57 Rallo Lombarte, A.: "El Tribunal de Justicia de la Unión Europea como juez garante de la privacidad en Internet", *UNED. Teoría y Realidad Constitucional*, núm. 39, 2017, p. 584; http://revistas.uned.es/index.php/TRC/article/view/19150; y también, Piñar Mañas, J.L.; Recio Gayo, M.: *El derecho a la protección de datos en la jurisprudencia del Tribunal de Justicia de la Unión Europea*, Wolters Kluwer-La Ley, Madrid, 2018, p. 300.

desarrollos tecnológicos que nos invaden[58], que están propulsando la distinción entre datos biométricos de primera y de segunda generación. Y propicia que en ciertos casos el tratamiento de estos datos se puede hacer perfectamente sin que el titular de los datos lo perciba, lo que a su vez complica la verificación de la actuación de los responsables del tratamiento de acuerdo con la normativa de protección de datos. Este riesgo se retroalimenta con otro, la posible elaboración de perfiles, que pueden favorecer categorías o clasificaciones, camino perfecto para propiciar un estigma social.

En consecuencia, el tratamiento de los datos biométricos no será en todos los casos igual (así se pronunció también el TEDH en la Sentencia de 4 de diciembre de 2008, caso "Marper"), de modo que habrá que estar al grado de injerencia de cada uno. En todo caso, habrá que respetar los principios de necesidad, idoneidad y proporcionalidad en el tratamiento, así como la adopción de determinadas medidas de seguridad basadas en cifrado y en control de acceso de acuerdo con la finalidad de obtención de los datos biométricos: control de presencia, identificación, control de la información o control de acceso. Se establece la necesidad de medidas concretas en caso de datos sensibles, almacenándose en plantillas biométricas, no almacenamiento centralizado de los datos, sino en dispositivos cifrados, recomendándose que se supriman los datos biométricos de forma automática cuando se cumpla el tiempo necesario para el fin por el que se recogieron. Y se establece la obligación del responsable del tratamiento de establecer un protocolo de control de acceso que registre qué persona ha accedido a los datos, fecha y hora en que se accedió y los datos a los que se ha accedido.

Por su parte, el art. 9 del Reglamento configura unos requisitos, como son la necesidad de que exista consentimiento explícito en un documento donde se especifique la finalidad para la que se obtienen esos datos biométricos, así como la evaluación de impacto sobre los datos y, por supuesto, el debido registro de actividades de tratamiento (como mínimo: nombre y datos de contacto – responsable, corresponsable, representante del responsable, delegado de protección de datos-, fines del tratamiento, descripción de las categorías interesados y de las categorías de datos personales, así como de los plazos previstos para la supresión de las diferentes categorías de datos).

El gran dilema que se nos presenta como sociedad es manejar adecuadamente las excepciones que permiten la injerencia en los derechos y libertades de las personas a través de sus datos (biométricos). El entorno que nos rodea, en el que hay una clara cesión de garantías y derechos como respuesta "necesaria(?)" para

58 Muñoz ruiz, A.B.: *Biometría y sistemas automatizados de reconocimiento de emociones: Implicaciones jurídico-laborales,* Ed. Tirant lo Blanch, Valencia, 2023, p. 25.

garantizar la "seguridad", nacional e internacional, del Estado, el interés público, el orden público (conceptos indeterminados que exigen concreción), nos lleva al punto de partida, generado con la irrupción de la tecnología disruptiva, el albor algorítmico y la inteligencia artificial, que no es otro que el "humanismo está en retirada", como señala Lasalle[59], fruto de esa fascinante servidumbre maquínica, que nos convierte en proletariado digital. Es imprescindible configurar contrapesos a esa atractiva y fascinante emergencia tecnológica. Los medios existen: los límites legales y éticos, nacionales y supranacionales, la función tuitiva de los tribunales, y la mirada crítica de los investigadores.

2. La teoría nos la sabemos, pero qué sucede en la práctica.

El equilibrio entre lo posible y lo refutable lo tenemos claro y la Unión Europea y los diversos Estados miembros han hecho un gran esfuerzo por fijar un marco de permisibilidad versus restricción de la utilidad de los datos biométricos. Los tribunales están velando igualmente por mantener ese equilibrio. Sin embargo, los desafíos son enormes y la expansión de su usabilidad ha venido aflorando situaciones alarmantes. Si bien es palmario que el marco normativo ha esclarecido con carácter general los límites inquebrantables cuando de datos biométricos se trata, la práctica nos ofrece algunos casos que merecen tomarse en consideración.

A) Seguridad frente a la sofisticada criminalidad, derivada de la globalización.

En los albores del siglo XXI asistimos a una metamorfosis del planeta, de la mano de la globalización, que propulsó una transformación social, económica, cultural, social, sociológica, ideológica, etc., alterando los modelos de Estado configurados a lo largo del siglo XX. La globalización cambió los Estados (minimizados ante una economía que devora la política) y el significado de las fronteras. Esta mutación favoreció la movilidad para lo bueno y para lo malo, favoreciendo igualmente una proliferación de la criminalidad, también en cuanto a su sofisticación, aflorando la delincuencia organizada y el terrorismo internacional. Surgieron motivos de seguridad y orden público que desequilibran la balanza en desfavor de los derechos de la persona y, por supuesto, del derecho a la protección de datos personales. Comenzó el tratamiento masivo de los datos para favorecer el intercambio de información en materia de cooperación entre autoridades policiales y judiciales europeas y su transferencia a terceros países[60].

59 Lasalle, J.M.: *Ciberleviatán*, Barcelona, Ed Arpa, 2019, p. 50.

60 Sobre estas cuestiones Gutiérrez Zarza, A.: "Terrorismo yihadista, crisis migratorias, fronteras, prueba electrónica, encriptado, referéndum y otras palabras clave del espacio LSJ", en *Diario La Ley, Sección Tribuna*, núm. 8904, 2016, http://diariolaley.laley.es/home/DT0000240761/20170111/Terrorismo-yihadista-crisis-migratorias-fronteras- prueba-electronica-encriptado-, acceso el 3 de febrero de 2024.

Son ya múltiples las herramientas "asimétricas" y "heterogéneas" que desequilibran esa protección de datos enmarcada en las normas expuestas: SIS (Sistema de Información de Schengen) y SIS II (Sistema de Información de Schengen de segunda generación); EURODAC; VIS (Sistema de Información de Visados); API (Información Previa sobre Pasajeros); SIA (Sistema de Información Aduanero); PRÜM I y II[61] (Instrumentos de la UE para prevenir y combatir el terrorismo y otras formas graves de delincuencia transfronteriza, que intercambian ADN, datos dáctiloscópicos, registros de matriculación de vehículos y datos personales y no personales relacionados con la cooperación policial transfronteriza); ECRIS (Sistema de Información Europeo de Antecedentes Penales[62]); Registro de Nombres de Pasajeros (PNR)[63]; Programa de seguimiento de la financiación del terrorismo, además de generar Unidades y Organismos (de Información Financiera; de Recuperación de Activos; Europol; Eurojust para cooperación en investigaciones y actuaciones relativas a la delincuencia grave que afecta al menos a dos Estados miembros).

El equilibrio entre la protección de los datos, como derecho fundamental, y la lucha contra la criminalidad, por otro, está propulsando en el seno de la UE acciones que comportan la necesidad de actuar por motivos de interés público y en deterimento del interés individual o colectivo de la ciudadanía. Hay excepciones por motivos de "seguridad", bajo el debido respeto a la proporcionalidad, amén de-según la Directiva de protección de datos en el ámbito penal- una necesidad indiscutible y autorización, ora de las autoridades nacionales ora de las europeas, además de concurrir en su tratamiento y uso las garantías adecuadas. Esa naturalización de "excepcionalidad" es lo que se otorga en el Reglamento IA (AI Act 2024), delimitando las prohibiciones y sobre todo configurando los supuestos en que de forma excepcional y bajo determinadas condiciones, podría justificarse el empleo de sistemas algorítmicos y de inteligencia artificial que traspasen las barreras de la protección de datos configurada en la UE y reforzada por la Carta de Derechos Fundamentales de la UE. En todo caso, la excepcionalidad debe interpretarse restrictivamente, siendo un habitat adecuado cuando se pretende luchar contra la delincuencia organizada y el terrorismo.

61 Reglamento (UE) 2024/9823 del Parlamento Europeo y del Consejo, de 13 de marzo de 2024, relativo a la búsqueda y al intercambio automatizado de datos para la cooperación policial, y por el que se modifican las decisiones 2008/615/JAI y 2008/616/JAI del Consejo y los reglamentos (UE) 2018/1726 (UE) 2019/817 y (UE) 2019/818 del Parlamento Europeo y del Consejo (Reglamento Prüm II).

62 ECRIS permite el intercambio de información, a través de una red segura, sobre las condenas pronunciadas contra una persona determinada por los órganos jurisdiccionales penales en la Unión Europea; información de identificación alfanumérica, aunque es posible el intercambio de datos biométricos. Comisión Europea: "Sistemas de información más sólidos e inteligentes para la gestión de las fronteras y la seguridad", COM (2016) 205 final, de 14 de septiembre de 2016.

63 Catalina Benavente, M.A.: "La recogida y tratamiento masivo de los datos PNR: algunas cuestiones para preocuparse", en AAVV, *Claves de la Justicia Penal. Feminización, Inteligencia Artificial, Supranacionalidad y Seguridad, (*ed. por S. Barona Vilar), Tirant lo Blanch, Valencia, 2019, pp. 279-295.

El Parlamento Europeo ha aprobado la creación de una base de datos biométricos de huella dactilar o de la cara del usuario de los más de 500 millones de habitantes de la UE; una base de datos centralizada que incluirá la información habitual (nombre, dirección, fecha de nacimiento y número de identidad) y datos biométricos de la huella dactilar o de la cara del usuario (con foto incluida), y escaneos faciales. Esta nueva base de datos se denomina *Common Identity Repository (CIR)*[64], que unificará los registros de 500 millones de ciudadanos de la UE, estando a disposición de las fuerzas de seguridad, incluidas las responsables de los pasos fronterizos de los países miembros[65].

B) Algunos Proyectos nacionales e internacionales en marcha con datos biométricos. Dudas.

Existe igualmente un proyecto piloto en Menorca en virtud del cual se permite (Aena así lo ha aprobado con Air Europa) subirse al avión mediante reconocimiento facial utilizando detectores biométricos. Es un sistema que pretende, por un lado, de forma más ágil y rápida identificar la persona física que quiere subir al avión con el que es portador del billete. Si su empleo fuere solo para identificar al pasajero, podría aceptarse como medida piloto, empero plantea dudas cuando el sistema va más allá, detectando estados de ánimo, de salud, ADN del pasajero y un largo etcétera que vienen a generar información sensible de las personas que no deben ni pueden ser almacenadas, clasificadas, y explotadas. Para que se tratara de una finalidad lícita se requiere el consentimiento del viajero[66]. Y, en todo caso, debe evitarse el sistema de tarjeta o crédito social, prohibido en el art. 5 Reglamento IA.

La discusión está en la explotación que puede efectuarse de los datos sensibles que se obtienen a través de estas tecnologías biométricas, o si se quiere, los fines pretendidos por quienes realizan estas acciones. En China, por ejemplo, se permite el uso de gafas con reconocimiento facial y ADN, piel, comportamiento de movilidad, etc., para identificar sospechosos (no necesariamente de delitos, sino también de acciones políticamente inapropiadas o contrarias al régimen). En China existe el sistema de crédito social, denominado *scoring,* que es un instrumento que utiliza el *big data* para calificar el comportamiento de los usuarios, de manera que las personas con bajo crédito social tienen prohibido adquirir billetes de tren y de avión; o permiten detectar en las escuelas el absentismo escolar, y en Shangai se habla de incorporar en los autobuses un sistema de reconocimiento facial

64 "EU Interoperability framework for border management systems. Secure, Safe and Resilient Societies", 5 junio 2018, Brussels, European Commission, https://www.securityresearch-cou.eu/sites/default/files/02.Rinkens.Secure%20safe%20societies_EU%20interoperability_4-3_v1.0.pdf. El CIR unificará la información contenida en sistemas como Schengen Information System, Eurodac, Visa Information System (VIS), European Criminal récords System (ECRIS-TCN), Entry/Exit System (EES) y European Travel Information and Authorisation System (ETIAS).

65 Una medida que ya funciona en los principales aeropuertos de EEUU, China, India.

66 Barona Vilar,baroBbb S.: *Algoritmización del derecho y de la justicia*, cit., p. 498.

que detecte la fatiga de los conductores (en algunos automóviles de tecnología avanzada ya existe en Europa). O, en los baños públicos del Cielo de Pekín, se usa una máquina que escanea el rostro del usuario, le dispensa de un trozo de papel higiénico de 60 centímetros de longitud y no le permite volver a usar más hasta que han pasado nueve minutos[67].

En ciertos casos, la vulneración de derechos por el uso de reconocimiento facial sin consentimiento podría justificarse por razones de interés o seguridad públicos, por ejemplo, para la detención de terroristas, como sucedió durante la marathon de Boston en 2013, o en supuestos como, por ejemplo, la búsqueda de desaparecidos[68]. Además, desde el punto de vista de salud, desde el Instituto de Genoma Humano se están utilizando estas técnicas para detectar algunas enfermedades genéticas raras[69].

C) Worldcoin, el proyecto de escaneo del iris a cambio de criptomonedas; un negocio redondo a costa de datos biométricos.

La situación de nebulosa en la que transitamos, a pesar del marco normativo, ha llevado a algunas empresas tecnológicas a aprovechar la coyuntura para "negociar" con los datos biométricos, todo y que amparadas en el "consentimiento". Un ejemplo paradigmático reciente es la prohibición por la Agencia de Protección de datos del denominado Proyecto "Worldcoin" de escaneo del iris. Más de 300.000 personas en nuestro país han participado en el mismo, con la finalidad de crear una identidad digital única, siendo su contraprestación otorgar, por la entidad "Tools for Humanity", "tokens" o criptomonedas WLD, que pueden almacenarse o intercambiarse por dinero u otras criptomonedas a través de Internet. Esta entidad, con sede en San Francisco y en Berlín, fue fundada por el CEO de OpenAI, Sam Altman.

Worldcoin utiliza "orbes" esféricos para escanear el iris de los usuarios, proporcionándoles una identidad digital registrada en la blockchain de Worldcoin, actuando como un registro en el que se almacenan todas las transacciones, saldos e intercambios dentro de la red "Worldcoin"; transacciones que se agrupan en bloques (es algo similar a Bitcoin o Ethereum). Con este sistema se garantiza que en las operaciones económicas hay un humano y no un robot realizando las transacciones.

67 Rubio, I.: "Reconocimiento facial: la tecnología que lo sabe todo", en *El País, 25 de mayo de 2019,* https://elpais.com/tecnologia/2019/05/21/actualidad/1558455279_966010.html?rel=mas.

68 "Indian Police trace 3.000 missing children in just four days using facial recognition Technology", en *Independent, 24 de abril de 2018,* https://www.independent.co.uk/life-style/gadgets-and-tech/news/india-police-missing-children-facial-recognition-tech-trace-find-reunite-a8320406.html. O también en relación con niños desparecidos puede verse http://missingchildreneurope.eu/facts&figures.

69 Barona Vilar,baroBbb S.: *Algoritmización del derecho y de la justicia*, cit., p. 499.

Las dudas éticas y de transparencia del consentimiento han llevado a cuestionar esta acción empresarial, que comporta la recopilación de datos biométricos sensibles, sin garantías respecto de un posible uso indebido y la protección de la información personal, amén del carácter irreversible del intercambio de datos a cambio de criptomonedas, aun cuando la empresa ha manfiestado en diversos momentos que cualquier persona puede revocar el consentimiento sobre sus datos biométricos. A mayor abundamiento, se ha detectado una alta participación de menores de edad en el proyecto sin la debida autorización. Y en muchos casos, los usuarios no tienen claro en qué consiste esa cesión de datos biométricos a partir del escaner del iris (Orb), interesándose tan solo por la contraprestación que se obtiene.

Las derivaciones de esta cesión de datos biométricos, en este caso a través del iris, puede integrar incluso datos acerca de la salud de una persona, lo que podría, si se explotaren o vendieren los datos, derivar en consecuencias tales como no asegurar a la persona por padecer alguna enfermedad o denegarle un transplante por esta misma razón, entre otras.

Se trata, en suma, de la posible obtención de datos biométricos sensibles, con apariencia de consentimiento del donante, todo y que en muchos casos sin que se tenga conocimiento de las consecuencias que pueden derivarse, con enormes líneas rojas que no pueden ni deben traspasarse.

Ante la situación descrita, la Agencia Espanola de Protección de datos ha exigido en marzo de 2024 el cese en la recogida y tratamiento de categorías especiales de datos personales así como el bloqueo de los recopilados. Decisión que fundamenta en el consentimiento insuficiente, la imposibilidad de retirar el consentimiento y en la captación de menores, por lo que solicita el cese inmediato del tratamiento, para prevenir la cesión de datos a terceros y la salvaguarda del derecho funbdamental a la protección de datos personales. Esta prohibición temporal de la actividad en Espana tiene un periodo de validez máximo de tres meses. La medida cautelar se fundamenta en el Reglamento General de Protección de Datos, que considera el tratamiento de los datos biométricos como de especial protección, dados los riesgos y potenciales daños irreparables que conlleva para los derechos de las personas. La decisión de la AEPD fue recurrida a la Audiencia Nacional, quien ha rechazado el recurso, sosteniendo que "ateniendo a la ponderación de los intereses en conflicto y, a la vista de las circunstancias concurrentes, debe prevalecer la salvaguarda del interés general que consiste en la protección de datos personales de los interesados frente al interés particular de la empresa recurrente de contenido fundamentalmente económico"[70].

70 https://www.poderjudicial.es/cgpj/es/Poder-Judicial/Audiencia-Nacional/Oficina-de-Comunicacion/Notas-de-prensa/La-Audiencia-Nacional-avala-el-cese-cautelar-de-la-recopilacion-de-datos-a-traves-del-iris-de-Worldcoin-acordado-por-la-Agencia-de-Proteccion-de-datos.

D) Utilización biométrica en entradas y salidas empresariales y otros fines laborales.

Hemos venido reiterando que los datos biométricos pueden utilizarse solo si son adecuados, pertinentes y no excesivos, ateniendo a la necesidad, propocionalidad de los datos tratados y si la finalidad prevista podría alcanzarse mediante un medio menos intrusivo. Y hemos encontrado exponentes en diversos ámbitos en los que el desarrollo tecnológico, en sentido maximalista, ha ido convirtiendo también el cuerpo humano en una suerte de espacio de computación, lo que favorece e impulsa las posibilidades de control. Precisamente, en el ámbito laboral surgen situaciones cada vez más sofisticadas, en las que la integración de algoritmos, inteligencia artificial y robótica inciden cada vez más, favoreciendo el uso de sistemas biométricos en el mundo del trabajo. En unas ocasiones, para favorecer los registros de la jornada laboral (en el primer estadio se empleaba la huella digital), para ir poco a poco incorporando sistemas de biometría vocal (especialmente en los supuestos de teletrabajo), el control a través de retina o iris o el reconocimiento facial. Incluso se habla en los últimos tiempos del uso de los latidos del corazón como herramienta biométrica. Todos ellos como sistemas de individualización y también de control (por ejemplo, para verificar el cumplimiento de la prestación laboral o incluso para implantar medidas de seguridad frente a riesgos graves)[71].

También en el ámbito laboral el uso o mal uso por el empresario de los sistemas biométricos puede traer consecuencias diversas, y sobre todo debe tomarse en consideración cuanto se ha venido exponiendo sobre la necesidad, proporcionalidad y fines pretendidos. Curiosa es la reciente Sentencia del Juzgado de lo Social n 2 de Alicante 190/2023, de 15 de septiembre (REC 489/2023), que declaró la vulneración del derecho a la intimidad personal y familiar y a la propia imagen del trabajador por la utilización de su información biométrica sin su consentimiento para el fichaje de entrada y salida, condenando a la empresa a una indemnización moral de más de seis mil euros. El trabajador solo había autorizado a la empresa el uso de sus derechos de imagen para publicaciones en páginas web y redes sociales, propiedad de la empresa, campañas, revistas, publicaciones, folletos, publicidad corporativa y demás materiales de apoyo, pertinentes para la difusión y promoción de la actividad de la empresa, pero no había autorizado que la empresa realizara una fotografía de la cara de los empleados desde un dispositivo de "entrea" y que esa imagen fuera usada para fichar la entrada y la salida en el puesto de trabajo; de hecho, el trabajador manifiesta que ni siquiera fue informado del uso de los datos biométricos.

71 Un desarrollo *ad extensum* acerca del uso de estso sistemas biométricos en el mundo laboral y el posible control del empresario, puede verse en Muñoz ruiz, A.B.: *Biometría y sistemas automatizados de reconocimiento de emociones: Implicaciones jurídico-laborales,* Tirant lo Blanch, Valencia, 2023.

En suma, hemos venido reiterando que la tecnología no es buena ni mala, pero es palmario que no es neutra, y el uso de los sistemas biométricos tampoco lo es. El gran dilema de la sociedad actual se halla en ese proletariado digital que nos asiste, en el que hemos aceptado sin resistencia el cambio de moneda: los datos, nuestros datos, personales y no personales, físicos, fisiológicos y conductuales, que concedemos, en muchas ocasiones de forma inconsciente o irreflexiva, a cambio de información, de comodidad, de bienes o de seguridad. Forma parte de la herencia de la globalización, que nos ha venido inoculando *un modus operandi* de masas, acrítico, en el que aceptamos el control, la categorización, los perfiles, la vigilancia predictiva masiva, la efectividad, la inmediatez, a cambio de "nosotros". El uso de este *Big data* se expande a todo, al sector público, al sector privado y al sector empresarial, y muy especialmente con consecuencias en la Justicia, en los principios procesales, en la prueba y en la decisión judicial; Biometría, algoritmos e inteligencia artificial se convierten en un magnífico coctel del eficientismo, si bien... No todo vale.

BIBLIOGRAFÍA

Abs, M.: "Biometrik", en *Historisches Wörterbuch der Philosophie,* (ed. por J. Ritter, J.; K. Gründer; G. Schwabe), AG Verlag, Basel, 1971.

Agencia española de protección de datos: *14 equívocos en relación con la identificación y autenticación biométrica,* 2020, https://www.aepd.es/guias/nota-equivocos-biometria.pdf.

Barona Vilar,baroBbb S.: *Algoritmización del derecho y de la justicia: de la Inteligencia Artificial a la Smart Justic*e, Tirant lo Blanch, Valencia, 2021.

Boulgouris, N. V. et alt.: *Biometrics, Theory, Methods, and Applications*, IEEE and WILEY, Estados Unidos, 2010.

Caneppele, S.; Ribeaux, O.: "Forensic intelligence", *"The Routledge International Handbook of Forensic Intelligence and Criminology",* Routledge, 2017.

Catalina Benavente, M.A.: "La recogida y tratamiento masivo de los datos PNR: algunas cuestiones para preocuparse", en AA.VV.: *Claves de la Justicia Penal. Feminización, Inteligencia Artificial, Supranacionalidad y Seguridad, (*ed. por S. Barona Vilar), Tirant lo Blanch, Valencia, 2019.

Clouston, T. S: "The Developmental Aspects of Criminal Anthropology", *The Journal of the Antropological Institute of Great Britain and Ireland*, vol. 23.

De Miguel, R.; Victoria, M.; Nadal, S.: "Londres instalará cámaras de reconocimiento facial", El País, sábado 25 de enero de 2020.

Díaz Rodríguez, V.: "Sistemas biométricos en materia criminal: un estudio comparado", *Revista IUS vol. 7, núm. 31,* Puebla, enero-junio 2013, en http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-21472013000100003.

Ecured: "Biometría por ADN", en https://www.ecured.cu/Biometr%C3%ADa_por_ADN

Escajedo San Epifanio, L.: *Reconocimiento e Identificación de las personas mediante Biometrías estáticas y dinámicas,* Tesis Doctoral, Alicante, diciembre 2015, *open Access*.

Etxeberría Guridi, J.F.: "Obtención de perfiles de ADN a la luz de la nueva Orden Europea de Investigación (OEI): diversas alternativas", AAVV, *Claves de la Justicia Penal. Feminización, Inteligencia Artificial, Supranacionalidad y Seguridad*, (ed. por S. Barona Vilar), Tirant lo Blanch, Valencia, 2019.

Etxeberría Guridi, J.F.: "Sistemas biométricos (el reconocimiento facial en particular) y sus aplicaciones", AAVV *Inteligencia Artificial y Administración de Justicia*, (dir. por S. Calaza López y M. Llorente Sánchez-Arjona), Thomson Reuters-Aranzadi, Cizur Menor (Navarra), 2022.

Ferrer, C.: "¿Cómo cumplir el RGPD si manejas datos biométricos?", en *https://protecciónd atos-lopd.com/empresas/datos-biometricos-rgpd/,* 9 de julio 2018.

Ferri, E.: *Principios de Derecho Criminal,* Ed. Reus, Madrid, 1933.

Galton, F.: " Spirit of Biometrika", editorial del número primero de la Revista *Biometrika*, 1901.

García, J.G.: "El reconocimiento facial aprende a identificar mascarillas", *Retina, El País Economía,* mayo 2020.

Gargantilla, P.: "Puedes acabar en la cárcel por la huella de tu oreja", publicado el 26 de mayo de 2019 en https://www.abc.es/ciencia/abci-puedes-acabar-carcel-huella-oreja-201905260149_noticia.html

Garófalo, R.: *La criminología. Estudio sobre el delito y sobre la teoría de la represión,* Analecta Editorial, 1900.

González Sánchez, M.E.: *Análisis biométrico de las orejas,* Tesis Doctoral, Departamento de Informática y Sistemas, Universidad de Las Palmas de Gran Canaria, 2008, p. 6, en https://accedacris.ulpgc.es/bitstream/10553/3435/1/Analisis_biometrico_orejas.pdf

Grupo de trabajo de protección de las personas en lo que respecta al tratamiento de datos personales (markt/12168/02/es wp 80): *Documento de trabajo sobre biometría*, adoptado el 1 de agosto de 2003, https://www.informatica-juridica.com/documento-trabajo/documento-trabajo-biometria/.

Grupo de trabajo de protección de las personas en lo que respecta al tratamiento de datos personales: Agencia espanola de protección de datos, *Dictamen 3/2012 sobre la evolución de las tecnologías biométricas* de 27 de abril de 2012 (WP193), https://www.aepd.es/documento/wp193_es.pdf.

Gutiérrez Zarza, A.: "Terrorismo yihadista, crisis migratorias, fronteras, prueba electrónica, encriptado, referéndum y otras palabras clave del espacio LSJ", *Diario La Ley, Sección Tribuna*, núm. 8904, 2016, http://diariolaley.laley.es/home/DT0000240761/20170111/Terrorismo-yihadista-crisis-migratorias-fronteras-prueba-electronica-encriptado-.

Han, B-CH: *En el enjambre,* Herder, Barcelona, 2014.

Instituto nacional de ciberseguridad (incibe): *Tecnologías biométricas aplicadas a la ciberseguridad. Una guía de aproximación para el empresario,* 2016, en https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_tecnologias_biometricas_aplicadas_ciberseguridad_metad.pdf

Jiménez, M.: "Open AI lanza una herramienta de audio capaz de clonar las voces humanas", *El País* 30 de marzo de 2024.

Lasalle, J.M.: *Ciberleviatán*, Ed Arpa, Barcelona, 2019.

Muñoz ruiz, A.B.: *Biometría y sistemas automatizados de reconocimiento de emociones: Implicaciones jurídico-laborales,* Ed. Tirant lo Blanch, Valencia, 2023.

Pérez Colomé, J.: "Marbella, el mayor laboratorio de videovigilancia de España", *El País, 22 de noviembre de 2019*, https://elpais.com/tecnologia/2019/11/21/actualidad/1574348695_231540.html.

Piñar Mañas, J.L.: Recio Gayo, M.: *El derecho a la protección de datos en la jurisprudencia del Tribunal de Justicia de la Unión Europea*, Wolters Kluwer-La Ley, Madrid, 2018.

Planchadell Gargallo, A.: "Inteligencia Artificial y medidas cautelares", en AA.VV.:*Justicia algorítmica y neuroderecho: una mirada multidisciplinar,* (ed. por S. Barona Vilar), Tirant lo Blanch, Valencia, 2021.

Prasanthi Jasmine, K.; Naga Prakash, K.: *Reconocimiento de emociones humanas a partir de imágenes de rostros*, Ed. Nuestro Conocimiento, 2021.

Rallo Lombarte, A.: "El Tribunal de Justicia de la Unión Europea como juez garante de la privacidad en Internet", *UNED. Teoría y Realidad Constitucional*, núm. 39, 2017.

Romero Moreno, M.: *Reconocimiento del Andar Humano basado en ensamble de clasificadores utilizando silueta y contorno*, Tesis de Maestría, Instituto Nacional de Astrofísica, Óptica y Electrónica, Tonantzinla, Puebla, 2008, en https://inaoe.repositorioinstitucional.mx/jspui/bitstream/1009/558/1/RomeroMM.pdf.

Ruane Dawson, M.: *Gait Recognition. Final Report,* Department of Computing Imperial College of Science, Technology and Medicine, Londres, 2002.

RUBIO, I.: "Reconocimiento facial: la tecnología que lo sabe todo", *El País, 25 de mayo de 2019, https://elpais.com/tecnologia/2019/05/21/actualidad/1558455279_966010.html?rel=mas.*

SADIN, E.: *La humanidad aumentada,* Ed Caja Negra, 2017.

STIGLER, S.M.: "The Problematic Unity of Biometrics", Revista *Biometrics*, 2000.

TECNOLOGÍA Y TRATA DE PERSONAS: EL USO DE ALGORITMOS PREDICTIVOS PARA MEJORAR LA DETECCIÓN DE VÍCTIMAS DE TRATA*

TECHNOLOGY AND HUMAN TRAFFICKING: THE USE OF PREDICTIVE ALGORITHMS TO IMPROVE THE DETECTION OF VICTIMS OF TRAFFICKING

Actualidad Jurídica Iberoamericana Nº 21, agosto 2024, ISSN: 2386-4567, pp. 332-359

* Este trabajo ha sido escrito en el marco del proyecto de investigación "Claves para una justicia digital y algorítmica con perspectiva de género" (expediente: PID2021-123170OB-I00), financiado por el Ministerio de Ciencia e Innovación de España.

Agradezco enormemente y con mucho cariño a Elisa Simó Soler, por sus comentarios, sugerencias e intercambios de ideas, sin los cuales este artículo no hubiera sido posible.

María
BARRACO

ARTÍCULO RECIBIDO: 29 de mayo de 2023
ARTÍCULO APROBADO: 1 de julio de 2024

RESUMEN: Existen diversas barreras que obstaculizan la correcta identificación de las víctimas de trata de personas. Ello implica, por un lado, una posible violación de los Estados respecto a sus obligaciones internacionales, así como también un deficiente acceso de las víctimas a una justicia adecuada, asistencia y protección. Este artículo busca responder la siguiente pregunta: ¿podría utilizarse la tecnología para superar estas barreras y mejorar la detección de víctimas? Para ello, se explora la posibilidad de implementar un sistema similar a VioGén implementado en España para casos de violencia de género, mediante el empleo de un algoritmo predictivo que permita automatizar el riesgo de que una persona sea víctima de trata. El artículo concluye afirmando que un sistema de estas características tiene un gran potencial para mejorar la identificación de las víctimas, siempre y cuando tenga en cuenta los riesgos que el uso de la tecnología entraña.

PALABRAS CLAVE: Trata de personas; derechos humanos; tecnología; algoritmos predictivos, Sistema VioGén.

ABSTRACT: *There are various barriers preventing the correct identification of victims of human trafficking. This would imply, on one hand, a potential violation of the international obligations of the States, as well as a poor access for victims to an adequate access to justice, assistance, and protection. This article aims to answer the following question: can technology be used to overcome these barriers and improve the detection of victims? To this end, the use of a system similar to VioGén implemented in Spain for cases of gender violence is explored, through the use of a predictive algorithm that allows the automatization of the risk of a person being a victim of human trafficking. The article concludes by affirming that a system with these characteristics has a great potential to improve the identification of victims, as long as it takes into consideration the risks that using technology entail.*

KEY WORDS: *Human trafficking; human rights; technology; predictive algorithms; System VioGén.*

SUMARIO.- I. INTRODUCCION: TRATA DE PERSONAS Y LAS BARRERAS EN LA DETECCIÓN DE CASOS. II. EL USO DE ALGORITMOS PREDICTIVOS PARA MEJORAR LA DETECCIÓN DE VÍCTIMAS DE TRATA DE PERSONAS.- 1. Obligaciones en materia de derechos humanos.- 2. La propuesta de un algoritmo predictivo para identificar de manera preventiva y temprana a las víctimas de trata de personas.- *A) Algoritmos predictivos para detectar riesgos: repensar el modelo de VioGén para los casos de trata de personas.- B) El formulario y sus indicadores, los riesgos asociados y las medidas estatales a adoptar.*- 3. La utilización del sistema algorítmico en la práctica: una aproximación a los desafíos y las oportunidades.- III. REFLEXIONES FINALES.

I. INTRODUCCION: TRATA DE PERSONAS Y LAS BARRERAS EN LA DETECCIÓN DE CASOS.

La trata de personas es un delito que se encuentra definido en el artículo 3 del Protocolo para prevenir, reprimir y sancionar la trata de personas, especialmente mujeres y niños (Protocolo de Palermo),[1] y comprende:

"la captación, el transporte, el traslado, la acogida o la recepción de personas, recurriendo a la amenaza o al uso de la fuerza u otras formas de coacción, al rapto, al fraude, al engaño, al abuso de poder o de una situación de vulnerabilidad o a la concesión o recepción de pagos o beneficios para obtener el consentimiento de una persona que tenga autoridad sobre otra, con fines de explotación. Esa explotación incluirá, como mínimo, la explotación de la prostitución ajena u otras formas de explotación sexual, los trabajos o servicios forzados, la esclavitud o las prácticas análogas a la esclavitud, la servidumbre o la extracción de órganos".

Es decir, el delito de trata de personas está compuesto por tres elementos: (i) una acción (tal como la captación o el transporte); (ii) un medio comisivo (amenaza o uso de la fuerza, entre otros); y (iii) una finalidad de explotación (por ejemplo, la explotación sexual).[2] [3] Este último elemento indica que no es necesario que la explotación en sí ocurra, ya que solamente se requiere que exista una finalidad de explotación en la intención de la persona que cometió el delito.[4]

1 Este Protocolo complementa la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional.

2 Gallagher, A.: *The International Law of Human Trafficking*, CUP, Nueva York, 2010, p. 29.

3 De conformidad con el artículo 3.c del Protocolo, si la víctima es un niño/a de menos de 18 años, entonces se configurará el delito de trata de personas únicamente con la presencia de dos elementos: la acción y la finalidad de explotación.

4 UNODC, "Manual sobre la lucha contra la trata de personas para profesionales de la justicia penal", *Naciones Unidas*, 2010, p. 5, disponible en: https://www.unodc.org/documents/congress/background-information/Human_Trafficking/TIP_Manual_es_module_01.pdf, último acceso 17 de abril de 2024.

• María Barraco
Abogada por la Universidad de Buenos Aires (UBA). Magíster en Derechos Humanos por la Universidad Queen Mary de Londres (QMUL)

El artículo 3 del Protocolo de Palermo enumera algunos ejemplos que se encuentran comprendidos dentro de la finalidad de explotación, incluyendo a la esclavitud, la servidumbre, y las formas análogas a la esclavitud. A pesar de que el concepto de "explotación" no se encuentra definido, la Corte Interamericana de Derechos Humanos (Corte IDH) entendió en el caso *Ramírez Escobar vs. Guatemala* que si bien no se cuenta con una lista exhaustiva con las finalidades de explotación, hay algunos elementos que permiten comprenderlas. Por ejemplo, la Corte IDH afirmó que en la explotación se le atribuye un valor a una persona, el cual es convertido en un beneficio propio a través de la cosificación.[5]

Actualmente, existen aproximadamente 50 millones de personas víctimas de algún tipo de esclavitud moderna – concepto que incluye el delito de trata de personas, así como otras formas de explotación.[6] Si bien esta cifra pone de manifiesto la gran cantidad de personas que están siendo víctimas de estos delitos, la Oficina de Naciones Unidas contra la Droga y el Delito (UNODC) afirmó recientemente en su Informe Mundial sobre Trata de Personas 2022 que se observa una disminución en las víctimas de trata de personas identificadas, ocasionado por la dificultad de detectar este delito.[7] La UNODC también reconoció que las barreras en la identificación fueron exacerbadas por la pandemia de la COVID-19.[8]

Al margen de las dificultades específicas que surgieron a raíz de la pandemia, tal como la disminución en la denuncia de casos o las cuarentenas que dificultaron la investigación,[9] la realidad es que la identificación de las víctimas continúa siendo

5 Específicamente, la Corte IDH afirma que: "[…] las formas de explotación que generalmente se incluyen de manera expresa, evidencian que la finalidad de explotación implica que el traficante realice el acto con el objetivo de utilizar una persona de manera abusiva para su propio beneficio. De esta manera, se atribuye un valor al individuo, por ejemplo por medio de su mano de obra, para después convertirlo en un beneficio propio, bajo condiciones abusivas e injustas o fraudulentas, beneficio que es el resultado de la cosificación o comercialización del mismo individuo." Corte IDH. *Caso Ramírez Escobar y otros vs. Guatemala*. Fondo, Reparaciones y Costas. Sentencia de 9 de marzo de 2018. Serie C No. 351, párr. 31

6 ILO, OIM y Walk Free Foundation, "Global Estimates of Modern Slavery: Forced Labour and Forced Marriage", *ILO*, 2022, pp. 1 y 13, disponible en: https://www.ilo.org/wcmsp5/groups/public/---ed_norm/---ipec/documents/publication/wcms_854733.pdf, último acceso 17 de abril de 2024.

7 UNODC, "Global Report on Trafficking in Persons", *Naciones Unidas*, 2022, pág. III, disponible en: https://www.unodc.org/documents/data-and-analysis/glotip/2022/GLOTiP_2022_web.pdf, último acceso 17 de abril de 2024. Puede consultarse un resumen en español, disponible en: https://www.unodc.org/lpomex/uploads/documents/Publicaciones/Crimen/GLOTiP_Executive_Report_Final_Esp.pdf, último acceso 17 de abril de 2024.

8 UNODC, "Impact of the Covid-19 Pandemic on Trafficking in Persons", *Naciones Unidas*, p. 1, disponible en: https://www.unodc.org/documents/Advocacy-Section/HTMSS_Thematic_Brief_on_COVID-19.pdf, último acceso 17 de abril de 2024. De manera similar, ver, por ejemplo: OSCE Office for Democratic Institutions and Human Rights (ODIHR) and The United Nations Entity for Gender Equality and the Empowerment of Women (UN Women), "Guidance: Addressing Emmerging Human Trafficking Trends and Consequences of the Covid-19 Pandemic", *OSCE*, 2020, disponible en: https://www.osce.org/files/f/documents/2/a/458434_4.pdf, último acceso 17 de abril de 2024.

9 UNODC, "The Effects of the COVID-19 Pandemic on Trafficking in Persons and Responses to the challenges", *Naciones Unidas*, 2021, p. 26, disponible en: https://www.unodc.org/documents/human-trafficking/2021/The_effects_of_the_COVID-19_pandemic_on_trafficking_in_persons.pdf, último acceso 17 de abril de 2024.

un gran obstáculo en la práctica.[10] Además de ser un delito oculto,[11] existen múltiples barreras estructurales que impiden una correcta identificación de las víctimas de trata. Entre ellas, podemos mencionar las limitaciones que pueda tener la víctima en reconocerse como tal y denunciar el delito debido a, entre otros, el miedo a sufrir amenazas por parte de los/as tratantes o a sufrir estigma social.[12] También existen los mitos alrededor de la trata de personas,[13] a los cuales se les suma la falta de capacitación, pudiendo ocasionar que los/as funcionarios/as públicos/as y operadores/as estatales no identifiquen a una víctima si no cumple con ciertos parámetros. Identificar a las víctimas es clave, ya que garantiza que el Estado cumpla con sus obligaciones estatales, incluyendo investigar el delito y sancionar a los/as responsables, así como asistir y reparar a la víctima. Sin una correcta identificación, es muy probable que la víctima de trata continúe viendo vulnerados sus derechos,[14] o sea confundida con una migrante irregular y sufra, por ejemplo, la expulsión del país de que se trate.[15]

En este contexto, se hace primordial encontrar una herramienta que permita superar estas barreras y mejorar la detección de víctimas, lo que a su vez mejorará el acceso de las víctimas a la asistencia, a la justicia y a la obtención de una reparación que sea acorde a los estándares de derechos humanos. Según un informe presentado en 2023 por el Relator Especial de Naciones Unidas sobre las formas contemporáneas de la esclavitud, incluidas sus causas y consecuencias, Tomoya Obokata, la tecnología -incluyendo la inteligencia artificial ('IA') - puede ser una herramienta útil a la hora de luchar contra la esclavitud moderna, y de identificar a sus víctimas.[16] En este escenario, cabe preguntarse: ¿podría utilizarse la tecnología para superar estas barreras y mejorar la detección de víctimas?

10 Informe de la Sra. María Grazia Giammarinaro, Relatora Especial sobre la trata de personas, especialmente mujeres y niños, UN.Doc./A/70/260, *Naciones Unidas*, 2015, párr. 24.

11 UNODC, "Cuestiones probatorias en casos de trata de personas", *Naciones Unidas*, 2017, p. vii, disponible en: https://www.unodc.org/documents/human-trafficking/2021/Cuestiones_Probatorias_en_Casos_de_Trata_de_Personas._Case_Digest.pdf, último acceso 17 de abril de 2024.

12 UNODC, "Identification of Victims", *Naciones Unidas*, disponible en: https://www.unodc.org/e4j/en/tip-and-som/module-8/key-issues/identification-of-victims.html#:~:text=Even%20if%20a%20person%20is,community%20and%20even%20social%20exclusion, último acceso 17 de abril de 2024.

13 American Bar Association, "Voices for Victims: Lawyers Against Human Trafficking Tool Kit for Bar Associations", (2013). Este documento es citado por Naciones Unidas, en: UNODC, "Misconceptions regarding trafficking in persons", *Naciones Unidas*, disponibles en: https://www.unodc.org/e4j/en/tip-and-som/module-6/key-issues/misconceptions-regarding-trafficking-in-persons.html#:~:text=Initial%20consent%20to%20commercial%20sex,be%20a%20victim%20of%20trafficking, último acceso 17 de abril de 2024.

14 Informe del Alto Comisionado de las Naciones Unidas para los Derechos Humanos al Consejo Económico y Social, "Principios y Directrices recomendados sobre los derechos humanos y la trata de personas", UN Doc. E/2002/68/Add.1, *Naciones Unidas*, 2022, Directriz 2.

15 UNODC, "Identification of Victims", *Naciones Unidas*, disponible en: https://www.unodc.org/e4j/en/tip-and-som/module-8/key-issues/identification-of-victims.html, último acceso 17 de abril de 2024.

16 Informe del Relator Especial sobre las formas contemporáneas de la esclavitud, incluidas sus causas y consecuencias, Tomoya Obokata, U.N.Doc./A/78/161, *Naciones Unidas*, 2023, párr. 36.

Este artículo busca abordar esta pregunta, a través de una estructura que se divide en tres partes. En un primer apartado, se hará referencia a las obligaciones de derechos humanos en materia de trata de personas, haciendo énfasis en la obligación de investigar de manera adecuada el delito y de identificar a las víctimas. También se mencionará el rol que tienen las empresas en detectar a las víctimas de trata de personas que puedan existir en las cadenas de producción ("supply chains"). En una segunda parte, se propondrá un sistema que utilice algoritmos predictivos para automatizar el riesgo de que una persona sea víctima de trata, inspirado en el Sistema VioGén. En esta sección también se diseñará el formulario que podría utilizarse, se determinarán los riesgos y se identificarán las medidas estatales que deberían articularse según el riesgo identificado. En una tercera parte, se brindará una aproximación a las ventajas y desafíos de contar con este sistema. El artículo concluye afirmando que un sistema como el aquí propuesto puede ser una buena herramienta para mejorar la identificación de víctimas y superar las barreras existentes en la investigación, siempre y cuando se tengan en cuenta (y se aborden de manera adecuada) los riesgos que su propio uso entraña.

II. EL USO DE ALGORITMOS PREDICTIVOS PARA MEJORAR LA DETECCIÓN DE VÍCTIMAS DE TRATA DE PERSONAS.

1. Obligaciones en materia de derechos humanos.

Además de ser un delito definido en el Protocolo de Palermo, la prohibición de cometer el delito de trata de personas está contenida en diversos tratados internacionales de derechos humanos. Entre ellos, se encuentra: el artículo 8 del Pacto Internacional de Derechos Civiles y Políticos (PIDCP);[17] el artículo 6 de la Convención sobre la Eliminación de todas las Formas de Discriminación contra la Mujer (CEDAW);[18] el artículo 32 de la Convención de Naciones Unidas sobre los Derechos del Niño;[19] el artículo 5 de la Carta Africana sobre los Derechos Humanos y de los Pueblos;[20] el artículo 6 de la Convención Americana sobre Derechos Humanos (CADH);[21] el artículo 4 de la Convención Europea de

17 UN General Assembly, *International Covenant on Civil and Political Rights*, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171.

18 UN General Assembly, *Convention on the Elimination of All Forms of Discrimination Against Women*, 18 December 1979, United Nations, Treaty Series, vol. 1249, p. 13.

19 UN General Assembly, *Convention on the Rights of the Child*, 20 November 1989, United Nations, Treaty Series, vol. 1577, p. 3.

20 Organización para la Unión Africana (OUA), Carta Africana de Derechos Humanos y de los Pueblos, 27 Junio 1981, CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982).

21 Organización de los Estados Americanos (OEA), *Convención Americana sobre Derechos Humanos, Costa Rica*, 22 Noviembre 1969.

Derechos Humanos (CEDH);[22] y el Convenio del Consejo de Europa sobre la lucha contra la trata de seres humanos.[23]

Que la prohibición de trata de personas esté contemplada en distintas convenciones de derechos humanos no es menor, ya que el Protocolo de Palermo no es una convención de derechos humanos.[24] Es por ello que, a la hora de analizar las obligaciones estatales en materia de derechos humanos vinculadas al delito de trata de personas, también habrá que considerar los tratados internacionales de derechos humanos mencionados anteriormente. Asimismo, abordar este delito con un enfoque de derechos humanos permite reconocer que la trata de personas es una violación de derechos humanos,[25] ubica a la víctima en el centro de cualquier acción que realice el Estado,[26] y promueve un enfoque holístico que fortalece la prevención y la lucha contra la trata.[27]

Existen distintas obligaciones estatales de derechos humanos vinculadas a la prohibición de trata de personas. Una de ellas es la de prevenir la trata de personas, por ejemplo, abordando los factores que aumentan la vulnerabilidad de las personas a ser víctimas de trata (tal como la desigualdad y la pobreza),[28] o adoptando "medidas preventivas en casos específicos en los que es evidente que determinados grupos de personas pueden ser víctimas de trata".[29] La obligación de prevención también incluye la de contar con un marco legislativo adecuado que criminalice a la trata de personas.[30] También se recomienda que los Estados

22 Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14*, 4 November 1950, ETS 5.

23 Council of Europe, *Council of Europe Convention on Action Against Trafficking in Human Beings*, 16 May 2005, CETS 197.

24 Piotrowicz, R. y Redpath-Cross, J.: "Human trafficking and smuggling", en AA.VV.: *Foundations of International Migration Law*, (ed. por B. Opeskin), CUP, Nueva York, 2012, p. 283.

25 Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (ACNUDH), "Principios y Directrices recomendados sobre derechos humanos y trata de personas", *Naciones Unidas*, 2018, p. 3, disponible en: https://acnudh.org/wp-content/uploads/2018/07/Principios-y-Directrices-recomendados-sobre-derechos-humanos-y-trata-de-personas.pdf, último acceso 17 de abril de 2024.

26 OHCHR, "Human Rights based approach to trafficking", *Naciones Unidas*, 2011, disponible en: https://www.ohchr.org/en/stories/2011/11/human-rights-based-approach-trafficking#:~:text=The%20human%20rights%20based%20approach,violations%20in%20the%20trafficking%20cycle, último acceso 17 de abril de 2024.

27 Obokata, T.: "A Human Rights Framework to Address Trafficking of Human Beings", 24 *Netherlands Quarterly of Human Rights*, 2006, vol. 24, p. 384.

28 ACNUDH, "Principios y Directrices", cit., p. 110.

29 Corte IDH. *Caso Trabajadores de la Hacienda Brasil Verde Vs. Brasil*. Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 20 de octubre de 2016. Serie C No. 318, párr. 320.

30 Tribunal Europeo de Derechos Humanos (TEDH), *Caso V.C.L. & A.N. v. the United Kingdom*, 16 de febrero de 202, apps. nos. 77587/12 and 74603/12, párr. 151; Corte IDH, *Caso Trabajadores*, cit., párr. 319.

dispongan de una línea telefónica gratuita para denunciar casos[31] y realicen campañas de prevención.[32]

Otra de las obligaciones estatales está vinculada con la investigación del delito. Esta investigación debe ser efectiva,[33] y debe conducir a la identificación y posterior sanción de las personas responsables.[34] La investigación deberá emprenderse de manera urgente en aquellos casos en los cuales "exist[a] la posibilidad de rescatar a las personas de la situación denunciada".[35] Además, el Estado deberá investigar de oficio si existe una denuncia o razón fundada para creer que una persona está siendo víctima de trata de personas.[36] El deber de investigación también incluye la obligación "realizar inspecciones u otras medidas de detección de dichas prácticas".[37]

Por otra parte, los Estados tienen la obligación de asistir, proteger y reparar a las víctimas de trata,[38] lo que incluye la prestación de asistencia física y psicológica.[39] Esta obligación también incluye la de garantizar la seguridad física de las víctimas y otorgarles asistencia legal (en un idioma que la víctima pueda comprender), respetando siempre su intimidad.[40]

Finalmente, y vinculado con el tema del presente artículo, los Estados tienen la obligación de identificar a las víctimas.[41] Dentro de las medidas que pueden llevar a cabo los Estados para mejorar la detección, se puede mencionar la elaboración de instrumentos que faciliten la identificación de víctimas y la capacitación del funcionariado fronterizo y agentes policiales.[42] Como ya se ha explicado previamente, la identificación de las víctimas de trata de personas es clave: ello, debido a que "de no identificar rápida y correctamente a las víctimas de la trata

31 OHCHR, "Preliminary findings, UN Special Rapporteur on Trafficking in persons, especially women and children, Maria Grazia Giammarinaro Visit to Malaysia (23 -28 February 2015)", *Naciones Unidas*, 2015, disponible en: https://www.ohchr.org/en/statements/2015/03/preliminary-findings-un-special-rapporteur-trafficking-persons-especially-women, último acceso 17 de abril de 2024.

32 Organización Internacional para las Migraciones (OIM), "Sustento Teórico para la Prevención de la Trata de Personas y el Tráfico Ilícito de Migrantes, *OIM*, 2017, p.15, disponible en: https://ecuador.iom.int/sites/g/files/tmzbdl776/files/documents/ST_TdP_TIM.pdf, último acceso 17 de abril de 2024.

33 Corte IDH, *Caso Trabajadores*, cit., párr. 319.

34 ACNUDH, "Los Derechos Humanos y la Trata de Personas. Folleto Informativo No. 36", *Naciones Unidas*, 2014, pág. 65, disponible en: https://www.ohchr.org/sites/default/files/Documents/Publications/FS36_sp.pdf, último acceso 17 de abril de 2024.

35 Corte IDH, *Caso Trabajadores*, cit., párr. 364; TEDH, *Caso Rantsev Vs. Chipre y Rusia*, 7 de enero de 2010, app. No. 25965/04, párr. 288.

36 Corte IDH, *Caso Trabajadores*, cit., párr. 319.

37 Ibid.

38 TEDH, *Caso Krachunova v. Bulgaria*, app. No. 18269/18, párr. 158 & 173; Corte IDH, *Caso Trabajadores*, cit., párr. 319; ACNUDH, "Los Derechos Humanos", cit., p. 15 y 34.

39 ACNUDH, "Principios y Directrices", cit., p. 149.

40 ACNUDH, "Principios y Directrices", cit., p. 133 y 156.

41 Corte IDH, *Caso Trabajadores*, cit., párr. 364; TEDH, *Caso Rantsev*, cit., párr. 233.

42 ACNUDH, "Los Derechos Humanos", cit., p. 13.

de personas hace que cualquier derecho que se reconozca a esas personas sea "puramente teórico e ilusorio".[43]

Más allá de las obligaciones que tienen los Estados, también las empresas tienen ciertas responsabilidades vinculadas a la trata y explotación de personas. Los Principios Rectores sobre las Empresas y los Derechos Humanos de las Naciones Unidas – también llamados "Principios de Ruggie"- reconocen que las empresas tienen la responsabilidad de respetar los derechos humanos, lo que implica el deber de evitar "consecuencias negativas sobre los derechos humanos", así como el deber de prevenir y mitigar dichas consecuencias.[44] Si bien estos principios no son vinculantes, los mismos analizan prácticas estatales y empresariales, así como legislaciones nacionales e internacionales.[45]

Específicamente respecto de la prohibición de trata de personas, las empresas tienen ciertas obligaciones. Por ejemplo, existen diversas legislaciones nacionales dictadas recientemente que requieren que las empresas realicen dictámenes periódicos detallando los riesgos de esclavitud moderna en sus cadenas de producción y las acciones realizadas para mitigar estos riesgos.[46] También la Corte IDH ha delineado ciertas obligaciones estatales vinculadas a las empresas, tal como la obligación de fiscalizar y supervisar las actividades empresariales con el objetivo de detectar las condiciones laborales de los y las trabajadoras,[47] o realizar inspecciones para detectar casos de trata de personas.[48]

En el ámbito de la Unión Europea ("UE"), el Consejo y el Parlamento Europeo llegaron a un acuerdo a fines del 2023 respecto de la "Directiva sobre diligencia debida de las empresas en materia de sostenibilidad", con diversas normas vinculantes que las empresas deberán cumplir en materia de derechos humanos.[49] Esta legislación fue aprobada por el Consejo de la UE el 15 de Marzo de 2024, cuyo texto incluye en su artículo 4 una obligación de debida diligencia que implica que los Estados deberán velar por que las empresas detecten, prevengan y mitiguen

43 ACNUDH, "Principios y Directrices", cit., p. 75.

44 ACNUDH, "Principios Rectores sobre las Empresas y los Derechos Humanos", HR/PUB/11/04, *Naciones Unidas*, 2011, pp. 16 y 17, disponible en: https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_sp.pdf, último acceso 17 de abril de 2024.

45 ACNUDH, "La Responsabilidad de las Empresas de Respetar los Derechos Humanos", *Naciones Unidas*, 2012, disponible en: https://www.ohchr.org/sites/default/files/Documents/Publications/HR.PUB.12.2_sp.pdf, último acceso 17 de abril de 2024.

46 Entre ellas: Canadian Fighting Against Forced Labour and Child Labour in Supply Chains Act (Bill S-211); Australia, Modern Slavery Act (2018); UK, Modern Slavery Act (2015).

47 Corte IDH. *Caso de los Buzos Miskitos (Lemoth Morris y otros) Vs. Honduras*. Sentencia de 31 de agosto de 2021. Serie C No. 432, párr. 77.

48 Corte IDH, *Caso Trabajadores*, cit., párr. 319.

49 Consejo de la Unión Europea, "Directiva sobre diligencia debida de las empresas en materia de sostenibilidad: el Consejo y el Parlamento alcanzan un acuerdo para proteger el medio ambiente y los derechos humanos", 2023, disponible en: https://www.consilium.europa.eu/es/press/press-releases/2023/12/14/corporate-sustainability-due-diligence-council-and-parliament-strike-deal-to-protect-environment-and-human-rights/, último acceso 17 de abril de 2024.

los "efectos adversos reales o potenciales" sobre los derechos humanos.[50] De conformidad con el Anexo, dichos efectos incluyen la prohibición de la trata de personas. Si bien la Directiva adolece de ciertas críticas, como el hecho de que no aplique a pequeñas y medianas empresas,[51] es un gran avance en esta materia, ya que cristalizará – al menos en el ámbito de la UE – una serie de obligaciones en materia de trata de personas que las empresas deberán cumplir.

2. La propuesta de un algoritmo predictivo para identificar de manera preventiva y temprana a las víctimas de trata de personas.

A) Algoritmos predictivos para detectar riesgos: repensar el modelo de VioGén para los casos de trata de personas.

A los efectos de este artículo, consideraré la definición del artículo 3 del Reglamento del Parlamento y del Consejo en materia de IA, el cual entiende a un sistema de IA como "el software que se desarrolla empleando una o varias de las técnicas y estrategias que figuran en el anexo I[52] y que puede, para un conjunto determinado de objetivos definidos por seres humanos, generar información de salida como contenidos, predicciones, recomendaciones o decisiones que influyan en los entornos con los que interactúa".[53] La IA puede incluir la creación de algoritmos complejos que permitan obtener determinados resultados.[54]

Se entenderá por algoritmo a la "secuencia de instrucciones que conducen a la resolución de un problema".[55] La IA también incluye el machine learning ("ML"), el cual supone "el desarrollo de algoritmos que analizan información

50 Como indica el considerando 21, las empresas que deberán cumplir son las empresas de la UE con más de 500 trabajadores por término medio y un volumen de negocios neto mundial superior a 150 millones EUR en el ejercicio anterior al último ejercicio deben estar obligadas a cumplir con la diligencia debida. Es decir, las pequeñas y medianas empresas no están incluidas. Para más información sobre el ámbito de aplicación, ver, por ejemplo: Comisión Europea, "Economía justa y sostenible: la Comisión establece normas para que las empresas respeten los derechos humanos y el medio ambiente en las cadenas de suministro mundiales", 2022, disponible en: https://ec.europa.eu/commission/presscorner/detail/es/ip_22_1145, último acceso 17 de abril de 2024.

51 OHCHR, "EU Corporate Due Diligence Directive must be strengthened and prevent trafficking: UN expert", *Naciones Unidas*, 2023, disponible en: https://www.ohchr.org/en/statements/2023/04/eu-corporate-due-diligence-directive-must-be-strengthened-and-prevent, último acceso 17 de abril de 2024; Anti-Slavery International, "Landmark due diligence legislation agreed in the EU", 2023, disponible en: https://www.antislavery.org/latest/landmark-due-diligence-legislation-agreed-eu/, último acceso 17 de abril de 2024.

52 Este anexo menciona, por ejemplo, ciertas estrategias de aprendizaje automático y estrategias estadísticas.

53 Comisión Europea, *Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión*, COM(2021) 206 final, Bruselas, 21 de abril de 2021.

54 Sourdin, T.: "Judge v Robot? Artificial Intelligence and Judicial Decision-making", *UNSW Law Journal*, 2018, vol. 41, p. 1116.

55 Simó Soler, E. y Rosso, P.: "Inteligencia artificial y derecho: entre el mito y la realidad", *Diario La Ley*, 2022, núm. 9982, p. 6.

datificada, reconocen patrones y aprenden de los datos en un proceso llamado «entrenamiento» para proporcionar apoyo a la toma de decisiones."[56]

La IA, en sus diversas formas, ha comenzado a utilizarse en distintas áreas del derecho. Esta "algoritmización" de la justicia se manifiesta en diversos ámbitos y para cumplir funciones variadas, tal como lo evidencia el sistema de algoritmos diseñado por la Universidad de Londres en 2016 para predecir los resultados de determinadas sentencias del Tribunal Europeo de Derechos Humanos.[57] Vinculado específicamente con el tema de este artículo, el uso de la IA y de los algoritmos también están siendo aplicados para identificar a las víctimas de trata de personas.[58] En su reporte, el Relator Especial de Naciones Unidas, Tomoya Obokata, menciona como un buen ejemplo del uso de la IA y del análisis de datos para facilitar la identificación de víctimas a la aplicación Traffic Jam. **[59]** Esta herramienta utiliza ML para analizar datos disponibles en internet, y así detectar patrones de trata de personas,[60] logrando la identificación de alrededor de 6.800 víctimas de trata con fines de explotación sexual desde el año 2018.[61]

Tomoya Obokata también explica que "los algoritmos de inteligencia artificial son capaces de detectar posibles indicadores de prácticas similares a la esclavitud, como condiciones laborales de explotación, servidumbre por deudas o rutas de trata de seres humanos."[62] En efecto, lo que se busca explorar en este apartado es mejorar la identificación de las víctimas de trata mediante la automatización del riesgo; para ello se propone la utilización de algoritmos predictivos que determinen el riesgo de que una persona esté siendo víctima de trata.

Un modelo parecido ya fue implementado en España, aunque aplicado a casos de violencia de género. El Sistema de Seguimiento Integral en los casos de Violencia de Género ("Sistema VioGén") fue puesto en funcionamiento por la Secretaría de Estado de Seguridad del Ministerio del Interior de España en el año 2007,[63] y

56 Ibid, p. 2.

57 Barona Vilar, S.: "Inteligencia Artificial o la Algoritmización de la vida y de la justicia: ¿solución o problema?", *Revista boliviana de Derecho de Derecho*, 2019, núm. 28, pp. 37 y 42.

58 Vicario Pérez, A.M.: "Sobre la criminalidad organizada y la trata de seres humanos. Especial referencia al uso de la inteligencia artificial en la identificación de las víctimas", en AA.VV.: *La Justicia en la Sociedad 4.0: Nuevos Retos para el Siglo XXI* (dir. por L. Fontestad Portalés y P.R. Suárez Xavier), Colex, A Coruña, 2023, p. 267; Tomoya Obokata, U.N.Doc./A/78/161, cit., párr. 15.

59 Tomoya Obokata, U.N.Doc./A/78/161, cit., párr. 19.

60 Office of the Special Representative and Co-ordinator for Combating Trafficking in Human Beings, "Leveraging innovation to fight trafficking in human beings: A comprehensive analysis of technology tools", *OSCE*, 2020, p. 45, disponible en: https://www.osce.org/files/f/documents/9/6/455206_1.pdf, último acceso 17 de abril de 2024.

61 Traffic Jam, "AI Solution to fight human trafficking", disponible en: https://static1.squarespace.com/static/53a47a8fe4b0bbc19776ffdf/t/6038212d9b6c5e1848bc76de/1614291247928/TRAFFIC+JAM+BROCHURE+2021.pdf, último acceso 17 de abril de 2024.

62 Tomoya Obokata, U.N.Doc./A/78/161, cit., párr. 15.

63 Disponible en: https://www.interior.gob.es/opencms/es/servicios-al-ciudadano/violencia-contra-la-mujer/sistema-viogen/ , último acceso 17 de abril de 2024.

tiene entre sus características ser un sistema informático (al estar disponible solo en versión online) y multiagencial (ya que vincula a diversos agentes estatales, tal como la policía y el sistema judicial).[64] Partiendo de la base de que puede predecirse el riesgo de reincidencia de violencia contra la pareja a partir de ciertos factores de riesgo,[65] el Sistema Viogén tiene entre sus objetivos: "[f]acilitar la labor preventiva, emitiendo avisos, alertas y alarmas, a través de un subsistema de notificaciones automatizadas, cuando se detecte alguna incidencia o acontecimiento que pueda poner en peligro la integridad de la víctima"; y "[a]tendiendo al nivel de riesgo, proporcionar el seguimiento y, si es preciso, la protección a las víctimas, en todo el territorio nacional".[66]

A partir de la cumplimentación de un formulario que busca identificar indicadores de riesgo en el caso en concreto, el sistema determina un riesgo que acarrea acciones estatales acordes a dicho riesgo. El Sistema VioGén utiliza dos tipos de formularios:[67] (1) el formulario de Valoración Policial del Riesgo (VPR4.0) diseñado para evaluar el riesgo inicial[68] y valorar el riesgo de manera expedita,[69] está compuesto de 39 indicadores de riesgo agrupados en 4 dimensiones (historia de violencia, factores relacionados con el agresor, factores relacionados con la vulnerabilidad de la víctima y con la calidad de la relación, autopercepción de la víctima sobre la situación); y (2) el formulario de Valoración Policial de la Evolución del Riesgo (VPER4.0) diseñado para re-evaluar ese riesgo,[70] está compuesto de 43 indicadores de riesgo agrupados en 5 dimensiones (las mismas mencionadas anteriormente, junto con la dimensión de indicadores dinámico-relacionales). Los formularios integran una gran cantidad de indicadores, ya que buscan "una correcta y amplia valoración del riesgo de violencia".[71] A su vez, los formularios contienen casillas que se completan con «sí», «no», «no se sabe», permitiendo así "una codificación con elementos booleanos para el desarrollo de algoritmos predictivos".[72]

A la hora de dar valor a cada uno de los indicadores, el Sistema VioGén tiene en cuenta que "la exposición conjunta a dos o más indicadores puede conducir a un

64 López-Ossorio, J.J.; González-Álvarez, J.L. y Muñoz Rivas, M.: *La valoración policial del riesgo de violencia contra la mujer pareja en España – Sistema VioGén*, Ministerio del Interior. Gobierno de España, Madrid, 2018, p. 44.

65 López-Ossorio, J.J.; González-Álvarez, J.L. y Andrés-Pueyo, A.: "Eficacia predictiva de la valoración policial del riesgo de la violencia de género", *Psychosocial Intervention*, 2016, núm. 25, p. 2.

66 López-Ossorio, J.J.; González-Álvarez, J.L. y Muñoz Rivas, M.: *La valoración policial*, cit., p. 43.

67 Martínez García, E.; Borges Blázquez, R. y Simó Soler, E.: "Inteligencia artificial y perspectiva de género en la justicia penal", *Diario La Ley*, 2021, núm. 47, p. 8.

68 López-Ossorio, J.J.; González-Álvarez, J.L. y Muñoz Rivas, M.: *La valoración policial*, cit., p. 55.

69 López-Ossorio, J.J.; González-Álvarez, J.L. y Andrés-Pueyo, A.: "Eficacia predictiva", cit., p. 4.

70 López-Ossorio, J.J.; González-Álvarez, J.L. y Muñoz Rivas, M.: *La valoración policial*, cit., p. 55.

71 Ibid, p. 56.

72 Martínez García, E.; Borges Blázquez, R. y Simó Soler, E.: "Inteligencia artificial", cit., p. 8.

efecto superior a la de cada uno de ellos por separado".[73] A través de la utilización de algoritmos de valoración (aditivos y ponderados),[74] el sistema proporciona "un resultado automático del riesgo en que se encuentra la víctima, que el agente posteriormente puede confirmar o modificar según su experiencia".[75] Si bien se está explorando la posibilidad de que VioGén utilice ML, el sistema actual no requiere dicha tecnología.[76]

El formulario VPR4.0 da como resultado cinco tipos distintos de riesgo - no apreciado, bajo, medio, alto o extremo-,[77] asignando diversos tipos de medidas obligatorias y optativas según el riesgo. A modo de ejemplo: (1) en un riesgo no apreciado, se le facilita a la víctima recomendaciones de autoprotección; (2) en un riesgo bajo se le facilita a la víctima números de teléfono de contacto; (3) en un riesgo medio se realiza vigilancias ocasionales de los domicilios de la víctima; (4) en un riesgo alto las visitas a los domicilios de la víctima son frecuentes; y, finalmente, (5) en el riesgo extremo se realiza una vigilancia permanente, acompañado del diseño de un plan de seguridad personalizado.[78]

Un documento elaborado por el Ministerio del Interior de España menciona la posibilidad de ampliar el Sistema VioGén para proteger, entre otras, a las víctimas de trata de personas.[79] Un sistema similar al de VioGén aplicado al delito de trata de personas permitiría la automatización de la determinación del riesgo de que una persona sea víctima de trata, basado en una serie de indicadores, permitiendo a su vez que el Estado ponga en marcha las medidas necesarias según el tipo de riesgo identificado. Sin embargo, dado que el delito de trata de personas tiene ciertas particularidades, el sistema que se implemente deberá ser adaptado para contemplar estas especificidades a los fines de que sea eficiente en la identificación de víctimas de este delito en particular.

Uno de los motivos por los cuales se utilizan algoritmos que comparan lo que ha ocurrido y lo que puede ocurrir en casos de violencia de género es porque este es "un fenómeno claramente repetitivo".[80] Por el contrario, el delito de trata de personas es un delito dinámico que cambia según el país y/o la región de que se trate. Es decir, las modalidades de captación, traslado o acogida, los perfiles de

73 López-Ossorio, J.J.; González-Álvarez, J.L. y Muñoz Rivas, M.: *La valoración policial*, cit., p. 48.

74 Martínez García, E.; Borges Blázquez, R. y Simó Soler, E.: "Inteligencia artificial", cit., p. 11.

75 López-Ossorio, J.J.; González-Álvarez, J.L. y Muñoz Rivas, M.: *La valoración policial*, cit., p. 110.

76 Simó Soler, E.: "Domestic Violence in Spain from a Gender Perspective: Risk Assessment and Analysis", en AA.VV.: *Criminal Prosecution of Domestic Violence in Europe* (dir. por R. Erbaș), Springer, 2023 (en prensa).

77 López-Ossorio, J.J.; González-Álvarez, J.L. y Muñoz Rivas, M.: *La valoración policial*, cit., p. 52.

78 Ibid, 60.

79 Ibid, 86.

80 Magro Servet, V.: "La Inteligencia Artificial para mejorar la lucha contra la violencia de género", en AA.VV.: *Inteligencia Artificial Legal y Administración de Justicia* (dir. por S. Calaza López y M. Llorente Sánchez-Arjona), Thomson-Aranzadi, Pamplona, 2022, p. 398.

las víctimas de trata y las finalidades de explotación, entre otras características, van a cambiar según el país de que se trate.[81] Esto implicará que, a la hora de crear un formulario que capte los principales indicadores, se deberá contemplar la posibilidad de adaptarlo al país en cuestión. Ello asegurará que no se deje de lado ningún indicador relevante que permita identificar a una víctima de trata en ese país concreto.

Por otro lado, el Sistema VioGén tiene en cuenta que las víctimas de violencia de género pueden experimentar barreras a la hora de denunciar las violencias sufridas. Por ejemplo, la Guía de Procedimiento de VioGén reconoce que "las víctimas no suelen manifestar ni hablar de su situación espontáneamente, y que a menudo sienten miedo, vergüenza (…)", prosiguiendo a afirmar que "más allá de los mitos existentes, cada víctima puede reaccionar de una manera distinta durante las diligencias policiales y también cuando exprese el relato de las agresiones."[82] Algo similar sucede respecto de las víctimas de trata de personas. Como ya he mencionado, existen mitos o ideas erróneas acerca de lo que es la trata de personas,[83] que pueden incluso entorpecer la identificación de casos.[84] Entre los mitos alrededor de la trata se encuentra la creencia de que la trata de personas requiere que la víctima esté privada de su libertad, y que las víctimas se van a reconocer inmediatamente como tales y van a solicitar ayuda.[85] A los fines de que el sistema tenga en cuenta esta realidad, el formulario deberá estar, en la medida de lo posible, libre de estos mitos y deberá ser lo más objetivo posible para disminuir la posibilidad de que los "mitos" aparezcan en la persona que completa el formulario y ello pueda derivar en la no identificación de una víctima. También habrá que capacitar a las personas encargadas de completar el formulario, para que estén libres de estos mitos.

Si bien no es necesario el cruce de fronteras para estar frente a un supuesto de trata de personas,[86] existen casos que son transfronterizos. Estos suelen ser

81 Estos cambios en los perfiles de la víctima y del tipo de explotación pueden observarse en: UNODC, "Global Report", cit., p. 26. Ver, por ejemplo: OIM, "Changing patterns and trends of trafficking in persons in the Balkan region", 2004, disponible en: https://publications.iom.int/system/files/pdf/changing_patterns.pdf, último acceso 17 de abril de 2024.

82 Ministerio del Interior del Gobierno de España, "Guía de Procedimiento VPR5.0 y VPER4.1. Protocolo de valoración policial del riesgo y gestión de la seguridad de las víctimas de violencia de género", 2019, p. 3, disponible en: https://violenciadegenerotic.files.wordpress.com/2019/05/instruccion-4-2019.pdf, último acceso 22 de abril de 2024.

83 UNODC, "Misconceptions regarding trafficking in persons", disponible en: https://www.unodc.org/e4j/en/tip-and-som/module-6/key-issues/misconceptions-regarding-trafficking-in-persons.html, último acceso 17 de abril de 2024.

84 Solís, C.E, y Carreón, M.J.: "Derribando mitos sobre la trata de personas", *Revista Abogacía*, 2022, disponible en: https://www.revistaabogacia.com/derribando-mitos-sobre-la-trata-de-personas/, último acceso 17 de abril de 2024.

85 American Bar Association, "Voices for Victims: Lawyers Against Human Trafficking Tool Kit for Bar Associations", 2013, disponible en: https://www.nycourts.gov/LegacyPDFS/IP/human-trafficking/content/3.American%20Bar%20Association%20Toolkit.PDF, último acceso 17 de abril de 2024.

86 Gallagher, A.: *The International Law*, cit., p. 23.

complejos y difíciles de investigar.[87] Es decir que, a la hora de pensar las medidas estatales que deberán ponerse en marcha al aplicar este sistema a los casos de trata, habrá que considerar ciertas medidas transnacionales. Por ejemplo, repatriar a la víctima a su país de origen (en caso de que la víctima así lo desee), intercambiar información entre países para mejorar la detección e investigación, o establecer equipos conjuntos de investigación ("ECI").[88] También podría evaluarse la posibilidad de estandarizar el sistema (por ejemplo, estandarizar los niveles de riesgo) entre países fronterizos donde haya una alta prevalencia y/o un alto riesgo de trata de personas, para asegurar que la víctima se identificada ya sea al salir de un país o al entrar al otro.

También es importante destacar que existe una deficiencia en las estadísticas de trata, las cuales no suelen ser fiables.[89] A su vez, hay una cantidad de víctimas no identificadas que no forman parte de las estadísticas oficiales, conformando la llamada "figura oscura de la trata de personas".[90] Esta escasez estadística dificulta el empleo de ML, cuyas predicciones serán más precisas a partir de mayor data.[91]

Finalmente, será importante evaluar la posibilidad de incluir las voces de las víctimas y sobrevivientes del delito de trata de personas a la hora de diseñar e implementar este sistema. La incorporación de las víctimas y sobrevivientes en el diseño y evaluación de políticas públicas de trata de personas es una manera de empoderarlas y reconocerlas como agentes de cambio social, y sus aportes tienen un papel muy importante.[92] En este caso en concreto, sus voces podrían ser tenidas en cuenta a la hora de, por ejemplo, diseñar preguntas del formulario y determinar las medidas que deberían implementarse según el riesgo que el sistema algorítmico determine.

87 Eurojust, "Report on Trafficking in Human Beings", 2021, p. 2, disponible en: https://www.eurojust.europa.eu/sites/default/files/assets/2021_02_16_thb_casework_report.pdf, último acceso 17 de abril de 2024.

88 En cuanto a la definición de ´equipos conjuntos de investigación´, ver, por ejemplo: Red de Expertos Nacionales en Equipos Conjuntos de Investigación, "Guía práctica de los equipos conjuntos de investigación", documento núm. 6128/1/17 REV 1, Bruselas, 2017, p. 4.

89 Asi, P.: "Strengthening the Evidence Base on Trafficking in Persons", *OIM*, 2023, disponible en: https://weblog.iom.int/strengthening-evidence-base-trafficking-persons, último acceso 17 de abril de 2024; Portal de Datos sobre Migración, "Trata de Personas", 2023, disponible en: https://www.migrationdataportal.org/es/themes/trata-de-personas, último acceso 17 de abril de 2024; UNODC, "Monitoreo de la Prevalencia de la Trata de personas a través de la estimación de Sistemas Múltiples", *Naciones Unidas*, 2022, p. 14, disponible en: https://www.unodc.org/documents/data-and-analysis/tip/2022/MSE_TIP_UNODC_ESP.pdf, último acceso 17 de abril de 2024; Informe de la Sra. Joy Ngozi Ezeilo, Relatora Especial sobre la trata de personas, especialmente mujeres y niños, UN.Doc./ A/HRC/10/16, *Naciones Unidas*, 2009, párr. 11. De manera similar, aunque referido específicamente a España, ver, por ejemplo: Diaconia, "La falta de datos en la trata de seres humanos: un problema latente en España", 2022, disponible en: https://diaconia.es/desactivalatrata/la-falta-de-datos-en-la-trata-de-seres-humanos-un-problema-latente-en-espana/, último acceso 17 de abril de 2024.

90 UNODC, "Global Report", cit., p. 40.

91 Turing, "Introduction to Statistics for Machine Learning", disponible en: https://www.turing.com/kb/introduction-to-statistics-for-machine-learning, último acceso 17 de abril de 2024.

92 Ver, por ejemplo: María Grazia Giammarinaro, UN.Doc./A/75/169, cit., párr. 21-25; Informe de la Sra. Rashida Manjoo, Relatora Especial Rashida Manjoo, Un.Doc./A/HRC/14/22, *Naciones Unidas*, 2010, párr. 29.

B) El formulario y sus indicadores, los riesgos asociados y las medidas estatales a adoptar.

En este apartado desarrollaré los pasos iniciales para poder automatizar el riesgo en los casos de trata de personas, siguiendo el modelo del Sistema VioGén. Es decir, (1) diseñaré el formulario y definiré los indicadores que el mismo debería contemplar para identificar correctamente a las víctimas de trata, (2) explicaré brevemente cómo deberían ser las relaciones lógicas del algoritmo predictivo y cuáles deberían ser los distintos tipos de riesgos, y (3) desarrollaré las principales medidas que deberían ser puestas en funcionamiento según el tipo de riesgo. Antes de abordar cada uno de estos tres elementos, haré la aclaración de que este sistema está pensado para la trata de personas adultas. No se ha incluido la situación de los/las niños/as, ya que la trata de menores tiene ciertas particularidades (por ejemplo, el tipo penal contenido en el artículo 3 del Protocolo de Palermo solo requiere dos elementos - una acción y la finalidad de explotación – prescindiendo del elemento "medios comisivos") que exceden el alcance de este trabajo.

El diseño del formulario deberá captar factores o indicadores de relevancia a la hora de identificar a una víctima de trata de personas. Hay distintos organismos que han elaborado indicadores de trata de personas, tal como UNICEF,[93] la Organización Internacional del Trabajo (OIT)[94] y la Organización Internacional para las Migraciones (OIM).[95] Sin embargo, a los fines de este artículo, me basaré en los "Indicadores de trata de personas de UNODC" ("Indicadores UNODC"). Ello, debido a que la UNODC es el organismo de Naciones Unidas encargado específicamente de abordar los elementos del delito de trata de personas, y de asistir a los Estados con su conocimiento en la materia.[96]

Los Indicadores UNODC brindan información sobre qué debe tenerse en cuenta a la hora de determinar si una persona es víctima de trata. La lista incluye más de 100 indicadores divididos en seis categorías (Indicadores Generales; Niños; Explotación en el Servicio Doméstico; Explotación Sexual; Explotación Laboral; Mendicidad y Delitos Menores), incluyendo, por ejemplo, si la persona trabaja largas jornadas sin descansar o si su pasaporte fue confiscado.[97] En el documento

93 UNICEF, "Identification of Victims / Persons ´At-risk´ of Trafficking in Human Beings", disponible en: https://www.unicef.org/eca/media/24371/file/Identification%20of%20Persons%20At-Risk%20of%20Trafficking%20in%20Human%20Beings.pdf, último acceso 17 de abril de 2024.

94 OIT, "Operational indicators of trafficking in human beings", 2009, disponible en: https://www.ilo.org/wcmsp5/groups/public/---ed_norm/---declaration/documents/publication/wcms_105023.pdf, último acceso 17 de abril de 2024.

95 OIM, "Indicators of Trafficking in Persons", disponible en: https://www.iom.int/sites/g/files/tmzbdl486/files/documents/atip_levant/indicators-of-trafficking-in-persons-1.pdf, último acceso 17 de abril de 2024.

96 UNODC, "Human Trafficking Facts", *Naciones Unidas*, disponible en: https://www.unodc.org/unodc/en/human-trafficking/faqs.html, último acceso 17 de abril de 2024.

97 UNODC, "Indicadores de Trata de Personas", *Naciones Unidas*, disponible en: https://www.unodc.org/documents/human-trafficking/HT_indicators_S_LOWRES.pdf, último acceso 17 de abril de 2024.

que contiene los indicadores, UNODC aclara que "[n]o todos los indicadores que figuran más adelante se presentan en todas las situaciones de trata de personas. Si bien la presencia o ausencia de cualquiera de los indicadores no prueba ni deja de probar que se esté frente a un caso de trata de personas, su presencia debería dar lugar a una investigación."

Al igual que el formulario implementado por el Sistema Viogén, el formulario para identificar a las víctimas de trata deberá englobar la mayor cantidad de los Indicadores UNODC, para lograr que el resultado sea lo más certero posible. Así mismo, se buscará agrupar bajo una misma pregunta varios indicadores. Por ejemplo, la pregunta "¿Siente que tiene la libertad de salir del lugar de trabajo y circular libremente?" incluye los siguientes siete Indicadores UNODC: ser incapaces de abandonar su lugar de trabajo; mostrar señales de que se están controlando sus movimientos; sentir que no se pueden ir de donde están; ser escoltadas cuando van y vuelven del trabajo; no abandonar nunca las instalaciones de trabajo sin su empleador; ser incapaces de movilizarse libremente; estar sujetas a medidas de seguridad destinadas a mantenerlas en las instalaciones de trabajo.

Además, las preguntas fueron elaboradas de tal manera que la respuesta sea "Si, No, No se sabe", a los fines de facilitar el desarrollo del algoritmo predictivo. Las únicas preguntas que inevitablemente tienen opciones de respuesta distintas son: la pregunta 1 referida al Género; la pregunta 2 referida a la Nacionalidad; y la pregunta 13 referida al trabajo a realizar. Por otra parte, las preguntas apuntan a respuestas lo más fácticas y objetivas posibles, justamente para limitar al máximo la posibilidad de que los "mitos" o las dificultades de las víctimas en reconocerse como tales puedan dificultar la identificación.

Si bien los Indicadores UNODC no han incluido al género como un indicador, he decidido agregar en el formulario una pregunta referida al género. Ello, debido a que el género podría ser un factor a tener en cuenta a la hora de identificar a una posible víctima de trata de personas. Por ejemplo, en aquellos países donde la mayoría de las víctimas son mujeres, el género será un factor relevante.

A partir de los Indicadores UNODC, y teniendo en cuenta las aclaraciones previas, se podría diseñar un formulario que unifique los principales indicadores en las siguientes 20 preguntas agrupadas en 4 factores. Las opciones de respuesta a cada una de las preguntas están incluidas luego de cada pregunta. El formulario incluye una sección vinculada al "Tipo de Riesgo", que será desarrollada a continuación. El formulario es de elaboración propia, a partir de los Indicadores UNODC.

A. Factores vinculados a la posible vulnerabilidad de la víctima.

1. *Género*: Opciones de respuesta: Mujer/ Hombre / Transgénero / otra.

TIPO DE RIESGO: BAJO.

2. *Nacionalidad:*[98] Opciones de respuesta: Se incluirán todos los países existentes actualmente.

TIPO DE RIESGO: BAJO.

3. *¿Habla el idioma oficial del país?*: Opciones de respuesta: Si/No/No se sabe.

TIPO DE RIESGO: BAJO.

B. Factores vinculados al elemento del tipo "acción".

4. *¿Le han pagado el transporte al lugar de traslado? (por ejemplo, el ticket de bus o el pasaje de avión)*: Opciones de respuesta: Si/No/No se sabe.

TIPO DE RIESGO: MEDIO.

5. *¿Ha recibido alguna indicación de cómo debe comportarse en los controles migratorios? (Por ejemplo, indicaciones de qué información debe brindar al agente migratorio)*: Opciones de respuesta: Si/No/No se sabe.

TIPO DE RIESGO: MEDIO.

6. *¿Se le ha obligado a utilizar un pasaporte o DNI falso?*: Opciones de respuesta: Si/No/No se sabe.

TIPO DE RIESGO: ALTO.

7. *¿Se vive en el mismo lugar en el cual se trabaja?*: Opciones de respuesta: Si/No/No se sabe.

TIPO DE RIESGO: MEDIO.

C. Factores vinculadas a la existencia de medios comisivos (engaño, amenazas, etc.).

8. *¿Siente que el trabajo que debe realizar es igual al que le ofrecieron inicialmente?*: Opciones de respuesta: Si/No/No se sabe.

TIPO DE RIESGO: MEDIO.

9. *¿Le han retenido el pasaporte y/o el documento de identidad?*: Opciones de respuesta: Si/No/No se sabe.

98 Los Indicadores UNODC incluyen el siguiente indicador: Provenir de un lugar que, según consta, es una fuente de trata de personas.

TIPO DE RIESGO: ALTO.

10. *¿Siente que tiene la libertad de salir del lugar de trabajo y circular libremente?*: Opciones de respuesta: Si/No/No se sabe.

TIPO DE RIESGO: ALTO.

11. *¿Puede comunicarse fácilmente con sus familiares?*: Opciones de respuesta: Si/No/No se sabe.

TIPO DE RIESGO: MEDIO.

12. *¿Ha sufrido amenazas, maltratos, lesiones u algún otro tipo de agresión (ya sea física, psicológica o verbal)?*: Opciones de respuesta: Si/No/No se sabe.

TIPO DE RIESGO: ALTO.

D. Factores vinculados a la finalidad de explotación.

13. *¿Cuál es el trabajo que debe realizarse? ¿En qué rubro se ubica?*[99]: Opciones de respuesta: Las opciones de respuesta a esta pregunta dependerán del país en el que se implemente, para captar las principales formas de explotación de dicho país. Por ejemplo, las opciones podrían ser: textil, agricultura, ganadería, supermercado, venta de productos, albañilería, trabajos domésticos, etc.

TIPO DE RIESGO: BAJO.

14. *¿Se ha firmado un contrato laboral formal?*: Opciones de respuesta: Si/No/No se sabe.

TIPO DE RIESGO: MEDIO.

15. *¿Recibe una remuneración escasa o nula?*: Opciones de respuesta: Si/No/No se sabe.

TIPO DE RIESGO: ALTO.

16. *¿Se le ha reclamado alguna deuda y/o se le realizan descuentos de su salario? (por ejemplo, por el traslado al trabajo o por residir en el lugar de trabajo)*: Opciones de respuesta: Si/No/No se sabe.

99 Los Indicadores UNODC incluyen el siguiente indicador: Las personas que han sido objeto de trata con fines de explotación laboral son generalmente obligadas a trabajar en sectores como los de agricultura, construcción, entretenimiento, industria de servicios y manufactura (talleres clandestinos).

TIPO DE RIESGO: ALTO.

17. *¿Siente que las condiciones del lugar de trabajo son inadecuadas para trabajar? (Por ejemplo, es un lugar que no cumple con requisitos mínimos de habitabilidad, se encuentra deteriorado y/o es peligroso)*: Opciones de respuesta: Si/No/No se sabe.

TIPO DE RIESGO: MEDIO.

18. *¿Tiene frecuentemente jornadas laborales extensas (más de 40 horas por semana)?*[100]: Opciones de respuesta: Si/No/No se sabe.

TIPO DE RIESGO: ALTO.

19. *¿Se le otorgan días de descanso?*: Opciones de respuesta: Si/No/No se sabe.

TIPO DE RIESGO: MEDIO.

20. *¿Siente la libertad de poder terminar el contrato laboral de así desearlo?*: Opciones de respuesta: Si/No/No se sabe.

TIPO DE RIESGO: ALTO.

Como puede observarse, se ha agregado una sección vinculada al "Tipo de Riesgo", asignando tres tipos de riesgo distinto (Bajo, Medio y Alto) a cada factor. Para determinar qué nivel de riesgo debe asignársele a cada factor, tuve en cuenta la definición de explotación desarrollada por la Corte IDH mencionada anteriormente, según la cual la explotación es un "acto con el objetivo de *utilizar una persona de manera abusiva para su propio beneficio.* De esta manera, se atribuye un valor al individuo, por ejemplo por medio de su mano de obra, para después convertirlo en un beneficio propio, bajo condiciones abusivas e injustas o fraudulentas, beneficio que es el resultado *de la cosificación o comercialización del mismo individuo*." (el resaltado es propio)

Con esto en mente, el riesgo se distribuyó de la siguiente manera: cuanto más cerca esté el indicador de producir la cosificación de la persona, mayor será el riesgo. Así, por ejemplo, no hablar el idioma oficial del país será un riesgo bajo, ya que no denota por sí mismo una cosificación (aunque sí puede ser un factor de vulnerabilidad que pueda ser aprovechado por el/la tratante). En cambio, que la persona no tenga días de descanso es un indicador de riesgo medio, ya que comienza a aparecer un aprovechamiento por parte del tratante. Finalmente, sufrir

100 El dato de 40 horas por semana se extrae a partir del siguiente documento: Organización Internacional del Trabajo (OIT), *Recomendación sobre la reducción de la duración del trabajo*, 1962 (núm. 116), disponible en: https://www.ilo.org/dyn/normlex/es/f?p=NORMLEXPUB:12100:0::NO::P12100_ILO_CODE:R116, último acceso 17 de abril de 2024.

maltratos físicos y/o psicológicos, o ser sometido/a a jornadas laborales extensas es un indicador alto, ya que son factores que demuestran una objetivación hacia otro individuo con el fin de obtener un beneficio propio.

Al llenar el formulario, el Sistema propuesto dará como resultado 4 tipos de riesgo distintos: 1) riesgo no apreciado; 2) riesgo bajo; 3) riesgo medio; y 4) riesgo alto. Entonces, la próxima pregunta a desarrollar es: al aplicar el algoritmo, ¿qué combinaciones de los indicadores dará como resultado los diferentes riesgos?

En el año 2009, la OIT elaboró unos indicadores de trata de personas, donde a partir de la utilización del "método Delphi", se identifica factores y se les asigna un riesgo.[101] Si bien el documento data de varios años, es útil para pensar esta pregunta, ya que indica que una dimensión (por ejemplo, la dimensión de "condiciones de trabajo explotativas" o "el abuso de la situación de vulnerabilidad en el lugar de destino") será positiva respecto del caso concreto si existen, por ejemplo, dos indicadores altos, o tres medios. El documento también dice que, luego de que se analice cada dimensión, habrá que combinar el análisis de todas las dimensiones para determinar si la persona es víctima de trata, aunque no detalla cómo hacer ese análisis.

Ello me llevó a pensar en cómo debería diseñarse el algoritmo para este sistema. La correlación que podría hacer el algoritmo para dar como resultado los distintos riesgos se presenta en el siguiente cuadro. El formulario desarrollado a continuación no es exhaustivo ni definitivo, sino meramente ilustrativo a los fines de que se entienda cómo se podría pensar el algoritmo y la manera de determinar los distintos riesgos. El formulario es de elaboración propia.

Habrá RIESGO ALTO si:

- hay tres o más de tres indicadores de riesgo alto

- hay dos indicadores altos distribuidos entre dos factores distintos

- hay dos indicadores altos y uno medio

- hay al menos tres indicadores medios

Habrá RIESGO MEDIO si:

- hay dos indicadores altos en el mismo factor

- hay dos indicadores medios

101 OIT. "Operational indicators", cit.

- hay un indicador alto y un indicador medio

- hay un indicador medio y al menos dos indicadores bajos

Habrá RIESGO BAJO si:

- hay solamente un indicador alto

- hay un indicador alto y uno o más indicadores bajos

- hay solamente un indicador medio

- hay un indicador medio y uno o más indicadores bajos

- hay tres o más indicadores bajos

Habrá RIESGO NO APRECIADO si:

- hay dos o menos indicadores bajos, o ningún indicador

Finalmente, procederé a desarrollar las medidas estatales que deberían ser articuladas para cada nivel de riesgo. Las medidas desarrolladas a continuación son acciones que el Estado ya está obligado a cumplimentar, o se recomienda que el Estado realice. Es decir, este sistema no estaría creando medidas nuevas, sino que estaría estandarizando obligaciones y recomendaciones pre-existentes, según el riesgo obtenido. La lógica es la misma que sigue el Sistema Viogén, es decir, cuanto mayor riesgo se identifique, más intensas son las medidas.[102]

1. Riesgo no apreciado (nivel 1): se entregará un folleto informativo sobre el delito de trata de personas.

2. Riesgo Bajo (nivel 2): se repite la medida del nivel 1, y se le otorga a la posible víctima un teléfono de contacto de una línea directa y gratuita para eventualmente denunciar el delito. También se le puede solicitar a la víctima que, de manera voluntaria, otorgue su teléfono de contacto, a los fines de que se realice una llamada para monitorear su situación.

3. Mediano (nivel 3): se repiten las medidas del nivel 1 y 2, y se le pide a la víctima que, de manera voluntaria, otorgue los datos generales del lugar de trabajo (tal como la dirección del lugar o el nombre del/la empleador/a), que pueden ser utilizados para monitorear el caso (por ejemplo, realizar una inspección de rutina).

102 López-Ossorio, J.J.; González-Álvarez, J.L. y Muñoz Rivas, M.: *La valoración policial*, cit., p. 53-54.

4. Alto (nivel 4): se inicia de oficio una investigación para determinar la posible existencia del delito. Se realiza una inspección de rutina en el los domicilios vinculados a la posible comisión del delito de trata de personas. Si existe un caso de trata transfronterizo, se activa el intercambio de información con el país de que se trate y se evalúa la posibilidad de establecer un ECI. Se activa la asistencia y protección temprana a la víctima. Se debe tener en cuenta los cuidados especiales hacia la víctima, por ejemplo, considerar que puede estar bajo alguna amenaza o peligro de represalia.

Al poner en práctica estas medidas, los Estados deberán tener un enfoque centrado en las víctimas y en los derechos humanos ("*human rights and victim-centred approach*").[103] También deberán tener en cuenta el principio de no punibilidad, según el cual "[l]as víctimas de trata de personas no deberían ser objeto de enjuiciamiento, sanción ni otro tipo de castigo por los actos ilegales que hayan realizado como consecuencia directa de haber sido objeto de trata."[104]

Este modelo podría ser implementado en distintos espacios donde se suele entrar en contacto con víctimas de trata y en donde la misma puede pasar desapercibida. Ello incluye, entre otras, las zonas de frontera (tal como el cruce migratorio en los aeropuertos o en zona terrestre), o en el marco de una inspección laboral de rutina. También se puede pensar en su implementación en el marco de una denuncia, por ejemplo, por malas condiciones laborales que en realidad podría ser un caso de trata de personas con fines de explotación laboral; o una denuncia por una privación ilegítima de la libertad que pueda derivar en un caso de trata de personas. Este modelo también podría ser pensado para que las empresas identifiquen posibles casos de trata en su cadena de producción.

3. La utilización del sistema algorítmico en la práctica: una aproximación a los desafíos y a las oportunidades.

Si bien automatizar decisiones mediante la utilización de algoritmos presenta ventajas, tal como la optimización de la toma de decisiones, también presenta ciertos riesgos.[105] En 2019, el Grupo de expertos de alto nivel sobre IA (un grupo de expertos independientes constituido por la Comisión Europea) elaboró el documento "Directrices Éticas para una IA fiable".[106] Este documento desarrolla

103 Informe de la Sra. María Grazia Giammarinaro, Relatora Especial sobre la trata de personas, especialmente mujeres y niños, U.N.Doc./A/75/169, *Naciones Unidas*, 2022, párr. 36.

104 Grupo Interinstitucional de Coordinación contra la Trata de Personas, "Nota Informativa 8: La No Penalización de las Víctimas de Trata de Personas", *Naciones Unidas*, 2020, disponible en: https://icat.un.org/sites/g/files/tmzbdl461/files/v1912063_new_spanish_version.pdf, último acceso 17 de abril de 2024.

105 Castillejo Manzanares, R.: "Digitalización y/o Inteligencia Artificial", en AA.VV.: *Inteligencia Artificial Legal y Administración de Justicia* (dir. por S. Calaza López y M. Llorente Sánchez-Arjona), Thomson-Aranzadi, Pamplona, 2022, p. 77.

106 Comisión Europea, Dirección General de Redes de Comunicación, Contenido y Tecnologías, *Directrices éticas para una IA fiable*, Oficina de Publicaciones, 2019, disponible en: https://data.europa.eu/

siete requisitos que los sistemas que utilicen IA deben respetar, entre los que se incluye la "Diversidad, no discriminación y equidad" y la "Transparencia". El primero refiere a la necesidad de "garantizar la inclusión y la diversidad a lo largo de todo el ciclo de vida de los sistemas de inteligencia artificial", lo que incluye la necesidad de evitar sesgos. Por otro lado, la transparencia "guarda una relación estrecha con el principio de explicabilidad e incluye la transparencia de los elementos pertinentes para un sistema de IA".[107] A los efectos de este artículo, me limitaré a desarrollar de manera no exhaustiva los riesgos específicos vinculados a esos dos principios.

En primer lugar, habrá que tener cautela respecto de los datos que se utilizarán para entrenar al algoritmo, a los fines de evitar la discriminación algorítmica.[108] En efecto, la selección de datos con los que se entrenará al algoritmo debe ser representativa y libre de sesgos, ya que si una categoría relevante no es incluida, existe el riesgo de que se produzcan resultados discriminatorios.[109] El riesgo de que el uso de tecnologías para luchar contra la trata sean discriminatorias fue resaltado por el Grupo de expertos del Consejo de Europa en lucha contra la trata de personas (GRETA).[110]

En el caso del sistema propuesto en este artículo, hay dos momentos en donde podría aparecer un riesgo de discriminación algorítmica. En primer lugar, habría que tener precaución al momento de diseñar el formulario, ya que si falta alguna categoría relevante es posible que haya problemas en la detección y se produzcan resultados discriminatorios. Asimismo, si en un futuro se utiliza aprendizaje automático o ML, será importante considerar con cautela los datos que se utilizarán para la fase de entrenamiento, ya que si existe una infra-representación de un grupo específico, el sistema también podría derivar en resultados discriminatorios.

Es por ello que, como he remarcado previamente, habrá que adaptar el formulario aquí propuesto al país específico de que se trate, para asegurar que todas las categorías relevantes para ese país específico estén presentes. Por ejemplo, podría derivar en un resultado discriminatorio, al completar el formulario, se selecciona una nacionalidad o un género cuyas víctimas son minoritarias o nulas (en un caso hipotético, podría ser nacionalidad Argentino – género hombre), y el resultado de nulo por el simple hecho de tratarse de un una persona de

doi/10.2759/14078, último acceso 17 de abril de 2024.

107 La Guía explica que "La explicabilidad concierne a la capacidad de explicar tanto los procesos técnicos de un sistema de IA como las decisiones humanas asociadas (por ejemplo, las áreas de aplicación de un sistema de IA). La explicabilidad técnica requiere que las decisiones que adopte un sistema de IA sean comprensibles para los seres humanos y estos tengan la posibilidad de rastrearlas."

108 Martínez García, E.; Borges Blázquez, R. y Simó Soler, E.: "Inteligencia artificial", cit., p. 6.

109 Ibid.

110 GRETA, "Online and technology-facilitated trafficking in human beings", *COE*, 2022, p. 21, disponible en: https://rm.coe.int/online-and-technology-facilitated-trafficking-in-human-beings-full-rep/1680a73e49, último acceso 17 de abril de 2024.

determinado género y de determinada nacionalidad (hombre de nacionalidad Argentina).

En segundo lugar, el sesgo podría aparecer en el/la funcionario/a público/a que complete el formulario. Como se ha remarcado en el apartado anterior, será necesario capacitar a quienes completen el formulario, a los fines de que comprendan las particularidades del delito de trata de personas, así como también el funcionamiento de este sistema y las distintas categorías incluídas en el formulario. De hecho, GRETA refirió específicamente a la importancia de que se entrene a quienes utilicen tecnologías en la lucha contra la trata de personas.[111]

Por otro lado, existe el riesgo de la falta de transparencia y trazabilidad, en donde se desconoce cuál fue el proceso que llevó a un sistema a obtener determinado resultado.[112] Ello puede ser el resultado, por ejemplo, de la negación por parte del órgano estatal o de la empresa privada (según sea el caso) a brindar información sobre el algoritmo utilizado.[113] En el caso del sistema aquí propuesto, será necesario que se permita la realización de auditorías que permitan entender qué datos se están utilizando para entrenar a este modelo y qué tipo de algoritmo se está utilizando.

En cuanto a las principales ventajas, este sistema permitiría superar algunas de las barreras de identificación nombradas previamente. Entre ellas, se disminuiría la posibilidad de que aparezcan "los mitos de la trata", así como las dificultades de las víctimas de reconocerse como tales. Una vez cumplimentado el formulario, y obtenido un resultado de riesgo, se pondrán en marcha las medidas aparejadas independientemente de si la víctima y/o el/la funcionario/a reconocen los hechos como una potencial situación de trata de personas.

Además, en un delito que suele ser oculto, contar con un sistema que dé una respuesta rápida e inmediata permitiría aprovechar instancias claves en donde un/a funcionario/a toma contacto con una potencial víctima, tal como en un control aeroportuario o en el marco de una inspección laboral. Considerando que la trata es un delito donde se suele explotar a varias víctimas al mismo tiempo (por ejemplo, en el marco de talleres clandestinos o de prostíbulos), contar con un sistema que permita mejorar la identificación de una víctima, a la larga, maximiza la posibilidad de identificar a otras víctimas – ya que identificando a una víctima es probable que pueda identificarse a otras que estaban siendo explotadas en el marco de la misma red de trata.

111 GRETA, "Online and technology-facilitated", cit., p. 83 y ss.

112 Simó Soler, E. y Rosso, P.: "Inteligencia artificial", cit., p. 5.

113 Gómez Colomer, J.L.: "Derechos fundamentales, proceso e Inteligencia Artificial: una reflexión", en AA.VV.: *Inteligencia Artificial Legal y Administración de Justicia* (dir. por S. Calaza López y M. Llorente Sánchez-Arjona), Thomson-Aranzadi, Pamplona, 2022, p. 286.

Este sistema también permitiría estandarizar una línea mínima a partir de la cual existirá una identificación, ya que los casos que presenten ciertas características van a ser necesariamente identificados. También aseguraría una base mínima de acciones estatales, ya que frente a los distintos riesgos, el Estado al menos deberá implementar las medidas así determinadas por el sistema. Finalmente, como consecuencia del aumento en la identificación de víctimas, este sistema permitiría mejorar el acceso de las víctimas a sus derechos humanos, incluido el derecho de acceso a la justicia.

III. REFLEXIONES FINALES.

Frente a la existencia de una víctima de trata de personas, existe un deber estatal de identificarla lo más rápidamente posible. A más de veinte años de la entrada en vigor del Protocolo de Palermo, hay un gran camino por recorrer. Actualmente, sigue habiendo un gran número de víctimas de trata de personas que se encuentran ocultas, como consecuencia, en gran medida, de la existencia de barreras que dificultan la identificación. La gravedad de esta situación radica no solo en que los Estados estarían incumpliendo sus obligaciones internacional, sino principalmente en el hecho de que una víctima de trata no identificada es una víctima que sigue siendo explotada, y sus derechos violados de manera continuada.

En este escenario, un sistema de IA que utilice algoritmos predictivos para mejorar la identificación de las víctimas, inspirado en el Sistema VioGén como el propuesto en este artículo, surge como una herramienta que parecería eficaz para superar las barreras. Ello, siempre y cuando se tengan en cuenta los diversos riesgos que vienen acompañados de la utilización de estos sistemas, y que su implementación sea acompañada de la capacitación de las personas a cargo de ponerlas en marcha.

Más allá de la posibilidad de mejorar la identificación de las víctimas de trata, es importante recordar que los Estados deben seguir implementando medidas eficaces para prevenir este delito y hacer frente a las causas subyacentes de la trata de personas, tal como la desigualdad y la pobreza. Será únicamente a través de políticas públicas que busquen transformar la realidad actual, y que prioricen principalmente la transformación de las realidad de las víctimas y supervivientes de este delito, que la trata de personas podrá ser eficientemente abordada, y eventualmente, erradicada.

BIBLIOGRAFÍA

Barona Vilar, S.: "Inteligencia Artificial o la Algoritmización de la vida y de la justicia: ¿solución o problema?", *Revista boliviana de Derecho de Derecho*, 2019, núm. 28.

Castillejo Manzanares, R.: "Digitalización y/o Inteligencia Artificial", en AA.VV.: *Inteligencia Artificial Legal y Administración de Justicia* (dir. por S. Calaza López y M. Llorente Sánchez-Arjona), Thomson-Aranzadi, Pamplona, 2022.

Gallagher, A.: *The International Law of Human Trafficking*, CUP, Nueva York, 2010.

Gómez Colomer, J.L.: "Derechos fundamentales, proceso e Inteligencia Artificial: una reflexión", en AA.VV.: *Inteligencia Artificial Legal y Administración de Justicia* (dir. por S. Calaza López y M. Llorente Sánchez-Arjona), Thomson-Aranzadi, Pamplona, 2022.

Jasi, P.: "Strengthening the Evidence Base on Trafficking in Persons", *OIM*, 2023.

López-Ossorio, J.J.; González-Álvarez, J.L. y Andrés-Pueyo, A.: "Eficacia predictiva de la valoración policial del riesgo de la violencia de género", *Psychosocial Intervention*, 2016, núm. 25.

López-Ossorio, J.J.; González-Álvarez, J.L. y Muñoz Rivas, M.: *La valoración policial del riesgo de violencia contra la mujer pareja en España – Sistema VioGén*, Ministerio del Interior. Gobierno de España, Madrid, 2018.

Magro Servet, V.: "La Inteligencia Artificial para mejorar la lucha contra la violencia de género", en AA.VV.: *Inteligencia Artificial Legal y Administración de Justicia* (dir. por S. Calaza López y M. Llorente Sánchez-Arjona), Thomson-Aranzadi, Pamplona, 2022.

Martínez García, E.; Borges Blázquez, R. y Simó Soler, E.: "Inteligencia artificial y perspectiva de género en la justicia penal", *Diario La Ley*, 2021, núm. 47.

Obokata, T.: "A Human Rights Framework to Address Trafficking of Human Beings", 24 *Netherlands Quarterly of Human Rights*, 2006, vol. 24.

Piotrowicz, R. y Redpath-Cross, J.: "Human trafficking and smuggling", en AA.VV.: *Foundations of International Migration Law*, (ed. por B. Opeskin), CUP, Nueva York, 2012.

Simó Soler, E.: "Domestic Violence in Spain from a Gender Perspective: Risk Assessment and Analysis", en AA.VV.: *Criminal Prosecution of Domestic Violence in Europe* (dir. por R. Erbaş), Springer, 2023 (en prensa).

Simó Soler, E. y Rosso, P.: "Inteligencia artificial y derecho: entre el mito y la realidad", *Diario La Ley*, 2022, núm. 9982.

Solís, C.E. y Carreón, M.J.: "Derribando mitos sobre la trata de personas", *Revista Abogacía*, 2022.

Sourdin, T.: "Judge v Robot? Artificial Intelligence and Judicial Decision-making", *UNSW Law Journal*, 2018, vol. 41.

Vicario Pérez, A.M.: "Sobre la criminalidad organizada y la trata de seres humanos. Especial referencia al uso de la inteligencia artificial en la identificación de las víctimas", en AA.VV.: *La Justicia en la Sociedad 4.0: Nuevos Retos para el Siglo XXI* (dir. por L. Fontestad Portalés y P.R. Suárez Xavier), Colex, A Coruña, 2023.

RETOS PARA UNA INTELIGENCIA ARTIFICIAL INCLUSIVA DE LOS COLECTIVOS VULNERABLES

CHALLENGES FOR AN INCLUSIVE ARTIFICIAL INTELLIGENCE OF VULNERABLE GROUPS

Actualidad Jurídica Iberoamericana Nº 21, agosto 2024, ISSN: 2386-4567, pp. 360-383

Ana Isabel
BLANCO
GARCÍA

ARTÍCULO RECIBIDO: 29 de mayo de 2023
ARTÍCULO APROBADO: 1 de julio de 2024

RESUMEN: La revolución tecnológica de la inteligencia artificial es una realidad innegable. Todos los sistemas, aplicaciones, herramientas… que calificamos como inteligentes están llamados a transformar los actuales modelos de convivencia, de comunicación e, incluso, de tutela de nuestros derechos. Ahora bien, a pesar del progreso y avance que ello está suponiendo en nuestra sociedad, como sucede con todo cambio trascendental, son muchos los desafíos que genera, especialmente si queremos garantizar un modelo de Justicia caracterizado por la inclusión y la igualdad.

PALABRAS CLAVE: Artificial Intelligence; algorithms; vulnerable group; equality; inclusion.

ABSTRACT: *Technological Revolution of Artificial Intelligence is an undeniable reality. All systems, applications, tools... qualified as intelligent are meant to transform the current models of living and communication, and even the protection of human rights. However, despite the progress and advances in our society, there are many challenges as a transcendental change, especially when the aspiration is an inclusive and fair model of Justice.*

KEY WORDS: *Inteligencia Artificial; algoritmos; colectivos vulnerables; igualdad; inclusión.*

SUMARIO.- I. PUNTO DE PARTIDA: HACIA UNA INTELIGENCIA ARTIFICIAL INCLUSIVA, CONFIABLE Y ÉTICA.- II. LA IA Y LOS ODS: SU NECESARIA ALINEACIÓN.- 1. Primer reto: sesgos algorítmicos.- 2. Segundo reto: trazabilidad y explicabilidad del algoritmo.- 3. Tercer reto: la motivación de las resoluciones.- III. LA IA Y LA PERSPECTIVA DE VULNERABILIDAD: UNA REFLEXIÓN FINAL.

I. PUNTO DE PARTIDA: HACIA UNA INTELIGENCIA ARTIFICIAL INCLUSIVA, CONFIABLE Y ÉTICA.

La revolución tecnológica ha sufrido, en los últimos tiempos, un salto cualitativo gracias a la irrupción -masiva, atropellada y algo caótica- de la Inteligencia Artificial (en adelante, IA), donde su presencia es ya una constante en prácticamente todos los ámbitos y sectores de la sociedad. Atrás vamos dejando las confusiones sobre qué es la IA y sobre lo que no es IA para adentrarnos de lleno en su necesaria -y esperada- regulación que permita sentar las bases de un marco jurídico eficaz. Así es, la novedad de los sistemas informáticos y de la digitalización de los procesos ha quedado superada. Y, obviamente, el ámbito de la Justicia no ha quedado al margen de esta modernización, donde ya se aplican sistemas y herramientas de IA.

La utilización de sistemas de IA por parte de entidades de sectores productivos y económicos de forma transversal a lo largo de la cadena de valor conlleva una serie de consideraciones de relevancia para el ámbito jurídico. La mayoría cumplen finalidades como la prevención del fraude, del blanqueo de capitales o de comisión de delitos dentro de la propia organización. Otras se configuran como *softwares* asistenciales -los conocidos como Chatbots- e incluso también pueden servir para resolver quejas y reclamaciones sencillas y que permitan una estandarización en la reparación de los daños causados a las personas usuarias de tales servicios o productos.

Indudable es, también, el potencial de las herramientas de IA en la mejora, agilización y sostenibilidad del sistema de Justicia actual, gracias no solamente a la propia aplicación de tecnología sino también a la automatización de los procedimientos y distintas actuaciones, lo que permitirá una redistribución más eficiente de los recursos disponibles.

Nos hallamos, pues, en un escenario en el que el progreso y transformación del paradigma de Justicia se muestra favorable a la calidad, seguridad y eficiencia de los procesos y medios de tutela. Sin embargo, la otra cara de la moneda, menos amable, viene representada por todos los riesgos inherentes a la aplicación de estas tecnologías y su posible afectación de derechos fundamentales.

• Ana Isabel Blanco García
Profesora Titular de Derecho procesal, Universitat de València. Correo electrónico: a.isabel.blanco@uv.es

Una serie de desafíos que derivan de la implantación de esta IA y de las funciones variadas que desempeña, desde la mejora del acceso a la justicia, la asistencia jurídica, la resolución de conflictos a través de plataformas online[1], hasta la función jurisdiccional, donde puede cumplir funciones predictivas y funciones decisorias en el seno del proceso judicial[2], auxiliando en distintos ámbitos como la valoración del riesgo, la valoración de la prueba o la calificación jurídica[3].

Con carácter previo a la identificación y estudio de estos desafíos, es importante entender qué es una herramienta de IA, para así poder mostrar cómo podemos tratar de preservar la equidad y la igualdad de la sociedad, de los valores, de los principios y de los derechos de las personas.

Concretamente, se entiende que la IA engloba "sistemas con la capacidad de realizar funciones asociadas a la inteligencia humana como percibir, aprender, entender, adaptarse, razonar e interactuar imitando un comportamiento humano inteligente"[4]. Por su parte, y más recientemente, el Reglamento de Inteligencia Artificial, aprobado por el Parlamento Europeo el día 13 de marzo de 2024[5] viene a armonizar el concepto de IA[6], pues hasta la fecha se contaba con distintas definiciones. Así, este texto concibe la IA como "un sistema basado en una máquina diseñado para funcionar con distintos niveles de autonomía, que puede mostrar capacidad de adaptación tras el despliegue y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar

1 En palabras de Barona, el desarrollo de una plataforma digital ODR es una fórmula que "rompe el sistema de resolución de conflictos e introduce la algoritmización en la toma de decisiones al trabajar con la plataforma digital no solo en lo formal sino también en lo material, en la solución del conflicto en sí". Barona Vilar, S.: "Inteligencia artificial o la algoritmización de la vida y de la justicia", *Revista Boliviana de Derecho,* núm. 28, 2019, p. 40. Sobre la aplicación de la IA en los ODR, véase, Marcos Francisco, D.: "Smart ODR y su puesta en práctica: el salto a la inteligencia artificial", *Revista General de Derecho Procesal,* 2023, núm. 59.

2 Martín Diz, F.: "Justicia digital post-covid19: el desafío de las soluciones extrajudiciales electrónicas de litigios y la inteligencia artificial", *Revista de Estudios Jurídicos y Criminológicos,* 2020, núm. 2, p. 63. Sobre la repercusión jurídica de las herramientas de IA en las distintas fases del proceso, véase, Montesinos García, A.: "Empleo de la inteligencia artificial en algunas fases del proceso judicial civil: prueba, medidas cautelares y sentencia", *Actualidad civil*, 2022, núm. 11, pp. 1-31.

3 Castillejo Manzanares, R.: "Las nuevas tecnologías y la inteligencia artificial como retos post-covid19", *Revista General de Derecho Procesal,* 2022, núm. 56, p. 12.

4 Oliver, N., *Inteligencia Artificial, naturalmente. Un manual de convivencia entre humanos y máquinas para que la tecnología nos beneficie a todos,* ONTSI, Madrid, 2020, p. 28. Disponible en: https://www.unav.edu/documents/26661763/0/InteligenciaArtificialNuriaOliver.pdf/b527ddf6-b04a-025b-2000-8ba3d157d1ae?t=1625572030005

5 European Parliament legislative resolution of 13 March 2024 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)). Documento disponible en: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.html#title2

6 Barona Vilar la concibe como "una suerte de noción omnicomprensiva (panconcepto) que permite abrigar desde las primeras manifestaciones de la máquina inteligente, siquiera lo fuere para desplegar una suerte de talento en una determinada ciencia, arte, cultura, hasta cuestionarnos, en este imparable mundo expansivo digital que vivimos, nuevas fórmulas inteligentes, no solo en cuanto a tecnología de última generación, sino también en cuanto a su accesibilidad y amabilidad de uso". Barona Vilar, S.: *Algoritmización del Derecho y de la Justicia. De la Inteligencia Artificial a la Smart Justice,* Tirant lo Blanch, Valencia, 2021, p. 80.

información de salida, como predicciones, contenidos, recomendaciones o decisiones, que puede influir en entornos físicos o virtuales" (artículo 3.1).

Esta tecnología inteligente diluye la separación y límites entre la tecnología y las personas, entre el factor tecnológico y el factor humano. Vivimos inmersos en el fenómeno de "la algoritmización de la vida"[7], que nos avizora para cambiar nuestro entorno, pero también la forma de crear, interpretar y aplicar el Derecho. Tanto es así que ya se habla incluso de la aparición de un nuevo sujeto o figura como es el juez robot o juez IA, definido por Gómez Colomer como "una máquina inteligente que dicta sentencias con base en los algoritmos introducidos en ella y en los hechos y datos del caso real producido"[8], de forma que puedan automatizarse procedimientos sencillos[9], dado que han demostrado resultar útiles, ágiles y eficaces. No obstante, no podemos olvidar que deberá, en todo caso, delimitarse la relación entre el factor tecnológico y el factor humano dada la prohibición de que la IA ocupe "el lugar de un ser humano a la hora de dictar sentencia o tomar decisiones"[10].

Sobre este aspecto, en el marco de un proceso penal, Barona insiste en la necesidad de valorar si el juez robot podría llegar a sustituir al juez humano en el proceso penal. Al respecto, considera que "extrapolar estas iniciativas de robotización judicial a la sede penal llevaría a la liquidación del proceso penal, al convertir este en un expediente automatizado que impediría el ejercicio de los derechos reconocidos a quienes son sujetos del proceso penal; mermarían las garantías de defensa y propulsarían una mecanización judicial que, cuando menos, chocaría con el proceso lógico jurídico de razonamiento judicial que aplica la norma al caso concreto, al sujeto concreto y bajo unas circunstancias concretas, modulando y justificando esta modulación en la motivación de los hechos probados"[11].

En suma, la incorporación de estos sistemas reporta beneficios en términos de simplicidad, agilización y reducción de costos. Ahora bien, como toda novedad,

7 Barona Vilar, S.: "Inteligencia artificial", cit., p. 23.

8 Gómez Colomer, J. L.: "Unas reflexiones sobre el llamado «juez-robot», al hilo del principio de independencia judicial", en AA.VV.: *Justicia algorítmica y neuroderecho: una mirada multidisciplinar"* (dir. por S. Barona Vilar), Tirant lo Blanch, Valencia, 2021, p. 258.

9 Conde Fuentes se muestra crítico con la automatización de los procesos judiciales al cuestionarse qué debería entenderse por sencillo y el alcance de la automatización, dudando de su efectividad en la fase decisoria. Conde Fuentes, J.: "La inteligencia artificial y la figura del juez-robot", en AA.VV.: *Modernización, eficiencia y aceleración del proceso* (dir. por S. Pereira Puigvert y M.J. Pesqueira Zamora), Aranzadi, Cizur Menor (Navarra), 2022, pp. 118-119.

10 Resolución del Parlamento Europeo, de 20 de enero de 2021, sobre inteligencia artificial: cuestiones de interpretación y de aplicación del Derecho internacional en la medida en que la UE se ve afectada en los ámbitos de los usos civil y militar, así como de la autoridad del Estado fuera del ámbito de la justicia penal, ap. 69. (2020/2013(INI)). (DOUE C 456/04, de 10 de noviembre de 2021).

11 Barona Vilar, S.: "Cuarta revolución industrial (4.0.) o ciberindustria en el proceso penal: revolución digital, inteligencia artificial y el camino hacia la robotización de la justicia", *Revista Jurídica Digital UANDES*, 2019, vol. 3, núm. 1, pp. 15-16.

también presenta múltiples desafíos en relación con su propia naturaleza y con el impacto de sus aplicaciones, especialmente en lo que concierne a la transparencia, la privacidad de los datos, la gobernanza y el entrenamiento de los algorítmicos. Lo que más preocupa es su posible contribución a la amplificación de los sesgos presentes en los datos que los alimentan, exacerbando así las desigualdades, las brechas sociales y la inequidad. Por ello reviste de gran importancia la necesidad de asentar los cimientos y andamiaje de estos sistemas inteligentes par poder desarrollar un entorno confiable.

Precisamente, la confiabilidad de la IA ha sido una preocupación de organismos internacionales, como la Organización para la Cooperación y el Desarrollo Económicos quien, mediante la adopción, en mayo de 2019, de los Principios de la OCDE sobre la Inteligencia Artificial[12], busca proteger los estándares internacionales dirigidos a la construcción y despliegue de sistemas de IA fiables, seguros y justos. Los estándares son siempre necesarios, pero aquí devienen esenciales para la aplicación en procesos en los que se hallen vinculadas personas en riesgo de vulnerabilidad o vulnerables, respetando en todo momento la dignidad humana y contribuyendo a una sociedad inclusiva.

En concreto, el Principio 1 ha reconocido que la inteligencia artificial debe fundamentar su desarrollo en el crecimiento inclusivo, el desarrollo sostenible y en el bienestar que, aunado con el Principio 2, se deberá realizar con base en unos valores centrados en el ser humano y la Justicia, donde destaca la importancia de los valores democráticos, la biodiversidad y la equidad para lograr una sociedad más justa. En este progreso no puede olvidarse la necesidad de transparencia y capacidad de explicación de los algoritmos (Principio 3), así como su trazabilidad para poder ponderar los riesgos (Principio 4) y evitar, así, una vulneración o merma de los derechos de las personas y que los sistemas de IA se caractericen por la robustez, la seguridad y la protección. Para su consecución, el Principio 5 cierra el ciclo al exigir la observancia del correcto funcionamiento de la IA al amparo de un régimen de responsabilidad.

Estos Principios deben complementarse con otros dos documentos clave. Por un lado, las Directrices Éticas para una IA fiable, establecidas por la Comisión Europea[13], que buscan orientar la aplicabilidad de estos sistemas inteligentes. Y, por otro lado, con la Recomendación sobre la ética de la inteligencia artificial de la UNESCO, adoptada el 23 de noviembre de 2021[14], dirigida a garantizar que todas estas transformaciones se alineen con los derechos humanos y los ODS.

12 Documento disponible en: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

13 Documento publicado el 8 de abril de 2019 y elaborado por el Grupo Independiente de Expertos de Alto Nivel sobre Inteligencia Artificial, creado en junio de 2018. Contenido del texto disponible en: https://op.europa.eu/es/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1

14 Documento disponible en: https://unesdoc.unesco.org/ark:/48223/pf0000381137_spa

Respecto de las Directrices Éticas, es importante señalar que el Grupo Independiente de Expertos resalta la importancia del seguimiento y cumplimiento de tales principios y estándares, en tanto en cuanto "la IA tiene el potencial de transformar significativamente la sociedad. La IA no es un fin en sí mismo, sino un medio prometedor para favorecer la prosperidad humana y, de ese modo, mejorar el bienestar individual y social y el bien común, además de traer consigo progreso e innovación.

En particular, los sistemas de IA pueden ayudar a facilitar el logro de los Objetivos de Desarrollo Sostenible de las Naciones Unidas, como la promoción del equilibrio entre mujeres y hombres y la lucha contra el cambio climático, la racionalización del uso que los seres humanos hacemos de los recursos naturales, la mejora de la salud, la movilidad y los procesos de producción y el seguimiento de los avances en los indicadores de sostenibilidad y cohesión social"[15]. Ahora bien, para alcanzar tal fin se torna imprescindible desarrollar protocolos y mecanismos para controlar y garantizar la fiabilidad de la IA, minimizando los potenciales riesgos que podrían colocar en una situación altamente perjudicial a las personas vulnerables o potencialmente vulnerables.

En este sentido, una IA fiable debe fundarse en estándares y valores que garanticen el respeto de los derechos fundamentales mediante la prevención de los riesgos inherentes a la utilización de este tipo de herramientas inteligentes, no solo a través de la protección de los principios de igualdad y equidad de las personas, sino también de neutralidad tecnológica, evitándose cualquier tipo de discriminación arbitraria, siendo imprescindible una mayor exigencia de transparencia y trazabilidad de la herramienta, sin olvidar el irrenunciable respeto de la autonomía humana en la adopción de las decisiones.

En la misma aparece la "Carta ética europea sobre el uso de la inteligencia artificial en los sistemas judiciales y su entorno"[16], identificando una serie de principios que pretender actuar como guía de la implementación de la IA en el ámbito judicial, a saber: respeto por los derechos fundamentales; prohibición de discriminación entre personas o grupos de personas; calidad y seguridad en los datos que sirvan para configurar los algoritmos; la transparencia, imparcialidad y Justicia de los códigos y lenguaje del algoritmo y, finalmente, el control de su correcto funcionamiento.

Con todo ello vuelve a quedar demostrada la relación y necesaria colaboración entre los factores tecnológico y humano para evitar que la IA se convierta en un

15 Directrices Éticas para una IA fiable, ap. 9.

16 Adoptada por el Grupo de Trabajo sobre la Calidad de la Justicia (CEPEJ-GT-QUAL) del Consejo de Europa en diciembre de 2018.

instrumento discriminatorio[17]. Para lograr este objetivo de establecer un marco para una IA fiable se deben garantizar principios como el respeto de los derechos humanos en la implementación sus servicios, tales como la protección de datos y de privacidad, la diversidad, la no discriminación y la equidad, al mismo tiempo que se asegure una gestión eficiente de la calidad de los sistemas, donde prime la seguridad y la imparcialidad de la decisión algorítmica.

Por lo tanto, es cierto que el uso responsable y ético de la IA contribuye a la mejora y rendimiento de procesos automatizados, así como agiliza y simplifica tareas arduas y costosas. Sin embargo, un uso irresponsable de la IA puede tener un efecto negativo y servir para reforzar y consolidar discriminaciones sistémicas, agrandar las brechas sociales, obstaculizar e incluso impedir el acceso de determinadas poblaciones y colectivos a los derechos sociales.

II. LA IA Y LOS ODS: SU NECESARIA ALINEACIÓN.

La Agenda 2030 y sus 17 Objetivos de Desarrollo sostenible[18] (en adelante, ODS) nacieron con la clara voluntad de transformar la sociedad, su pensamiento, su filosofía, su forma de hacer y entender la realidad…, pero siempre con la mira puesta en un objetivo claro: la sostenibilidad económica, social y ambiental. Con esta finalidad ha diseñado una hoja de ruta que viene delimitada por los 17 ODS y 169 metas que "hace necesario transformar el paradigma de desarrollo dominante en uno que nos lleve por la vía del desarrollo sostenible, inclusivo y con visión de largo plazo" y donde se "pone a la igualdad y dignidad de las personas en el centro"[19].

En este compromiso universal, llamado a mejorar nuestra sociedad, la IA puede jugar, y así lo hará, un papel determinante en la consecución y logro de las distintas metas proyectadas. Efectivamente, la tecnología más avanzada puede ponerse al servicio de las Agencias y Organizaciones Internacionales, de Administraciones, de ONGs, etc. y contribuir a la optimización de todos los análisis e indicadores, así como mejorar los procesos y tiempos de respuesta a los problemas y desafíos identificados.

En el ámbito de la Justicia son varias las muestras de lo que la IA puede contribuir en la mejora y agilización de los procesos. No obstante, aunque vamos poco a poco

17 Para Montesinos, la responsabilidad de la decisión final "debe recaer siempre en una persona". Montesinos García, A.: "Inteligencia Artificial y ODR·, en AA.VV.: *Justicia algorítmica y neuroderecho: una mirada multidisciplinar"* (dir. por S. Barona Vilar), Tirant lo Blanch, Valencia, 2021, p. 527.

18 El contenido de cada uno de los ODS establecidos en la Agenda 2030 se puede consultar en el siguiente enlace: https://www.un.org/sustainabledevelopment/es/2015/09/la-asamblea-general-adopta-la-agenda-2030-para-el-desarrollo-sostenible/

19 Agenda 2030, pág. 7. Documento disponible en: https://repositorio.cepal.org/server/api/core/bitstreams/cb30a4de-7d87-4e79-8e7a-ad5279038718/content

conociendo el poder, la capacidad, el alcance y el impacto de las herramientas de IA desarrolladas, su increíble potencial hace que continúe siendo desconocida en muchos aspectos. Igualmente, como todo avance y novedad, habida cuenta de su gran proyección en cuanto a su colaboración con los operadores jurídicos, son varios y complejos los desafíos que presenta.

En este trabajo hemos querido resaltar aquellos retos que, de no afrontarlos, profundizarían y perpetuarían las brechas y desigualdades sociales, perjudicando sobremanera a personas tradicionalmente castigadas por la discriminación y prejuicios de las sociedades. Estos desafíos pivotan en torno a la configuración de la IA mediante algoritmos, esas operaciones matemáticas complejas y tan poco comprensibles. En este sentido, la manera en que los algoritmos se nutren de datos y cómo los gestiona y analiza puede no ser la mejor ni la más adecuada al hallarse sesgos o elementos discriminatorios.

La posible existencia de sesgos algorítmicos se une a la opacidad de su creación y configuración, lo que dificulta la explicabilidad del algoritmo y, con ello, la posible quiebra de principios esenciales como el de motivación de las resoluciones si se deja la toma de decisión completamente en manos de la máquina. El equilibrio entre el factor humano y el factor tecnológico es clave para el correcto funcionamiento de estas herramientas y sistemas de IA.

1. Primer reto: sesgos algorítmicos.

El beneficio que puede aportar una herramienta de IA se verá diluido si su configuración perpetúa, consolida y agrava las desigualdades de nuestra sociedad. Los algoritmos se nutren de "un conjunto finito de reglas/comandos, generalmente en la forma de una lógica matemática, que permite obtener un resultado a partir de elementos de entrada"[20]. Sin embargo, todos sabemos que "ni la neutralidad maquínica es tan neutral, ni la neutralidad humana lo es"[21]. Las personas tenemos sesgos, prejuicios, opiniones, valores… que en no pocas ocasiones definen nuestra conducta, criterios o juicios, de forma que debemos trabajar en evitar impregnar de tal subjetividad a la máquina.

A tal fin, disponer de un buen *dataset* deviene crucial para el desarrollo de esta tecnología. Ahora bien, la compilación de información que servirá para alimentar la herramienta plantea una doble dificultad. Por un lado, la protección del derecho a la privacidad de los datos e información, muchas veces sensible. Para evitar la manipulación indebida o la comercialización de tales datos, deberá regularse la

20 Council of Europe Commissioner for Human Rights: *Unboxing Artificial Intelligence: 10 steps to protect Human Rights*, 2019, p. 24. Documento disponible en: https://rm.coe.int/unboxing-artificial-intelligence-10-steps-to-protect-human-rights-reco/1680946e64

21 Barona Vilar, S.: *Algoritmización del Derecho,* cit., p. 618.

recogida de datos buscando el equilibrio entre el derecho a la protección de datos y privacidad y la necesidad de configurar debidamente la herramienta de IA. Por otro lado, la codificación del lenguaje "inteligente" a partir de información de la realidad. Deberá atenderse a una correcta gestión y tratamiento de datos con el fin de contar con información completa, suficiente y carente de vicios o prejuicios, pues de lo contrario los resultados que arroje la máquina serán erróneos.

La codificación del lenguaje se antoja compleja dado que no todas las circunstancias pueden reducirse a números ni tampoco objetivarse hasta el punto de que la estandarización consecuente sea, al final, una mera generalización de los supuestos, sin atender a las particularidades de los distintos casos. Asimismo, la propia naturaleza de la IA permite su aprendizaje a partir de los datos introducidos o *feedback* y la interacción con el entorno. Este riesgo de sesgos o desviaciones se acentúa cuando se trata de herramientas de *Deep learning,* siendo actualmente la mayor preocupación la eliminación de los posibles sesgos.

Estas ecuaciones matemáticas analizan un importante número de datos[22], entre los que encontramos información sobre género, edad, nacionalidad e incluso, en ocasiones, creencias religiosas o ideológicas, extraídas de evidencias empíricas existentes, para poder arrojar un resultado -o una predicción- acerca de la probabilidad de que concurra una situación de riesgo, pero al hacerlo pueden servirse de criterios y soluciones pasadas que podían contener sesgos que ahora estas máquinas replicarán, excepto si se aplica un criterio o factor corrector para evitar esa codificación del pasado[23].

La existencia de sesgos es una de las grandes preocupaciones no solo de la utilización de la IA, sino también de su regulación. Inquietud compartida por la Comisión y expresamente recogida en las Directrices "Generar confianza en la inteligencia artificial centrada en el ser humano"[24], en concreto en lo que concierne precisamente a la "Diversidad, no discriminación y equidad" (título V).

La Comisión manifiesta que "[L]os conjuntos de datos utilizados por los sistemas de IA (tanto para el entrenamiento como para el funcionamiento) pueden verse afectados por la inclusión de sesgos históricos involuntarios, por no estar completos o por modelos de gobernanza deficientes. La persistencia en estos sesgos podría dar lugar a una discriminación (in)directa. También pueden producirse daños por

22 Pérez Estrada, J.: "La inteligencia artificial como prueba científica en el proceso penal español", *Revista Brasileira de Direito Processual Penal*, 2021, vol. 7, núm. 2, p. 1392.

23 Manifiestan la misma preocupación por la mirada de la técnica al pasado, Batelli, E.: "La decisión robótica: algoritmos, interpretación y justicia predictiva", *Revista de Derecho Privado*, 2020, núm. 38, p. 51 y Nieva Fenoll, J.: "Inteligencia Artificial y Proceso Judicial: perspectivas tras un alto tecnológico en el camino", *Revista General de Derecho Procesal,* 2022, núm. 57, p. 16.

24 Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: *Generar confianza en la inteligencia artificial centrada en el ser humano* (COM/2019/168 final).

la explotación intencionada de sesgos (del consumidor) o por una competencia desleal. Por otra parte, la forma en la que se desarrollan los sistemas de IA (por ejemplo, la forma en que está escrito el código de programación de un algoritmo) también puede estar sesgada. Estos problemas deben abordarse desde el inicio del desarrollo del sistema".

Una propuesta de solución para resolver estos problemas de sesgos algorítmicos sería el establecimiento de equipos de diseño heterogéneos y diversificados[25], que atendieran a la realidad plural y la diversidad sexual, racial, cultural que existe en el mundo. Igualmente, resulta de lo más conveniente y oportuno consultar a las partes interesadas que puedan verse afectadas por el sistema. Los sistemas de IA deberían atender a todo el abanico de capacidades, aptitudes, habilidades y necesidades humanas y aplicar un enfoque universal que permitiera alcanzar la igualdad de acceso a todas las personas.

Comprobamos, pues, que el sesgo algorítmico puede tener varias causas, que Lazcoz[26] agrupa en tres categorías y con gran impacto en la exacerbación de las desigualdades.

En primer lugar, "sesgos introducidos por datos incorrectos, irrelevantes o incompletos", que aluden a la insuficiencia del *dataset*, tanto a nivel cualitativo como cuantitativo. Por un lado, la base de datos puede no ser lo suficientemente completa como para constituir una muestra significativa porque un determinado colectivo haya quedado infrarrepresentado o "porque, en ocasiones, esos datos no constituyan reflejo fiel del espectro total de situaciones y realidades que se pretenden aprehender, al centrarse sólo en alguna o algunas de ellas"[27]. Por otro lado, aun cuando se disponga de un amplio conjunto de datos, puede suceder que no reflejen todo el abanico de situaciones y circunstancias (de vulnerabilidad), lo que ofrecería una visión parcial de la realidad (del vulnerable), no pudiendo analizar correctamente todas las situaciones.

En segundo lugar, "sesgos por una distribución desigual real de las variables" o "sesgos sociales", que son aquellos datos que reflejan situaciones sociales históricamente desiguales o discriminatorias y que son replicados al establecerse perfiles o patrones de conducta, lo que perpetuaría la situación discriminatoria, especialmente con personas de raza negra, migrantes, mujeres, o personas con discapacidad.

25 Con el mismo parecer, Scassera, S.: "La desigualdad automatizada. Industrialización, exclusión y colonialismo digital", *Nueva Sociedad,* 2021, núm. 294, 2021, p. 51.

26 Lazcoz Moratinos, G.: "Modelos algorítmicos, sesgos y discriminación", en AA.VV.: *FODERTICS 9.0. Estudios sobre tecnologías disruptivas y Justicia* (dir. por F. Bueno De Mata), Comares, Granada, 2021, pp. 286-287.

27 Saiz Garitaonandia, A.: "Personas vulnerables, justicia e inteligencia artificial. Motivos para permanecer alerta", cit., p. 99.

Finalmente, en tercer lugar, reconoce los "sesgos relacionados con la transformación de los datos para facilitar su procesamiento posterior por el modelo algorítmico", esto es, que el tratamiento y gestión de los datos que van a introducirse o han sido introducidos para su posterior análisis automatizado no sea el idóneo.

En consecuencia, la replicación o creación de sesgos y prejuicios por una mala configuración del *dataset* o del propio algoritmo preocupa sobremanera por su afectación y consecuencias negativas a los colectivos tradicionalmente oprimidos y vulnerables, lo que provocaría un recrudecimiento de la violencia, abuso y desigualdad estructural. Se trata de evitar, en definitiva, que los estereotipos ya existentes en nuestra sociedad pueden trasladarse, y perpetuarse, en el mundo digital.

Llama la atención el impresionante desarrollo de sistemas de IA en el orden penal, configurándose para atender distintos fines, tales como la predicción del riesgo de reincidencia, de delitos e incluso de fraudes -financieros o a la Seguridad Social-, entre otras funciones. Ahora bien, el ejemplo paradigmático de la existencia de sesgos en estas herramientas lo constituye el caso *Wisconsin vs. Loomis*[28], donde se demostró la existencia de un sesgo por razón del origen racial de las personas en la herramienta COMPAS (*Correctional Offender Management Profiling for Alternative Sanctions*), en la que un algoritmo predictivo de aprendizaje automático o *machine learning* adoptado por la Administración de Justicia de Estados Unidos arrojaba porcentajes de riesgo de reincidencia mucho mayores cuando la persona sospechosa era de raza negra.

Este suceso refleja no solo el problema de la opacidad de la configuración del algoritmo, sino también la asunción de la discriminación histórica de las personas de raza negra, sin la debida justificación de la necesidad de tomar en consideración la raza para el análisis y sin la combinación de dicho factor con otros que resultaren oportunos para verificar el nivel de riesgo como acusado. Llama la atención el contraste entre el refuerzo de los derechos y garantías de la persona acusada y la utilización de algoritmos predictivos que mantienen y reproducen las desigualdades estructurales de la sociedad. Unas distinciones (arbitrarias) que buscamos erradicar precisamente con la (supuesta) objetivación de los aspectos a tomar en consideración para estimar un determinado nivel de riesgo o la culpabilidad.

28 *State v. Loomis*, 881 N.W.2d 749 (Wis. 2016).
Para un análisis de esta resolución judicial y sus implicaciones en el proceso, véase, por todos, García Sánchez, M.D.: "Retos del uso de la Inteligencia Artificial en el proceso: impugnaciones con fundamentación algorítmica y Derecho a la tutela judicial efectiva", en AA.VV.: *FODERTICS 9.0. Estudios sobre tecnologías disruptivas y Justicia* (dir. por F. Bueno De Mata), Comares, Granada, 2021, pp. 233-244.

Por otra parte, encontramos también ejemplos de discriminaciones en el uso de la IA en otros ámbitos, no judiciales, pero con repercusiones jurídicas. En concreto en el ámbito del crédito, donde los sesgos son el resultado del análisis automatizado, por ejemplo, del nivel de riesgo para la concesión del crédito. A tal fin, las entidades elaboran un perfil[29] de la persona solicitante para lo que utilizan criterios tales como el nivel de renta, el historial crediticio o su capacidad de pago, pero también se ha descubierto que se tienen en cuenta factores como la edad o el género[30].

Desde instancias supranacionales se viene instando a todas las organizaciones a erradicar este tipo de discriminaciones injustificadas, y más aún evitar su reproducción en las herramientas de IA. Sin embargo, como podemos comprobar, las desigualdades y desequilibrios continúan, pues factores como el género no se entiende que sigan teniéndose en cuenta porque no aportan ningún tipo de factor ni elemento que pudiera afectar a la resolución de concesión o no de un crédito o de cualquier otro tipo de financiación.

Al contrario, simplemente sirve para perpetuar estereotipos que aumentan la brecha de género existente, especialmente en personas de mayor edad. Ello hace que, por ejemplo, personas con menores recursos económicos o que hubieran sido incluidas anteriormente en listados de morosidad sean inmediatamente excluidas o vean sus condiciones menos ventajosas, lo que agravaría su situación financiera e incrementaría el nivel de riesgo de exclusión social.

No olvidemos tampoco que la salud ha sido un factor considerado para la concesión de créditos, negándose automáticamente a personas con enfermedades como el cáncer, aun habiéndolo superado. Dos han sido las importantes consecuencias de esta realidad discriminatoria por culpa de la algoritmización.

La primera, el nacimiento de un nuevo derecho, el llamado "derecho al olvido oncológico"[31], que refiere a la potestad conferida a las personas a solicitar la

29 De conformidad con el artículo 4.4) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), debemos entender por elaboración de perfiles "toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física". (DOUE L 119/1, de 4 de mayo de 2016).

30 La propia Recomendación sobre la ética de la inteligencia artificial, adoptada el 23 de noviembre de 2021 por la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura ya recomendaba que "Los Estados Miembros deberían velar por que los estereotipos de género y los sesgos discriminatorios no se trasladen a los sistemas de IA, sino que se detecten y corrijan de manera proactiva" (ap. 90). Documento disponible en el siguiente enlace: https://unesdoc.unesco.org/ark:/48223/pf0000381137_spa

31 BARONA señala que, junto a este nuevo derecho, son múltiples las repercusiones jurídicas que tiene esta revolución digital, tales como "la regulación de las cookies y el marketing relacional, el régimen legal de las aplicaciones, la economía colaborativa, el ciberespacio, la cibercriminalidad, la ciberseguridad, la

supresión de información personal y datos relacionados, tal y como recoge el Reglamento General de Protección de Datos (RGPD). En concreto, podrán pedirlo pacientes que hayan superado un cáncer, siempre y cuando hubieran transcurrido 5 años desde la finalización del tratamiento sin recaída en el momento de la suscripción del crédito, seguro o hipoteca. Estamos ante la eliminación de una desigualdad histórica, cuyos efectos se han extendido también a otro colectivo tradicionalmente marginado y reprimido como las personas con la enfermedad VIH/SIDA.

Precisamente, desde instancias supranacionales se ha abordado esta causa de discriminación que tantos perjuicios estaba ocasionando para el desarrollo de las personas con normalidad, dictando la Resolución del Parlamento Europeo, de 16 de febrero de 2022, sobre el refuerzo de Europa en la lucha contra el cáncer: hacia una estrategia global y coordinada[32], aprobado el 16 de febrero de 2022, donde se indica que "Considerando que el objetivo del Plan no debe ser solo luchar contra un problema de salud pública esencial y ayudar a los pacientes a vivir más y mejor, sino que también debe ser iniciar una reducción de las desigualdades e injusticias y reducir la carga social y económica de la enfermedad; que la Comisión debe promover un enfoque centrado en el paciente y basado en los derechos de los ciudadanos integrando consideraciones de justicia, sostenibilidad, equidad, solidaridad, innovación y colaboración en el núcleo mismo del Plan, incluida su Iniciativa para Ayudar a los Niños con Cáncer" (ap. E).

Para dar cumplimiento con esta Resolución, que instaba a reforzar la lucha contra el cáncer mediante una estrategia global y coordinada en toda Europa, el 27 de junio de 2023 se aprobó por el Consejo de Ministros el Real Decreto-ley 5/2023, de 28 de junio, por el que se adoptan y prorrogan determinadas medidas de respuesta a las consecuencias económicas y sociales de la Guerra de Ucrania, de apoyo a la reconstrucción de la isla de La Palma y a otras situaciones de vulnerabilidad; de transposición de Directivas de la Unión Europea en materia de modificaciones estructurales de sociedades mercantiles y conciliación de la vida familiar y la vida profesional de los progenitores y los cuidadores; y de ejecución y cumplimiento del Derecho de la Unión Europea[33], que puso en marcha este derecho al olvido oncológico.

protección de los derechos fundamentales en internet, la e*Justice*, las nuevas técnicas de investigación tecnológicamente avanzadas, la incidencia del *Big Data* en todas las áreas jurídicas, la regulación de internet y especial protección de los menores en internet, el internet de las cosas, entre otros tantos. Barona Vilar, S.: *Algoritmización del Derecho,* cit., p. 73.

32 2020/2267(INI).

33 BOE núm. 154, de 29 de junio de 2023.
El Preámbulo, apartado III, señala que "el capítulo II incorpora medidas para hacer efectivo el derecho al olvido en la contratación de seguros y productos bancarios de los pacientes de patologías oncológicas una vez transcurrido un determinado período de tiempo desde la finalización del tratamiento sin recaída. Para ello se establece, por un lado, la nulidad de las cláusulas que excluyan a una de las partes por haber padecido cáncer; y, por otra, la prohibición de discriminación en la contratación de un seguro a una persona

En concreto, destacan los artículos 209, apartado Dos, por el que se modifica la DA 5ª de la Ley 50/1980, de 8 de octubre, de Contrato de Seguro y artículo 210, por el que se modifica la DA Única del Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias, aprobado por Real Decreto Legislativo 1/2007, de 16 de noviembre[34].

De conformidad con esta modificación, ya "no se podrá discriminar a las personas que tengan VIH/SIDA, ni por otras condiciones de salud. En particular, se prohíbe la denegación de acceso a la contratación, el establecimiento de procedimientos de contratación diferentes de los habitualmente utilizados por el asegurador o la imposición de condiciones más onerosas, por razón de tener VIH/SIDA, o por otras condiciones de salud, salvo que se encuentren fundadas en causas justificadas, proporcionadas y razonables, que se hallen documentadas previa y objetivamente".

Igualmente señala la nulidad, en relación con las cláusulas no negociadas individualmente, de "aquellas cláusulas, estipulaciones, condiciones o pactos que excluyan a una de las partes" bien por tener VIH/SIDA u otras condiciones de salud, bien por ser supervivientes de un cáncer antes de la fecha de suscripción del contrato o negocio jurídico, introduciendo un factor temporal de cinco años desde la finalización del tratamiento radical sin recaída posterior.

Esto es importante para la configuración de la herramienta de IA correspondiente, que "no puede estar diseñada, ni ser aplicada, generando discriminaciones, incurriendo en la creación de perfiles con sesgo, marginación o exclusión de colectivos especialmente vulnerables. El principio de igualdad, la presunción de inocencia, la protección de la privacidad y de los datos personales, así como el pleno ejercicio del derecho de defensa y el derecho a un proceso justo que no pueden verse afectados en ningún caso. Para ello es determinante la observancia de los Códigos éticos y sus principios desde las estructuras institucionales o privadas que apliquen sistemas de inteligencia artificial en el ámbito de la justicia"[35].

Dada la utilidad y funcionalidad de la IA, Saiz propone "sugerir el uso de la propia IA de cara a poder detectar esos sesgos. Su gran capacidad de proceso de datos y determinación de patrones puede ser de gran ayuda para percibir

por haber sufrido una patología oncológica, una vez transcurridos, en ambos casos, cinco años desde la finalización del tratamiento radical sin recaída posterior. Además, para suscribir un seguro de vida tampoco habrá obligación de declarar si se ha padecido cáncer una vez cumplido el mencionado plazo, ni se podrán tomar en consideración dichos antecedentes oncológicos, a estos efectos".

34 BOE núm. 287, de 30 de noviembre de 2007.

35 Martín Diz, F.: "Capítulo 45. Inteligencia artificial y proceso: garantías frente a eficiencia en el entorno de los derechos procesales fundamentales", en AA.VV.: *Justicia: ¿garantías "versus" eficiencia?* (coord. por R. Bellido Penadés), Tirant lo Blanch, Valencia, 2019, p. 822.

los *bias* ocultos en las decisiones pasadas, ser conscientes de los mismos y ponerlos remedio"[36]. Ello sería posible en tanto en cuanto las conclusiones o resultados que arrojan los algoritmos son resultado de complejas ecuaciones y operaciones que tratan de hallar patrones de conducta, establecer modelos de respuesta y, al hacerlo, pueden también estar replicando los sesgos introducidos por las personas, pudiendo incluso amplificarlos si no somos capaces de detectar el error y la desigualdad al manejar y analizar grandes cantidades de datos. De momento, empero, no contamos con algoritmos cuya finalidad sea la de eliminar las desigualdades existentes en género, raza, etnia, estatus socioeconómico, entre otros muchos factores.

La segunda de las consecuencias de este cambio normativo refiere del planteamiento sobre quién asumiría la responsabilidad de la vulneración del derecho a no ser objeto de discriminación arbitraria por motivos de raza, género, etnia, nivel económico, nivel educativo, o enfermedad. La atribución de los efectos jurídicos de la decisión o acción automatizada que origina una discriminación a ciertos colectivos no es baladí.

Rodríguez De Las Heras apunta a que tal responsabilidad se atribuiría al operador "en la medida en que controla (o debería poder controlar) los riesgos de operar un sistema de IA que decide integrar en su actividad y, por tanto, beneficiarse de su funcionamiento"[37] siendo, en este caso, la propia entidad la infractora del principio de no discriminación.

La falta de exhaustividad del marco jurídico de la IA, aún en construcción, y el exigido respeto a la dignidad, la igualdad y la no discriminación de las personas, sienta la necesidad de articular cómo "deberán diseñarse, implementarse y ponerse en servicio sistemas de IA para satisfacer los principios de trazabilidad, explicabilidad, transparencia, supervisión humana, auditabilidad, no discriminación, explicación razonada de las decisiones, o acceso a un mecanismo de revisión de decisiones significativas"[38], y a quiénes deberá atribuirse la responsabilidad (civil, penal, administrativa…) -y, correlativamente, la legitimación pasiva- en caso de infracción y discriminación.

Consecuencia de todo ello, podemos confirmar que la revolución que la IA ha supuesto -no solo en el ámbito de la Justicia sino también en general- y el elevado

36 Saiz Garitaonandia, A.: "Personas vulnerables, justicia e inteligencia artificial. Motivos para permanecer alerta", en AA.VV.: *Personas vulnerables y tutela penal* (dir. por N.J. De La Mata Barranco y A.I. Pérez Machío), Thomson Reuters Aranzadi, Cizur Menor (Navarra), 2023, p. 102. En la misma línea se pronuncia Ferrante, E.: "Inteligencia artificial y sesgos algorítmicos ¿Por qué deberían importarnos?", *Nueva Sociedad,* 2021, núm. 294, p. 34.

37 Rodríguez De Las Heras Ballell, T.: "Inteligencia Artificial en el sector bancario: reflexiones sobre su régimen jurídico en la Unión Europea", *ICE. Revista de Economía,* 2022, núm. 926, p. 103.

38 *Ibídem,* p. 105.

grado de fiabilidad que muchos sistemas han demostrado, servirá para alcanzar los ODS de la Agenda 2030, diseñando un sistema más justo e inclusivo para la ciudadanía. No obstante, su introducción en todos los ámbitos de la sociedad, pero en especial de la Justicia, debe realizarse de una forma garantista, tuitiva de los Derechos Fundamentales. A tal fin, reiteramos que la prevalencia del factor humano en el control y toma de decisiones deviene clave para lograr una justicia inclusiva, segura y confiable, precisamente para asegurar la protección y defensa, en términos de igualdad, de personas vulnerables o en una situación de vulnerabilidad.

2. Segundo reto: trazabilidad y explicabilidad del algoritmo.

La IA aporta un gran avance y cuenta con una importante proyección, pero también tiene limitaciones, entre las que destaca la opacidad del contenido del algoritmo. Precisamente, esta opacidad o falta de transparencia se equipara al concepto de caja negra[39] porque resulta muy complejo comprender y conocer los entresijos del algoritmo.

En otras palabras, la dificultad de la utilización de algoritmos o sistemas predictivos reside en la necesidad de mayor transparencia (ante la completa falta de ella) y, correlativamente, del conocimiento de la lógica del algoritmo y de la capacidad de justificación de la decisión. Por una parte, la transparencia en el tratamiento de datos, en la configuración y en la técnica empleada por el algoritmo debe ser un principio de actuación de la Administración de Justicia, sin olvidarnos, por otra parte, de la búsqueda de un equilibrio entre este principio y el derecho de protección de datos.

La administración de justicia ante una eventual vulneración de derechos por la existencia de sesgos en la IA, por ejemplo, se dificulta sobremanera dada la poca confiabilidad y transparencia del algoritmo. Estas exigencias de transparencia y fiabilidad obedecen a la necesidad de disponer de una explicación de la decisión que permita conocer el proceso de análisis y entender así el resultado que haya emitido la herramienta inteligente.

Es más, la falta de cualquiera de estos requisitos podría suponer la ilegalidad del propio algoritmo, tal como ha sucedido con SyRI, dedicado a la evaluación de características personales de los ciudadanos, declarado ilegal por el Tribunal de Distrito de la Haya, en su Sentencia de 5 de febrero de 2020[40], anteriormente

39 Price, W.N.: "Artificial Intelligence in Health Care: Applications and Legal Issues", *U of Michigan Public Law Research Paper,* 2017, núm. 599, p. 2.

40 Asunto C/09/550982/HA ZA 18-388 (NJCM et al./Países Bajos. Sobre esta Resolución, véase, Cotino Hueso, L.: "SyRI, ¿a quién sanciono? Garantías frente al uso de inteligencia artificial y decisiones automatizadas en el sector público y la sentencia holandesa de febrero de 2020", *La Ley Privacidad*, 2020, núm. 4.

utilizado por parte del Gobierno de los Países Bajos para combatir el fraude a la Seguridad Social. En consecuencia, la trazabilidad y explicabilidad del algoritmo permite lograr el objetivo de disponer de una IA confiable, dado que la confianza se basa en conocer cómo funciona el algoritmo y cuáles son los parámetros que considerar cuando analiza un supuesto concreto.

El Libro Blanco de la Unión Europea sobre Inteligencia Artificial aborda esta opacidad y la problemática que subyace para los derechos humanos, alegando que "[L]as características particulares de numerosas tecnologías de IA, como la opacidad («efecto caja negra»), la complejidad, la imprevisibilidad y un comportamiento parcialmente autónomo, pueden hacer difícil comprobar el cumplimiento de la legislación vigente de la UE sobre la protección de los derechos fundamentales e impedir su cumplimiento efectivo. Puede ser que las fuerzas y cuerpos de seguridad y las personas afectadas carezcan de los medios para comprobar cómo se ha tomado una decisión determinada con ayuda de la IA y, por consiguiente, si se han respetado las normas pertinentes. Las personas físicas y las personas jurídicas pueden enfrentarse a dificultades en el acceso efectivo a la justicia en situaciones en las que estas decisiones les afecten negativamente"[41].

Preocupación por la "transparencia e inteligibilidad del funcionamiento de los algoritmos y los datos con los que han sido entrenados" que también recoge la UNESCO debido a su impacto "en, entre otros, la dignidad humana, los derechos humanos y las libertades fundamentales, la igualdad de género, la democracia, los procesos sociales, económicos, políticos y culturales, las prácticas científicas y de ingeniería, el bienestar animal y el medio ambiente y los ecosistemas"[42].

La solución pasaría por disponer de *softwar*es abiertos que permitan conocer los *inputs* e información analizada, auditar los datos y poder cuestionar el resultado. Solo así se garantizarían los derechos y se evitaría la manipulación, mala interpretación o error en los *outputs*.

3. Tercer reto: la motivación de las resoluciones.

Mucho se habla de la automatización de los procesos, de la funcionalidad de las herramientas de IA, e incluso de la figura del Juez robot, esto es, del papel que debe desempeñar la IA en el sistema de justicia. Cuestión nada baladí, porque aunque parezca una realidad lejana, está cada día más próxima.

41 Libro Blanco de la Comisión Europea sobre Inteligencia Artificial titulado "Una aproximación europea a la excelencia y a la confianza", de 19 de febrero de 2020. COM (2020) 65 final, pp. 14-15.

42 UNESCO, *Recomendación sobre la ética de la inteligencia artificial*, 2021, p. 1. [SHS/BIO/REC-AIETHICS/2021]. Documento disponible en: https://unesdoc.unesco.org/ark:/48223/pf0000380455_spa

Como acertadamente señala Martín Diz, la IA debe desempeñar, de momento, una labor asistencial[43]. Las características y funcionamiento de las herramientas de IA justificarían esta necesidad de supervisión por parte del justiciable. En este sentido, como afirma Guzmán Fluja, el "desarrollo de la IA general y el continuo avance y perfeccionamiento en la programación de algoritmos, así como la depuración en cantidad y calidad de los datos a manejar, y la mejora del autoaprendizaje de las IA'[44] requieren del factor humano, lo que impediría, en un escenario futuro, prescindir del justiciable para la toma de la decisión.

Con todo, tampoco podemos despistarnos y olvidarnos de que la exigencia de motivación de las decisiones adoptadas en el marco de un proceso es un derecho comprendido en el derecho de acceso a la tutela judicial efectiva (artículo 24 de la Constitución), que establece la obligación del justiciable de ofrecer una "respuesta razonada, motivada y congruente con las pretensiones oportunamente deducidas por las partes", así como una exigencia consagrada en el artículo 120.3 y susceptible, en consecuencia, de amparo constitucional.

Una obligación que no desaparece con la utilización de una IA, más bien al contrario, debe reforzarse, ya que los *outputs* de la IA pueden "contribuir a motivar más y mejores decisiones ahora difíciles, ambivalentes, que en ocasiones se adoptan en el vacío o sin suficiente información fruto de la incapacidad de tener en cuenta ciertas variables o datos relacionados'[45].

En este sentido, conocer cuál ha sido el razonamiento y la interpretación que se ha dado de las circunstancias para determinar la concurrencia de uno o varios riesgos se convierte en el eje para garantizar el derecho a un proceso justo y el derecho de defensa. Por el contrario, desconocer cómo y por qué se ha emitido una probabilidad, un resultado o una decisión que afecta a los derechos de las personas, entrañaría un grave riesgo para la seguridad jurídica y para los principios procesales.

Aquí es donde entendemos, y vemos muy claro, que el factor humano no puede -o no debería- ser reemplazado por una máquina quien, de momento, no es capaz de replicar la función argumentativa del órgano juzgador, por lo que

43 Martín Diz, F., "Modelos de aplicación de Inteligencia Artificial en justicia: asistencial o predictiva versus decisoria", en AA.VV.: *Justicia algorítmica y neuroderecho: una mirada multidisciplinar* (ed. por S. Barona Vilar), Tirant lo Blanch, Valencia, 2021, pp. 65-85.

44 Guzmán Fluja, V. C., "Proceso penal y justicia automatizada", *Revista General de Derecho Procesal*, 2021, núm. 53, p. 33.

45 Simón Castellano, P.: *Justicia cautelar e Inteligencia Artificial*, Bosch, Madrid, 2021, p. 71. En el mismo sentido se pronuncia Pérez Ragone, A.: "Justicia civil en la era digital y artificial: ¿Hacia una nueva identidad?, *Revista Chilena de Derecho*, 2021, vol. 48, núm. 2, p. 215. y Planchadell Gargallo, A.: "Inteligencia Artificial y medidas cautelares", en AA.VV.: *Justicia algorítmica y neuroderecho, Una mirada multidisciplinar* (ed. por S. Barona Vilar.), Tirant Lo Blanch, Valencia, 2021, p. 410.

hablaríamos de un escenario donde el juzgador y la máquina de IA pudieran convivir para una mejora del sistema de justicia.

III. LA IA Y LA PERSPECTIVA DE VULNERABILIDAD: UNA REFLEXIÓN FINAL.

La introducción de aplicaciones de IA presenta un gran potencial y una impresionante proyección por su utilidad y eficacia para el progreso, pero también por su versatilidad, por su capacidad de adaptación y contribución al progreso en sectores como la medicina, la agricultura, la ciencia, la educación, etc., lo que nos permite afirmar que será una gran contribución y ayuda en la consecución de los ODS.

Sin embargo, todo este profundo impacto positivo en las sociedades y en su desarrollo económico, político, social y ambiental, quedara ensombrecido -y eclipsado en algunos aspectos- por el agravamiento de las desigualdades sociales ya existentes, reforzando la marginalización de algunas poblaciones.

El temor a los sistemas de IA no proviene tanto de la posibilidad de que las máquinas inteligentes reemplacen a las personas habida cuenta de la mayor optimización y eficacia de los procesos -algo que lleva sucediendo décadas- sino por el hecho de que estos sistemas tratan de emular y, en cierta manera, de reproducir, el pensamiento humano. Ahora bien, la gran diferencia que impide que esa aspiración se torne realidad, es la imaginación, la creatividad y la capacidad de crítica del ser humano y de las que la máquina aún carece. De ahí que la máquina se limite a valorar un resultado mediante la estandarización y patronaje de similares escenarios.

Aquí surge el mayor desafío. Si nos preguntamos si la IA puede llegar a agravar, exacerbar o generar situaciones de desequilibrio y desigualdad, deberíamos responder afirmativamente -al menos, de momento-. La privacidad de datos, la accesibilidad a la tecnología, la falencia de competencias digitales, entre otros, son elementos a considerar para evitar agravar las brechas sociales, la exclusión social y la discriminación, esto es, para impedir que colectivos que son actualmente vulnerables lo sigan siendo por culpa del uso de una IA que pretende ser útil, fiable y eficaz pero que, en realidad, no respeta los valores éticos ni la igualdad entre las personas.

Debe, por tanto, llevarse a cabo una reflexión profunda, sosegada, y bajo una perspectiva de vulnerabilidad, sobre la configuración y utilización de la IA en el ámbito judicial, estableciéndose límites inquebrantables que defiendan la legalidad, la igualdad y la no discriminación entre las personas.

BIBLIOGRAFÍA

Barona Vilar, S.: "Cuarta revolución industrial (4.0.) o ciberindustria en el proceso penal: revolución digital, inteligencia artificial y el camino hacia la robotización de la justicia", *Revista Jurídica Digital UANDES*, 2019, vol. 3, núm. 1, pp. 1-21.

Barona Vilar, S.: "Inteligencia artificial o la algoritmización de la vida y de la justicia", *Revista Boliviana de Derecho,* 2019, núm. 28.

Barona Vilar, S.: *Algoritmización del Derecho y de la Justicia. De la Inteligencia Artificial a la Smart Justice,* Tirant lo Blanch, Valencia, 2021.

Batelli, E.: "La decisión robótica: algoritmos, interpretación y justicia predictiva", *Revista de Derecho Privado*, 2020, núm. 38.

Castillejo Manzanares, R.: "Las nuevas tecnologías y la inteligencia artificial como retos post-covid19", *Revista General de Derecho Procesal,* 2022, núm. 56.

Conde Fuentes, J.: "La inteligencia artificial y la figura del juez-robot", en AA.VV.: *Modernización, eficiencia y aceleración del proceso* (dir. por S. Pereira Puigvert y M.J. Pesqueira Zamora), Aranzadi, Cizur Menor (Navarra), 2022, pp. 115-136.

Cotino Hueso, L.: "SyRI, ¿a quién sanciono? Garantías frente al uso de inteligencia artificial y decisiones automatizadas en el sector público y la sentencia holandesa de febrero de 2020", *La Ley Privacidad*, 2020, núm. 4.

Ferrante, E.: "Inteligencia artificial y sesgos algorítmicos ¿Por qué deberían importarnos?", *Nueva Sociedad,* 2021, núm. 294, pp. 27-36.

García Sánchez, M.D.: "Retos del uso de la Inteligencia Artificial en el proceso: impugnaciones con fundamentación algorítmica y Derecho a la tutela judicial efectiva", en AA.VV.: *FODERTICS 9.0. Estudios sobre tecnologías disruptivas y Justicia* (dir. por F. Bueno De Mata), Comares, Granada, 2021, pp. 233-244.

Gómez Colomer, J. L.: "Unas reflexiones sobre el llamado «juez-robot», al hilo del principio de independencia judicial", en AA.VV.: *Justicia algorítmica y neuroderecho: una mirada multidisciplinar"* dir. por S. Barona Vilar), Tirant lo Blanch, Valencia, 2021, pp. 243-263.

Guzmán Fluja, V. C.: "Proceso penal y justicia automatizada", *Revista General de Derecho Procesal*, 2021, núm. 53.

Lazcoz Moratinos, G.: "Modelos algorítmicos, sesgos y discriminación", en AA.VV.: *FODERTICS 9.0. Estudios sobre tecnologías disruptivas y Justicia* (dir. por F. Bueno De Mata), Comares, Granada, 2021, p. 283-294.

Marcos Francisco, D.: "Smart ODR y su puesta en práctica: el salto a la inteligencia artificial", *Revista General de Derecho Procesal,* 2023, núm. 59.

Martín Diz, F.: "Capítulo 45. Inteligencia artificial y proceso: garantías frente a eficiencia en el entorno de los derechos procesales fundamentales", en AA.VV.: *Justicia: ¿garantías "versus" eficiencia?* (coord. por R. Bellido Penadés), Tirant lo Blanch, Valencia, 2019, pp. 815-827.

Martín Diz, F.: "Justicia digital post-covid19: el desafío de las soluciones extrajudiciales electrónicas de litigios y la inteligencia artificial", *Revista de Estudios Jurídicos y Criminológicos,* 2020, núm. 2, pp. 41-74.

Martín Diz, F., "Modelos de aplicación de Inteligencia Artificial en justicia: asistencial o predictiva versus decisoria", en AA.VV.: *Justicia algorítmica y neuroderecho: una mirada multidisciplinar* (ed. por S. Barona Vilar), Tirant lo Blanch, Valencia, 2021, pp. 65-85.

Montesinos García, A.: "Empleo de la inteligencia artificial en algunas fases del proceso judicial civil: prueba, medidas cautelares y sentencia", *Actualidad civil*, 2022, núm. 11, pp. 1-31.

Montesinos García, A.: "Inteligencia Artificial y ODR", en AA.VV.: *Justicia algorítmica y neuroderecho: una mirada multidisciplinar"* (dir. por S. Barona Vilar), Tirant lo Blanch, Valencia, 2021, pp. 507-531.

Nieva Fenoll, J.: "Inteligencia Artificial y Proceso Judicial: perspectivas tras un alto tecnológico en el camino", *Revista General de Derecho Procesal,* 2022, núm. 57.

Oliver, N., *Inteligencia Artificial, naturalmente. Un manual de convivencia entre humanos y máquinas para que la tecnología nos beneficie a todos,* ONTSI, Madrid, 2020.

Pérez Estrada, J.: "La inteligencia artificial como prueba científica en el proceso penal español", *Revista Brasileira de Direito Processual Penal*, 2021, vol. 7, núm. 2, pp. 1385-1410.

Pérez Ragone, A.: "Justicia civil en la era digital y artificial: ¿Hacia una nueva identidad?, *Revista Chilena de Derecho,* 2021, vol. 48, núm. 2, pp. 203-229.

Planchadell Gargallo, A.: "Inteligencia Artificial y medidas cautelares", en AA.VV.: *Justicia algorítmica y neuroderecho, Una mirada multidisciplinar* (ed. por S. Barona Vilar.), Tirant Lo Blanch, Valencia, 2021, pp. 384-419.

Price, W.N.: "Artificial Intelligence in Health Care: Applications and Legal Issues", *U of Michigan Public Law Research Paper,* 2017, núm. 599, pp. 1-7.

Rodríguez De Las Heras Ballell, T.: "Inteligencia Artificial en el sector bancario: reflexiones sobre su régimen jurídico en la Unión Europea", *ICE. Revista de Economía,* 2022, núm. 926, pp. 93-107.

Saiz Garitaonandia, A.: "Personas vulnerables, justicia e inteligencia artificial. Motivos para permanecer alerta", en AA.VV.: *Personas vulnerables y tutela penal* (dir. por N.J. De La Mata Barranco y A.I. Pérez Machío), Thomson Reuters Aranzadi, Cizur Menor (Navarra), 2023, pp. 93-110.

Scassera, S.: "La desigualdad automatizada. Industrialización, exclusión y colonialismo digital", *Nueva Sociedad,* 2021, núm. 294, pp. 49-60.

Simón Castellano, P.: *Justicia cautelar e Inteligencia Artificial*, Bosch, Madrid, 2021.

UNESCO, *Recomendación sobre la ética de la inteligencia artificial*, 2021. [SHS/BIO/REC-AIETHICS/2021].

ALGORITMIZACIÓN DE LA CONCESIÓN DE MEDIDAS CAUTELARES EN EL PROCESO PENAL PARA LA PROTECCIÓN DE VÍCTIMAS DE VIOLENCIA DE GÉNERO. ¿ES CAPAZ VIOGEN DE INTERPRETAR EL "PERICULUM IN MORA"?*

ALGORITHMISATION OF THE GRANTING OF PRECAUTIONARY MEASURES IN CRIMINAL PROCEEDINGS FOR THE PROTECTION OF VICTIMS OF GENDER VIOLENCE. IS VIOGEN CAPABLE OF INTERPRETING THE "PERICULUM IN MORA"?

Actualidad Jurídica Iberoamericana Nº 21, agosto 2024, ISSN: 2386-4567, pp. 384-407

* Estudio redactado en el marco del Proyecto "Claves para una justicia digital y algorítmica con perspectiva de género", PID2021-123170OB-I00 financiado por MCIN/ AEI/10.13039/501100011033.

Raquel BORGES BLÁZQUEZ

ARTÍCULO RECIBIDO: 29 de mayo de 2023
ARTÍCULO APROBADO: 1 de julio de 2024

RESUMEN: La irrupción de la inteligencia artificial (IA) en el sector jurídico es una realidad. En el proceso penal español para la protección de las víctimas de violencia de género hace años que los agentes policiales hacen uso del sistema VIOGEN para la evaluación del riesgo de violencia. Este sistema hace un cálculo de la probabilidad de reincidencia de un agresor respecto de su víctima, una vez éste ha cometido una infracción que, además, ha sido denunciada. En la práctica observamos un elevado automatismo a aceptar la valoración del sistema actuarial, por ello la pregunta de investigación que buscamos resolver en este trabajo es si el sistema VIOGEN es capaz de interpretar el periculum in mora en la concesión de medidas cautelares que compete al juez. Respondida esta cuestión debemos plantearnos en qué supuestos, bajo qué parámetros y qué responsabilidad podríamos atribuirle a VIOGEN.

PALABRAS CLAVE: Medidas cautelares; VIOGEN; algoritmos; "periculum in mora"; violencia de género.

ABSTRACT: *The irruption in the use of artificial intelligence (AI) in the legal sector is a reality nowadays. Spanish Police officers have been using the VIOGEN system for years in order to assess the risk of violence in criminal proceedings regarding protection of gender-based violence victims. This system calculates the aggressor's probability to reoffend the victim after a first offence has been reported. In practice we observe a high degree of automatism in accepting the system's assessment. This is the reason for the research question in this paper which is to determine if the VIOGEN system is capable of interpreting the periculum in mora in the process of granting precautionary measures which lies within the judge's responsibilities. Once this question has been answered we must ask ourselves the amount of responsibility attributed to the VIOGEN system and in which cases or under what specific parameters should it be used.*

KEY WORDS: *Precautionary measures; VIOGEN; algorithms; "periculum in mora"; gender violence.*

I. LA ORDEN DE PROTECCIÓN COMO MEDIDA CAUTELAR EN EL PROCESO PENAL POR VIOLENCIA DE GÉNERO.

Si bien vamos a tratar las órdenes de protección de las víctimas de violencia de género como medidas cautelares, pues es así como las denomina el legislador penal español, antes de comenzar me gustaría alinearme con el planteamiento de la profesora Barona Vilar que diferencia entre medidas cautelares como aquellas que sirven a los fines del proceso y medidas preventivas como aquellas que no buscan garantizar la presencia del agresor en el juicio, sino proteger a la víctima de nuevos ataques.[1]

Refiere Gómez Neira en auto sobre medidas cautelares durante la instrucción que éstas "son instrumentos procesales que sirven para otorgar efectividad al proceso mismo y más específicamente a la sentencia que, en su día, se dicte. (…) la actuación del ius puniendi por parte del Estado a través del proceso penal requiere "tiempo", y precisamente ese tiempo implica en sí mismo un importante riesgo de que la resolución que en su día llegue a dictarse sea inútil; sobre todo cuando el sujeto pasivo aprovecha para sí mismo las indeseables dilaciones procesales, para hacer que dicha resolución sea ilusoria y por ende, inejecutable" En resumen, "la finalidad que da verdaderamente significado a la regulación de las medidas cautelares es la función de garantía de la efectividad del proceso, ya que comporta un real y efectivo aseguramiento de su desarrollo."[2]

Es ésta, "mutatis mutandis", la misma función que tienen las órdenes de protección. La decisión final respecto de la culpabilidad del agresor requiere de tiempo, pero el Estado tiene conocimiento de la comisión de un posible delito con el consecuente riesgo de reiteración delictiva. Para evitar que el agresor vuelva a

1 Barona Vilar, S.: *Medidas cautelares en el proceso penal,* Prontuario de Derecho Procesal 3, Honduras, 2015, pp. 74-77.

2 AJPII 20 mayo 2022 (ECLI:ES:JPII:2022:187), p. 2

• Raquel Borges Blázquez
Profesora Ayudante Doctora de Derecho Procesal, Universitat de València.
Correo electrónico: Raquel.Borges@uv.es

atentar contra bienes jurídicos protegidos de la víctima, el artículo 544ter ofrece la herramienta jurídica para dictar una medida cautelar de protección. Si bien aquí no estamos garantizando estrictamente los fines del proceso (el riesgo de fuga o la destrucción de pruebas garantizan estrictamente los fines del proceso), sí estamos garantizando la seguridad de la víctima y conjurando el riesgo de reiteración delictiva. Continúa el auto indicando que el objetivo de la medida es "evitar los riesgos de inefectividad de los derechos sujetos a protección que puedan ocasionarse por la duración de un proceso".[3] En otras palabras, de poco serviría que una mujer con un riesgo muy elevado denuncie a su agresor si el Estado, una vez tener conocimiento del hecho, no toma medidas. Tal vez se acabe condenando al agresor pero sin una medida cautelar de protección de la víctima, la condena poco o nada importe a la víctima si, para el día que se dicta la sentencia, la ha vuelto a agredir o, incluso, la ha matado.

Las órdenes de protección forman parte de la prevención terciaria, es decir, medidas dirigidas a evitar que se vuelva a producir una nueva agresión, una vez que se han producido otras agresiones previas. Una forma mediante la que la protección de las víctimas puede ser garantizada es incapacitando físicamente a sus agresores, esto es, privándolos de libertad para que dejen de atacar o amenazar a sus víctimas. Una alternativa menos invasiva son las órdenes de protección, en cuyo caso una autoridad judicial ordenará a la persona violenta que debe dejar a "su" víctima en paz.[4]

Con nuestra orden de protección, comparto con Serrano Hoyo, más que una nueva medida cautelar, lo que se creó fue un mecanismo de coordinación de las medidas cautelares penales y civiles ya existentes que además se proyecta en el ámbito asistencial. Y es que, por lo que se refiere al proceso penal, no se crearon nuevas medidas cautelares, sino que el artículo 544ter en su apartado sexto se limita a remitirse a las ya existentes siendo que la orden de protección tiene una naturaleza accesoria respecto del proceso penal en marcha. Su novedad radica en la posibilidad de articular las medidas cautelares penales ya existentes con medidas cautelares civiles -también ya existentes- en un mismo instrumento, dotándolas así de una mayor eficacia y ofreciendo la posibilidad de desplegar sus efectos también en el orden asistencial.[5]

3 Idem

4 Traducción libre: "One way in which protection can be procured is by physically incapacitating violent persons: by placing them in detention they can be prevented from attacking or harassing their victims anew. A less invasive alternative, however, is to issue a protection order, in which case a judicial authority orders the violent person to leave the victim in peace". Van Der Aa, S., Niemi, Johanna; S., Lorena; Ferreira, A., Baldry, A.: "Mapping the legislation and assessing the impact of Protection Orders in the European member states", *Daphne,* p. 31.

5 Serrano Hoyo, G.: "Algunas cuestiones procesales que plantea la Orden de Protección de las víctimas de la violencia doméstica", *Anuario de la Facultad de Derecho*, 2004, pp. 72-73.

Por tanto, deberá cumplir las características que les pedimos a las medidas cautelares, directamente vinculadas con su finalidad aseguratoria: "A) Instrumentalidad.- La medida cautelar se justifica solo con relación a un proceso. Garantizan tanto el proceso de declaración, mediante la presencia del sujeto y preservando cuantos elementos de prueba puedan servir en el mismo, como la efectividad del cumplimiento de la sentencia condenatoria, a saber, el proceso de ejecución. De ahí su naturaleza instrumental. B) Provisionalidad.- La medida cautelar no pretende convertirse en definitiva, y es por ello que desaparece cuando deja de ser necesaria en el proceso principal. Solo se mantienen en tanto en cuanto permanezcan las circunstancias que motivaron su imposición, y éstas pueden variarse en el tiempo. C) Temporalidad.- La duración de la medida cautelar es limitada, dado que, por su propia naturaleza, se extingue al desaparecer las causas que la motivaron. D) Variabilidad.- La medida cautelar puede ser modificada, e incluso alzada, cuando se altera la situación de hecho que dio lugar a su adopción. E) Jurisdiccionalidad.- Corresponde exclusivamente a los órganos del Poder Judicial adoptar las medidas cautelares".[6]

Sin intención de adelantar conclusiones, el objetivo del trabajo es valorar cómo podrían casar la jurisdiccionalidad que requiere la adopción de las medidas cautelares y el empleo de VIOGEN en la decisión de la posible adopción de la medida cautelar a modo de diligencia pericial para la valoración del riesgo. Actualmente, el sistema es utilizado por parte de los agentes policiales para la valoración policial del riesgo y la gestión de la seguridad de las víctimas de violencia de género. Más tarde, se incluye entre las circunstancias que valora el juzgador para la decisión de la adopción de la medida cautelar. Pero el juzgador no tiene acceso al algoritmo para ir modificando las respuestas dependiendo del riesgo intrínseco a cada momento del proceso. Por tanto, si el legislador decidiese incluir VIOGEN como una suerte de pericial que colabore con la motivación judicial, el juzgador debería tener la posibilidad de modificar las respuestas en atención a la variabilidad de la medida. Además, VIOGEN sería simplemente una herramienta de auxilio a la motivación puesto que "la jurisdiccionalidad, a su vez, implica lo siguiente: 1. La decisión cautelar es solo posible por el órgano jurisdiccional. 2. Toda medida cautelar ha de ser debidamente motivada. La motivación, es manifestación del artículo 120 CE y, por supuesto, del genérico derecho a la tutela judicial efectiva del artículo 24.1 CE. La necesidad de motivar exige al juez instructor exponer en la resolución de forma suficientemente comprensible cuales son los elementos y cuáles son las razones tenidas en cuenta en su adopción. 3. El juez instructor ha de realizar un examen formal de la proporcionalidad y de la racionalidad de la medida a adoptar, efectuando un juicio de ponderación entre el derecho o derechos afectados y los intereses que tal afectación trata de proteger".[7] Por lo

6 AJPII 20 mayo 2022 (ECLI:ES:JPII:2022:187), p. 2

7 Idem

tanto, la necesaria motivación del auto impediría dejar el control de la decisión en la máquina ya que no caben las motivaciones por remisión.

1. Requisitos que deben cumplir las medidas cautelares: el "fumus boni iuris" y el "periculum in mora".

Las medidas cautelares para garantizar el cumplimiento efectivo de la sentencia, se basan en los siguientes fundamentos:[8] 1) "periculum in mora", o daño específico derivado de la duración de la actividad jurisdiccional penal, que puede aprovecharse por el investigado para colocarse en una situación que puede acabar frustrando la ulterior efectividad de la sentencia, peligro que puede referirse tanto a la persona como al patrimonio del investigado; y 2) "fumus boni iuris", que comporta la probabilidad o verosimilitud de la existencia de un hecho criminal imputado (objeto), esto es, indicios suficientes que permitan mantener la imputación de un hecho delictivo al sujeto afectado por la medida o la responsabilidad civil de éste. Estos fundamentos deben ser interpretados desde la proporcionalidad, que requiere un juicio de razonabilidad sobre la finalidad perseguida y de las circunstancias concurrentes. Una medida desproporcionada o irrazonable, tal y como ha indicado el Tribunal Constitucional,[9] no sería propiamente cautelar, sino que tendría un carácter punitivo en cuanto al exceso.[10]

Ambos requisitos se encuentran indicados en el artículo 503 LECrim respecto de la prisión provisional como medida más gravosa de privación de libertad. Si el juzgador considerase que no es necesaria la privación de libertad para garantizar los fines del proceso, es posible hacer uso de una reducción, que no privación, de la libertad deambulatoria y de comunicación por medio de los artículos 544bis y 544ter que regulan las órdenes de alejamiento y protección. Además, existe un desarrollo jurisprudencial respecto del contenido y alcance de los requisitos puesto que la jurisprudencia, al fin y al cabo, es la encargada de valorar la existencia de éstos y motivar por medio de auto.

A modo de ejemplo, refiere la Audiencia Provincial de Bilbao, "El fumus boni iuris o apariencia y justificación del derecho subjetivo, estriba en el proceso penal en la atribución del hecho punible a una persona determinada conforme a criterios de racionalidad teniendo en cuenta el momento procesal en el que se acuerda la medida. Esto es tanto como decir que para que tomar esta decisión es necesario

8 Realizo un estudio más exhaustivo en: Borges Blázquez, R.: "Obligaciones estatales positivas de prevención y medidas de protección civiles para víctimas de violencia doméstica y de género. Una apuesta a favor de su regulación", *Actualidad Jurídica Iberoamericana,* 2020, núm. 13, pp. 898-929.

9 A este respecto: Barona Vilar, S.: "Prisión provisional: 'solo' una medida cautelar (Reflexiones ante la doctrina del TEDH y del TC, en especial de la STC 46/2000, 17 febrero)", *Actualidad Penal,* 2000, núm. 42, pp. 891-911.

10 Barona Vilar, S.: *Medidas cautelares,* cit., pp. 74-77; Barona Vilar, S.: "¿Una nueva concepción expansiva de las medidas cautelares en el proceso penal?", *Revista del Poder Judicial,* 2006, núm. especial 19, pp. 237-264.

que se haya producido una imputación. El periculum in mora o daño jurídico derivado de la duración del procedimiento viene determinado en el proceso penal, en principio, por el peligro de fuga o por el peligro de ocultación del imputado".[11]

En el mismo sentido, la Audiendia Provincial de Madrid, "Ha de incidirse que esta Sección de la Ilma. Audiencia Provincial ya ha señalado (STAP de 26/07/2012) que la afectación a derechos fundamentales de la persona a la que se impone una medida cautelar de esta naturaleza, como son los derechos a la libertad deambulatoria, y a la presunción de inocencia, en sus dos vertientes tradicionales, requiere que cualquier decisión que se adopte por parte del Juzgador, además de cumplir el deber general de motivación (expresivo de las razones jurídicas que le han movido a adoptar la decisión), se pondere específicamente la adecuación de la medida desde la contemplación de los riesgos que con ella se quieren conjurar, lo que exige un análisis específico del "fumus boni iuris", de que el riesgo puede ser conjurado (teniendo en cuenta la proporcionalidad), mediante el alejamiento de la persona a quien se imputan indiciariamente unos hechos graves, de la o las personas sobre las que se temen ataques a su vida, a su integridad física, a su libertad y al resto de los bienes jurídicos expuestos en la LECRIM, y en el art. 57 CP. Por todo ello, y a los efectos de determinación del peligro, debe evaluarse los antecedentes existentes en la causa, de los que se pueda inferir que el denunciado puede seguir cometiendo hechos violentos atentatorios contra la integridad física o moral de la víctima, con objeto de determinar si es necesaria la medida, a fin de evitar nuevos actos de agresión." Continúa la Audiencia haciendo referencia a la inmediación: "también hemos de poner de manifiesto, el valor que en estos supuestos tiene el denominado principio de inmediación por parte del Juzgador de instancia, que es quien realmente ha practicado a lo largo de la instrucción de la causa las diligencias de investigación, y ha podido observar de primera mano aquellas circunstancias que concurren a la hora de acordar la medida cautelar".[12] En definitiva, el elemento humano que, como más adelante se explicará, la máquina no debe, ni puede con la Constitución actual, borrar.

En cuanto a la medida de alejamiento (incluida, o no, en una orden de protección), separar al agresor de la víctima es el elemento básico para garantizar la protección adecuada de la integridad de la víctima.[13] En relación con esta medida, sería recomendable reemplazar el sistema de protección que consiste en ocultar y refugiar a la víctima en centros de acogida, ya que esto conlleva una revictimización

11 AAP BI 26 Junio 2021 (ECLI:ES:APBI:2021:1172A), p. 2

12 AAP M 8 marzo 2023 (ECLI:ES:APM:2023:689A), p. 3.

13 El Pleno del Consejo General Judicial de 21 de marzo de 2001 indicó, en relación con la problemática jurídica que conlleva la violencia doméstica que "la adopción de estas prohibiciones y el ejecutivo cumplimiento por parte de los órganos jurisdiccionales, del Ministerio Fiscal y de las Fuerzas y Cuerpos de Seguridad aparece en este momento como una necesidad perentoria para lograr una protección real de las víctimas y alejar a éstas de la sensación de desamparo institucional que padecen"

que empeora la difícil situación en que las víctimas se encuentran.[14] La medida de alejamiento puede ser adoptada como medida cautelar, pena accesoria, medida de seguridad, condición para la suspensión o como una de las reglas que trae consigo la situación de libertad provisional. Si es como medida cautelar, su adopción urgente es necesaria para que el agresor reaccione y se dé cuenta de que el Estado castiga su conducta violenta. Explica Barona Vilar, esta medida no tiene como objetivo garantizar la presencia del agresor en el juicio, si no de que "su fundamento es meramente preventivo, no cautelar ni aseguratorio procesal del sujeto pasivo de la causa". De este modo, considera la autora, sí concurre el "fumus boni iuris" (elementos de convicción suficientes para poder sostener que es probable que el imputado sea autor de un hecho punible) pero no el "periculum in mora" (no hay riesgo de fuga ni de obstaculizar la investigación) siendo que el único fundamento es proteger a la víctima.[15]

Además, no resulta fácil establecer a priori si ambos requisitos se dan debido a la fase en la que nos encontramos: "esa valoración sobre la concurrencia de tales requisitos ha de enmarcarse, además, en el juicio de inferencia indiciaria propio de la fase procesal en que se encuentra la presente causa. En este sentido, conviene recordar que los indicios racionales de criminalidad (STS de 9/01/2006), según su especifica utilidad procesal, es decir, según para qué se necesitan en el desarrollo del procedimiento, significan siempre la asistencia de datos concretos reveladores de un hecho importante para las actuaciones judiciales, lo que exige, una mayor o menor, intensidad en cuanto a su acreditación, según la finalidad con que se utilizan. Así, la máxima intensidad ha de existir cuando esos indicios sirven como medio de prueba de cargo (prueba de indicios), en cuyos casos han de estar realmente acreditados y han de tener tal fuerza probatoria que, partiendo de ellos, pueda afirmarse, sin duda razonable alguna, la concurrencia del hecho debatido; y en otras ocasiones, sin que concurra una verdadera prueba, han de constar en las actuaciones procesales algunas diligencias a partir de las cuales puede decirse que exista probabilidad de delito y de que una determinada persona es el responsable del mismo."[16] En este sentido, como veremos en el siguiente apartado, la posibilidad de algorimizar el "periculum in mora" podría servir como herramienta de auxilio al juzgador para la decisión respecto de otorgar, o no, una medida cautelar.

2. ¿Cómo algorimizamos el "periculum in mora"?

Explica Neira Pena[17] que es posible algorimizar el "periculum in mora" pero no el "fumus boni iuris" porque la apariencia del buen derecho se refiere a un hecho

14 En este sentido, De Urbano Castillo, E.: "El alejamiento del agresor, en los casos de violencia familiar", *La Ley,* 2001, núm. 5248.

15 Barona Vilar, S.: *Medidas cautelares,* cit., pp. 74-77, p. 182.

16 AAP M 8 marzo 2023 (ECLI:ES:APM:2023:689A), p. 4.

17 Neira Pena, A. M.: "Inteligencia Artificial y tutela cautelar. Especial referencia a la prisión provisional", *Rev. Bras. de Direito Processual Penal,* Porto Alegre, 2021, vol. 7, num. 3, pp. 1897-1933.

que ya ha sucedido y los algoritmos funcionan prediciendo aquello que es posible o probable que suceda en el futuro.

Reflexiona brillantemente la autora respecto de la valoración del "fumus boni iuris", "implica reconstruir hechos pasados, atribuirles un nivel de verosimilitud y valorarlos jurídicamente, las herramientas de justicia predictiva o valoración de riesgos no deben de influir en absoluto en este juicio, que debe realizarse de forma independiente y autónoma a toda circunstancia ajena a la comisión del hecho delictivo que se investiga."[18] Concluye muy acertadamente al indicar que éste es "un juicio de imputación reforzado (…) reconstruir el pasado, valorando jurídicamente los hechos investigados, y no de predecir el futuro ni de asignar probabilidades a hechos inciertos. Y en este ámbito, la IA es más limitada. (…) Difícilmente puede sustituir al juicio jurisdiccional, que además ha de guiarse por principios como el in dubio pro reo o el favorecimiento de la libertad personal, que encierran auténticos valores, no siempre reducibles a una secuencia lógica o a un umbral estadístico".[19] En definitiva, coincido plenamente con la autora que el concepto de apariencia de buen derecho busca confirmar si se cometió el delito previo que daría lugar a la emisión de una medida de protección si, además, concurre el peligro en la mora. Pero esta apariencia de buen derecho no puede confundirse con la posibilidad de reincidir, pues éste es el segundo requisito para la concesión de una medida cautelar.

Respecto del uso de las herramientas algorítmicas para evaluar el peligro en la mora Neira Pena y Planchadell Gargallo no ven inconveniente. "La configuración legal del periculum in mora facilita que puedan incluirse en el algoritmo los distintos presupuestos legalmente previstos (riesgo de fuga, gravedad de la pena, riesgo de reiteración delictiva, riesgo de destrucción de pruebas) de forma que cuando los mismos concurran la máquina "recomiende" la adopción de la medida cautelar persona más adecuada."[20] El juicio de los propios juzgadores trae consigo sesgos y el uso de sistemas de IA podría compensarlos en la construcción del algoritmo y en la selección de datos[21] En el mismo sentido, Planchadell Gargallo considera que "la objetivación de dichos riesgos a través de algoritmo podría ser de utilidad para el órgano jurisdiccional, permitiéndole tomar la decisión más ponderada y proporcional posible a la situación concreta en que deba decidirse."[22]

18 Ibidem, p. 1907

19 Ibidem, p. 1908.

20 Planchadell Gargallo, A.: "Inteligencia Artificial y medidas cautelares", en AA. VV.: *Justicia algorítimica y neuroderecho. Una mirada multidisciplinar,* (coord. por S. Barona Vilar), Tirant lo Blanch, Valencia, 2021, p. 410.

21 Neira Pena, A. M.: "Inteligencia Artificial", cit., p. 1913

22 Planchadell Gargallo, A.: "Inteligencia Artificial", cit., p. 410.

Las decisiones deberán tomarse "respetando el principio de legalidad y asegurando la transparencia del proceso valorativo y decisional, el cual ha de desarrollarse de modo individualizado, atendiendo a las circunstancias particulares del caso concreto y de quienes sufren tales restricciones de derechos, lo que implica, en último término, que la decisión final, más o menos influida por la máquina, ha de ser tomada por aquel individuo en que se ha depositado la potestad jurisdiccional de forma exclusiva y excluyente, que no es otro que el juez."[23]

II. VIOGÉN Y ALGORITMIZACIÓN DEL RIESGO DE REINCIDENCIA.

Deviene necesario explicar, de manera muy breve el funcionamiento de la herramienta VIOGEN para, en los siguientes apartados poder valorar críticamente su futurible incorporación como una suerte de diligencia pericial que pueda emplear el juzgador en la motivación de la adopción de medidas cautelares.[24] Esta herramienta nació el año 2007 como materialización del mandato de los artículos 31.3 y 32 de la LOVG.[25] VIOGEN es, sin lugar a duda, el algoritmo más desarrollado de cuántos utilizan nuestras fuerzas y cuerpos de seguridad. Este algoritmo se ha desarrollado desde la SES del Ministerio del Interior. Su protocolo permite que los agentes valoren el riesgo que tiene una mujer que ya ha denunciado de sufrir una nueva agresión por parte de su pareja o expareja. En función del riesgo que le asigne el algoritmo, el protocolo contempla la adopción de determinadas medidas de protección policial para evitar la reincidencia gestionando el riesgo. La policía predictiva, por tanto, debe ir acompañada de intervenciones de algún tipo.[26]

Entre los objetivos generales de VIOGEN se encuentra el "facilitar la labor preventiva, emitiendo avisos, alertas y alarmas, a través de un subsistema de notificaciones automatizadas, cuando se detecte alguna incidencia o acontecimiento que pueda poner en peligro la integridad de la víctima."[27] Con ello, la policía tomará una serie de medidas dirigidas a garantizar la seguridad de la víctima. Más tarde, el formulario VIOGEN formará parte de aquellas diligencias que el juzgador tendrá en cuenta en la audiencia del artículo 544ter. Pero es precisamente el hecho de tomar una decisión de actuar de determinado modo después de obtener una valoración de riesgo lo que hace que nunca sepamos lo acertada que fue esa predicción. Supongamos que un algoritmo da un riesgo muy alto a una mujer víctima de

23 Neira Pena, A. M.: "Inteligencia Artificial", cit., p. 1927.

24 Respecto del sistema VIOGEN, escribí previamente un artículo más detallado y extenso en: Borges Blázquez, R.: "Inteligencia artificial y perspectiva de género: programar, investigar y juzgar con filtro morado", *Revista General de Derecho Procesal,* 2021, núm. 55, pp. 1-41.

25 González Álvarez, J. L.: "Sistema de seguimiento integral en los casos de violencia de género (sistema viogén)", *Cuadernos de la Guardia Civil,* 2018, núm. 56, p. 84.

26 González Álvarez, J. L., Santos Hermoso, J., Camacho-Collados, M.: "Policía predictiva en España. Aplicación y retos futuros", *Behavior & Law Journal,* 2020, vol. 6, núm. 1, pp. 29-30.

27 Guía de Procedimiento 2020 VIOGEN, p. 6.

violencia de género. Por tanto, la policía adopta inmediatamente medidas para evitar que su pareja vuelva a agredirla. Lo contrario, sería inmoral. Así, después de aplicar las medidas la pareja no la agrede. La cuestión que surge es: ¿acertó el algoritmo y fueron las medidas las que hicieron que no volviera a agredirla?, ¿o el riesgo no era tal y aún sin medidas la pareja no habría vuelto a agredirla? Hemos aceptado no conocer la efectividad real de la predicción a cambio de la protección de las víctimas.

Haciendo uso de la información disponible y con el objetivo de facilitar a los miembros de las fuerzas y cuerpos de seguridad del estado sus decisiones en materia de protección de víctimas refieren González Álvarez, Santos Hermoso y Camacho-Collados que se programó un mecanismo dual y transparente para los agentes que funciona del siguiente modo: cuando un policía recibe una denuncia por violencia de género cumplimenta la VPR. Tras la cumplimentación, el sistema VIOGEN aplica su primer algoritmo y calcula el riesgo de reincidencia que presenta el caso en ese momento pero no muestra el resultado todavía. Seguidamente, con la misma información calcula el riesgo de feminicidio utilizando el segundo de sus algoritmos. Si aparece riesgo mortal, se incrementa en un nivel el riesgo de reincidencia que se va a mostrar a los agentes junto con una alerta de riesgo de feminicidio que quedará reflejada en el atestado policial.[28] Respecto de la transparencia, como más adelante se verá, se ha criticado que VIOGEN no resulta tan transparente como sus creadores consideran ya que desconocemos el código fuente.[29]

La estabilidad y acierto de los pronósticos dependerá de si el episodio violento lo producen factores muy estáticos con una perspectiva futura poco modificable y, consecuentemente, un riesgo muy estable. O si, en cambio, se produce en presencia de circunstancias cambiantes y dependientes de las situaciones con pronósticos más sensibles a cualquier cambio y que solo se pueden anticipar mediante la evaluación de factores de riesgo dinámicos.[30] Además, el agente policial no tiene por qué aceptar sin más la evaluación del formulario, puede modificar el riesgo justificando los motivos de su actuación.[31] "Es importante señalar que, en todos los casos, la estimación del riesgo no descansa en una mera máquina, sino que el Sistema permite que los agentes policiales, que son los que mejor conocen los casos por

28 González Álvarez, J. L., Santos Hermoso, J., Camacho-Collados, M.: "Policía predictiva", cit., p. 33.

29 Cito expresamente el segundo resultado de la Auditoría Externa de VioGén: "VioGén no ha sido evaluado ni auditado de forma independiente. Los recursos y las encuestas al alcance público sobre la validez y la conveniencia de VioGén han sido realizados por personas que trabajan o tienen intereses en el ministerio y las fuerzas policiales. Los auditores o investigadores externos no tienen ninguna vía oficial o pública para acceder a los datos, y el acceso parece ser proporcionado por el Ministerio a su discreción". Éticas, *Auditoría Externa del Sistema VioGén,* Fundación Ana Bella, 2022, p. 34.

30 López-Ossorio, J. J., González Álvarez, J. L.; Andrés Pueyo, A.: "Eficacia predictiva de la valoración policial del riesgo de la violencia de género", *Psychosocial Intervention,* núm. 25, 2016, p. 3.

31 Ibidem, p. 7.

haberlos investigado en profundidad, puedan corregir el resultado automático del protocolo de valoración de riesgo cuando cuenten con información que así lo aconseje. (…) Así, al final de cada valoración policial de riesgo el Sistema VIOGEN resume las respuestas señaladas y pregunta por la conformidad del agente con el resultado automático, permitiendo que el usuario manifieste su desacuerdo y asigne el nivel de riesgo que él considera más apropiado, facilitando sus razones, permitiendo así el perfeccionamiento del Sistema."[32] Aunque en el 95% de los casos el personal de las Fuerzas y Cuerpos de Seguridad está de acuerdo con el riesgo asignado, existe la posibilidad de reasignación.[33]

A continuación vamos a explicar las diversas herramientas que componen VIOGEN por separado pues "cada una de estas herramientas funciona de manera autónoma, tienen sus propios factores de riesgo y su propio algoritmo matemático para la estimación final del nivel de riesgo." Además aunque sea una posibilidad con un uso anecdótico, esta "estimación policial del riesgo no descansa únicamente en el algoritmo matemático derivado de la investigación científica, sino que el Sistema permite que los agentes policiales puedan corregir, al alza, el resultado automático del protocolo, cuando cuenten con información que así lo aconsejen (Metodología Actuarial Ajustada)".[34]

1. VPR y VPER.

El sistema de valoración del riesgo tiene en cuenta dos factores y como interactúan. Por un lado, la peligrosidad del agresor. Por otro, la vulnerabilidad de la víctima. Es la interactuación de ambos factores la que nos ofrecerá el riesgo real del que debemos proteger a la víctima. Un mismo nivel de peligrosidad por parte del agresor puede dar resultados de riesgo diversos dependiendo de lo sumisa o empoderada que sea "su" víctima.

En España la valoración del riesgo se realiza mediante dos formularios (VPR y VPER) distintos pero complementarios. Este protocolo se implementa en un sistema informático en línea que conecta miles de usuarios de forma simultánea y multiagenda pues todos los entornos que se ocupan del seguimiento de las víctimas tienen acceso (policial, judicial, penitenciario y social).[35] El primer formulario "ayuda

32 González Álvarez, J. L., López-Ossorio, J. J., Muñoz Rivas, M.: "La valoración policial del riesgo de violencia contra la mujer pareja en España- Sistema Viogén", 2018, p. 56.

33 González Álvarez, J. L., López-Ossorio, J. J., Urruela, C., Rodríguez-Díaz, M.:"Integral Monitoring System in Cases of Gender Violence VioGén System", *Behavior & Law Journal*, 2018, num. 4(1), p. 37. Se obtuvo un elevado porcentaje de coincidencia (90,7%) en un estudio de casos registrados entre octubre y noviembre de 2016 con una muestra de 7.147 casos de seguimiento durante diez meses realizado para revisar el funcionamiento del sistema. López-Ossorio, J. J., Lonaiz, I., González Álvarez, J. L.: "Protocol for the police gender violence risk assessment (VPR4.0): Review of its performance", *Rev Esp Med Legal*, 2019, núm. 45(2), pp. 53-56.

34 Guía de Procedimiento 2020 VIOGEN, pp. 7-8.

35 González Álvarez, J. L., López-Ossorio, J. J., Muñoz Rivas, M.: "La valoración", cit., p. 43.

a los agentes a establecer el riesgo de que se repita la violencia a corto plazo en cinco niveles: no apreciado, bajo, medio, alto o extremo."[36] El segundo formulario, permite monitorizar los cambios y mantener actualizada la estimación del riesgo. El VPER solamente contempla dos variables -sin incidente o con incidente- y "se realiza una vez se celebre la vista judicial para resolver la solicitud de Orden de Protección, Alejamiento o la imposición de otras medidas cautelares o, en su caso, el correspondiente Juicio Rápido" para incorporar indicadores de riesgo y de protección sensibles a los escenarios que se abren después de la denuncia.[37]-

La herramienta VPR tiene una sensibilidad del 85% pero una especificidad del 53%[38] siendo una sensibilidad aceptable para confiarle las decisiones pero no una especificidad, pues su acierto equivale a lanzar una moneda al aire. De todas formas, nunca vamos a ser capaces de conocer su verdadera especificidad porque la adjudicación de un riesgo implica que se pongan en marcha una serie de medidas de protección y esto es esperable que influya en los parámetros de la siguiente valoración.

2. VPR 5.0-H. La valoración del riesgo de violencia mortal.

La valoración del riesgo de violencia mortal fue abordada en nuestro país tras la creación del Equipo Nacional de Revisión Pormenorizada de Homicidios por violencia de género. Parte de su éxito se debe a que se implicaron todas las instituciones gubernamentales que tenían responsabilidades en la materia (SES, Ministerio del Interior, Fiscalía, Delegación del Gobierno para la violencia de género, y el Observatorio contra la violencia doméstica y de género del CGPJ). Revisaron casos de diferentes años y de todo el territorio nacional con el objetivo de obtener una muestra lo suficientemente grande y representativa a nivel estadístico y territorial (víctima de violencia de género en entornos urbanos, en grandes urbes, en pequeñas ciudades, en entornos rurales, en pueblos, etc).[39] De los 60 feminicidios de media que se registran año tras año en nuestro país, en los años 2006 a 2019 solo el 26% contaban con denuncia previa. Esto puede deberse a que la víctima no quiso denunciar previamente a su agresor o a que no existían episodios previos al asesinato. Para poder realizar un análisis completo, se generaron VPR por parte de los equipos de revisión de aquellos feminicidios que no contaban con denuncia previa. Además, pudo comprobarse que los factores que utilizamos para predecir el riesgo de reincidencia no mortal no servían para predecir los feminicidios y viceversa. Esta conclusión era esperable ya que la bibliografía científica venía apuntando que la violencia mortal y no mortal en la

36 Ibidem, pp. 52 y 59.

37 Ibidem, pp. 61-63.

38 López-Ossorio, J. J., González Álvarez, J. L.; Andrés Pueyo, A.: "Eficacia predictiva", cit., pp. 1-7.

39 González Álvarez, J. L., Santos Hermoso, J., Camacho-Collados, M.: "Policía predictiva", cit., p. 32.

pareja pueden ser fenómenos diferentes asociados, por tanto, a circunstancias diferentes.[40]

Los resultados positivos[41] hicieron que esta escala se incluyese en el formulario de valoración del riesgo desde marzo de 2019. Así, este formulario tiene dos escalas diferentes: la primera (VPR), para estimar los riesgos de reincidencia con cinco niveles (no apreciado, bajo, medio, alto y extremo). La segunda (VPR 5.0-H), para apreciar el riesgo de feminicidio con dos niveles (bajo y alto).[42] Más adelante, se repite la valoración del riesgo de reincidencia (VPER) para aumentar la especificidad del instrumento.

III. FALENCIAS DEL SISTEMA VIOGEN.

Considero que VIOGEN debería modificar una serie de cuestiones si queremos convertirla en una verdadera herramienta algorítmica para el auxilio del juzgador en la decisión de toma de decisiones. Además, parece ser que el Ministerio del Interior está considerando incorporar una herramienta de "Machine Learning" al sistema VIOGEN. Esto no ha sido confirmado oficialmente pero "en diciembre de 2020 la empresa software SAS anunció que el Ministerio del Interior y la Unidad de Violencia de Género habían llegado a un acuerdo con SAS para incorporar la analítica de datos y lo que se ha denominado el "agente digital" para automatizar y agilizar ciertos procesos con el fin de aumentar la protección.'[43]

Sin intención de adelantar mis conclusiones, considero que ninguna herramienta de "Machine Learning" debería tener, con la constitución en la mano, la posibilidad de decidir respecto de la necesidad de una medida cautelar. Esta cuestión atentaría contra el derecho de defensa, al perder el hilo conductor y no poder conocer cómo se ha extraído dicho resultado. El tan manido ejemplo del caso Loomis a propósito del uso de COMPAS[44] que en este trabajo no vamos a tratar. Por tanto, en las próximas páginas, trataremos la posibilidad de convertir VIOGEN en una verdadera herramienta de valoración del "periculum in mora" como sistema actuarial. Aunque hoy en día los juzgadores hacen uso del sistema VIOGEN, la realidad es que no nació para el cálculo del "periculum in mora" sino como protocolo de valoración policial del riesgo de reincidencia. Si de verdad queremos otorgarle la capacidad de elemento decisorio del "periculum in mora" como

40 Ibidem, p. 33.

41 Esta herramienta presentó una sensibilidad de .81 y una especificidad de .61, un área bajo la curva de .81 y un valor predictivo positivo de .19 y un valor predictivo negativo de .97.

42 González Álvarez, J. L., Santos Hermoso, J., Camacho-Collados, M.: "Policía predictiva", cit., p. 33.

43 Éticas, *Auditoría Externa,* cit., p. 7.

44 Sobre este tema he escrito previamente. Puede leerse: Borges Blázquez, R.: "La inteligencia artificial en el proceso penal y el ¿regreso? de Lombroso", en AA. VV.: *Justicia algorítimica y neuroderecho. Una mirada multidisciplinar,* (coord. por S. Barona Vilar), Tirant lo Blanch, Valencia, 2021, pp. 157-182.

instrumento empleado por el juzgador, coincido con NEIRA PENA en que el principio de legalidad exigiría de una previsión normativa donde la ley especificase para qué tipo de riesgos emplearíamos el sistema, con qué límites y qué garantías de transparencia y contradicción le exigimos.[45]

1. La estandarización de las preguntas a las víctimas: fortaleza y debilidad.

El sistema VIOGEN ha estandarizado una serie de preguntas que se haría a las víctimas por medio de una evaluación clínica no estructurada. Por un lado, tiene la ventaja de incluir preguntas que, tal vez, el agente que toma los datos de la denuncia, obvia por falta de formación en género o por no considerarlas importantes. Pero por otra parte, esta virtud puede convertirse en defecto si la estandarización nos impide fijarnos en el caso concreto. Conscientes de lo abiertas que pueden resultar las preguntas, el propio ministerio del interior desarrolla una guía de procedimiento sobre el Protocolo de Valoración Policial del Riesgo y Gestión de la Seguridad de las víctimas de Violencia de Género donde da indicaciones sobre qué debe tenerse en cuenta respecto de cada indicador así como qué debe hacer el agente en caso de duda.[46] Una buena intervención previa es clave para que la mujer proporcione al agente "información útil y de forma espontánea" y si tras el discurso de la víctima el agente necesitase aclarar algún extremo podría preguntar a la víctima cuando lo considere conveniente y de forma flexible.[47]

Pero VIOGEN no solo estandariza las preguntas, también trata de objetivar el riesgo puesto que las víctimas no siempre son capaces de valorar objetivamente su riesgo. En este sentido, la AP de Madrid: "la orden de protección "está ideada para proteger cuando existe una situación de riesgo objetivo, que lógicamente no puede residenciarse únicamente en la manifestación de temor de la denunciante, ni en la posibilidad meramente teórica de que sufra una agresión o amenaza, sino que debe poder efectuarse un juicio de prognosis positivo de probable reiteración delictiva" y en el caso de autos, con los datos obrantes en la causa, se carece de indicios suficientes para ello (AAP Madrid, Sección 26, núm. 782/2017, de 21/06, y Sección 27, núm. 1349/2012, de 18/10, núm. 1264/2012, de 1/10, núm. 1963/2004, de 2/07, núm. 1135/2012, de 1/08, y núm. 244/2012, de 27/02)".[48] Reflexiona así la Audiencia respecto de la percepción de peligro de la víctima, subjetiva, y el riesgo objetivo merecedor de medidas de protección.

Así, que el juzgador disponga de un cuestionario de cribado rápido de responder (actualmente son menos de 40 preguntas) donde se enmarcan los

45 Neira Pena, A. M.: "Inteligencia Artificial", cit., p. 1920.

46 Por ejemplo, en caso de duda entre dos niveles recomienda aplicar el nivel más alto y si el agente no está conforme con la valoración puede modificarla subiendo el riesgo, pero nunca bajándolo.

47 Guía de Procedimiento 2020 VIOGEN, p. 13.

48 AAP M 8 marzo 2023 (ECLI:ES:APM:2023:689A), pp. 4-5.

principales riesgos a los que se enfrenta una mujer víctima de violencia de género en el ámbito de la pareja se convierte, por un lado, en fortaleza por facilitar la objetivación del riesgo. No obstante, si no se realiza una posterior valoración junto con otros elementos concurrentes y motivación judicial podría convertirse en debilidad al correr el riesgo de obviar u olvidar elementos del riesgo específicos de una víctima en concreto.

2. La falta de transparencia.

La forma de argumentar con y contra la predicción de un algoritmo es cuestionar la exactitud de los datos de entrada. La forma en que los algoritmos calculan los datos necesita del mismo escrutinio que la calidad de los datos en sí mismos.[49] A este respecto, las auditorías de datos[50] por agencias de protección de datos en manos del sector público y realizadas por trabajadores formados en la materia pueden servir para reducir sesgos. Como afirma Cotino Hueso, "hay que apostar por herramientas de IA para controlar a la propia IA. (..) La cuestión última es la de cómo controlar al controlador. Habrá que aplicar los principios éticos y la normativa y poder monitorear a las propias tecnologías de control."[51] Como se ha adelantado previamente, VIOGEN no es transparente. Refiere la auditoría externa de ética que "ni los auditores externos ni los grupos de mujeres tienen ningún tipo de acceso a los datos de VIOGEN. Para un sistema financiado con fondos públicos y de gran impacto (…) es inaceptable."[52] Esta falta de transparencia, como indicaré en conclusiones, hace, a mi juicio, que el sistema, hoy en día, no debiera utilizarse como la posible pericial que propongo a lo largo del trabajo. Salvando las distancias, la reflexión sería similar a la que se ha realizado en diversos estudios respecto del sistema COMPAS.[53] El problema principal del algoritmo COMPAS es su falta de transparencia que imposibilita el derecho de defensa al no poder argumentar contra la máquina a qué se debe el riesgo de reincidencia.

3. La atribución de responsabilidad.

Aunque se supone que los agentes de policía deben validar o modificar la puntuación de VIOGEN, la realidad práctica nos muestra que el 95% de éstos

49 Washington, A. L.: "How to argue with an algorithm: lessons from the Compas-Propublica debate", *Colo. Tech. L.J.,* 2019, vol. 17, núm. 1, p. 134.

50 Excede del objeto de este trabajo, pero de imprescindible lectura: Mcgregor, L., Murray D., NG, V., "International Human Rights Law as a Framework for Algorithmic Accountability", *ICLQ,* 2019, vol. 68, pp. 309-343.

51 Cotino Hueso, L.: "Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales", *DILEMATA*, 2017, núm. 24, pp. 42-43.

52 Éticas, *Auditoría Externa,* cit., p..34.

53 Excede del objeto del trabajo, puede leerse: Martínez Garay, L.: "Peligrosidad, Algoritmos y Due Process: el Caso State v Loomis", *Revista de Derecho Penal Y Criminología*, 2018, núm. 20, pp. 485-502. Martínez Garay, L., Montes Suay, F.: "El uso de valoraciones del riesgo de violencia en Derecho Penal: algunas cautelas necesarias", *InDret*, 2018, núm. 2.

acepta la puntuación.[54] Actuando así el sistema pasa de recomendar a, de facto, ser el decisor de las medidas de protección. Esta cuestión pudo haberla resuelto la AN a propósito de su sentencia de 30 de septiembre de 2020 indicando quién debe responder por un fallo en la valoración del riesgo, pero, como pasaremos a explicar, no entró a fijar las responsabilidades exactas de cada uno de los agentes implicados.

Con fecha 30 de septiembre la Sala de lo Contencioso-administrativo de la Audiencia Nacional ha condenado al Ministerio del Interior por la deficiente protección que la Guardia Civil otorgó a una mujer que solicitó una orden de protección. Un cuestionario de cribado le otorgó "riesgo bajo". Sin realizar más averiguaciones los agentes calificaron el riesgo como "no apreciado". Y esta misma valoración fue determinante para que también el juzgado denegase la medida de protección a la fallecida. Considera la sala que "la actuación de los agentes ante situaciones de violencia de género no debería quedar limitada a aspectos formales de atención a la denunciante, asistencia, información de derechos y citación a juicio, sino que su actuación exige una atención preferente de asistencia y protección de las mujeres que han sido objeto de comportamientos violentos en el ámbito familiar, a los efectos de prevenir y evitar, en la medida de lo posible, las consecuencias del maltrato".

El problema que surge respecto de la responsabilidad por el hecho es el siguiente: el cuestionario de cribado no apreció un riesgo que, por otra parte, el agente tampoco modificó. El automatismo en el ya indicado 95% de los casos nos muestra la relevancia práctica que tiene un sistema que, en un principio, debería servir de auxilio pero nunca sustituir la valoración personal. La sentencia aprecia un funcionamiento erróneo tanto en el servicio de la Guardia Civil como de la Policía Judicial. La respuesta se limitó a la recogida de datos automatizados, pero no previno la violencia ni reevaluó el riesgo por medio de agentes especializados en su tratamiento y sensibilizados con la lacra de la violencia de género. La sala reconoce el quebrantamiento de la obligación estatal positiva de proteger. Una víctima pidió ayuda y un sistema ajeno al género se la denegó. Existían indicios: su marido tenía antecedentes por maltrato en el país de origen, pero no se comprobaron; la violencia se ejercía delante de los menores e incluso delante de la madre del agresor, pero no se les tomó declaración. Además, las trabajadoras sociales describieron una víctima totalmente sometida, con pánico a su agresor.

La sentencia perdió una ocasión de oro para pronunciarse respecto del sistema de atribución de responsabilidades en el caso concreto, pues pese a reconocer que el sistema ha fallado no establece en qué medida son responsables cada una de las partes implicadas. En el caso de que el sistema VIOGEN pasase a integrar

54 Éticas, *Auditoría Externa,* cit., p. 9.

las medidas cautelares, considero que debería quedar legalmente indicado que es una herramienta de mero auxilio y que, además, por aplicación directa del 117 CE, el juzgador debería estar obligado a motivar por qué acepta la valoración de riesgo ofrecida por el algoritmo o, en cambio, por qué se aleja de ésta. Cualquier otra cuestión se alejaría de la jurisdiccionalidad que trae consigo la decisión sobre la imposición de una medida cautelar penal. En este sentido, "existe una íntima relación entre la motivación judicial entendida en el doble sentido de explicitación del fundamento de Derecho en el que se basa la decisión y, sobre todo, del razonamiento seguido por el órgano judicial para llegar a esa conclusión-, y las circunstancias fácticas que legitiman la adopción de la medida en cuestión".[55]

IV. BREVE REFLEXIÓN: ¿CUÁNTO PUEDE LA MÁQUINA AYUDAR AL JUEZ EN LA TOMA DE DECISIONES PARA LA CONCESIÓN DE MEDIDAS CAUTELARES A LAS VÍCTIMAS DE VIOLENCIA DE GÉNERO?

Hoy por hoy no es posible en España el uso de una IA que suplante la decisión del juez. Esto iría en contra de la función jurisdiccional tal y como se encuentra regulada en el artículo 117.3 CE: "El ejercicio de la potestad jurisdiccional de todo tipo de procesos, juzgando y haciendo ejecutar lo juzgado, corresponde exclusivamente a los Juzgados y Tribunales determinados por las leyes, según las normas de competencia y procedimiento que las mismas establezcan". De este artículo podemos extraer dos conclusiones: la primera, nuestra constitución excluye a otros sujetos o sistemas de la capacidad de juzgar. La segunda, el artículo dice quién debe ejercer la función: jueces y tribunales. Pero no específica ni cómo ni mediante qué herramientas. Por tanto, el uso de sistemas de IA de manera complementaria actuando como apoyo a la decisión que debe tomar el juzgador y nunca sustituyendo su razonamiento tendrían encaje en nuestro sistema. Comparto con Bueno De Mata en que el uso de estos sistemas no va dirigido a sustituir al juez, sino en brindarle ayuda a éste, igual que a los abogados y a los demás operadores jurídicos para así avanzar de manera más ágil en la solución del conflicto. Como refiere el autor, aplicar a través de un mapeo de datos y una comparación de casos similares en diferentes bases una tecnología que nos suministre una propuesta de decisión tras una comparación con diferentes indicadores y estadísticas.[56]

De entre todas las IAs la única que, considero, podría emplearse en el proceso penal es la "Soft" IA[57] con un circuito cerrado. Las redes neuronales no solo

55 AJPII 20 mayo 2022 (ECLI:ES:JPII:2022:187), p. 2.

56 Bueno De Mata, F.: "Macrodatos, Inteligencia Artificial y Proceso: Luces y Sombras", *Revista General de Derecho Procesal,* 2020, núm. 51, pp. 16-17.

57 Explica Barona Vilar que La IA débil se programa para una tarea concreta y no es capaz de ir más allá de aquello para lo que originalmente fue programada. En cambio, la IA fuerte es multifuncional y es la que es capaz de sustituir al ser humano ya que responde y actúa como un humano. Barona Vilar, S.:

son peligrosas si perdiésemos el control sobre ellas, también por el hecho de que la medida cautelar siempre modificará la respuesta. Si utilizásemos una IA de redes neuronales para minimizar el riesgo, dado que siempre vamos a actuar en el proceso penal, podría llegar a aprender que la concesión de medidas minimiza el riesgo sin tener en cuenta el verdadero "periculum in mora". Siendo así, el algoritmo sería cada vez más y más estricto, pudiendo llegar a considerar que la mejor opción es la prisión provisional porque solo así convierte el riesgo de la víctima en cero. Esto atentaría contra pilares básicos del proceso penal de la responsabilidad por el hecho, la presunción de inocencia, el "in dubio pro reo" y la ponderación de la medida. Considero que la IA en circuito cerrado puede servir para objetivar riesgos y como herramienta de apoyo al juzgador en la toma de decisiones, pero nunca como sustitutivo en sus decisiones. VIOGEN recoge una serie de preguntas que, en cierto modo, objetivan el "periculum in mora". Estas preguntas surgen de años de experiencia de trabajo con víctimas. Pero la herramienta no es infalible, de hecho, ha tenido diversas correcciones a lo largo de los años donde se han ido actualizando las preguntas.

Respecto de la pregunta inicial sobre si VIOGEN es capaz de valorar el "periculum in mora", considero que su sistema de evaluación actuarial puede aportar mucho a la decisión respecto de una medida cautelar, pero nunca puede sustituir el juicio profesional del juzgador que es quien, en mi opinión, debería tener la responsabilidad respecto de la decisión. La estandarización de preguntas puede servir como un elemento a tener en cuenta pero, además, el juzgador debería motivar la decisión respecto de la adopción de la medida cautelar. Aunque esta motivación se base en los resultados del sistema VIOGEN, la decisión no puede basarse en la automaticidad actual donde en el 95% de los casos los agentes de policía aceptan la valoración del sistema. El juzgador debería incluir una motivación que no bastaría con la simple remisión al algoritmo, convirtiéndolo en el último responsable respecto de la decisión tomada. Además, esta cuestión debería regularse y reglamentarse para, como indica NEIRA PENA, no afectar al principio de legalidad penal.[58]

Continuando con la necesidad de motivación, observamos como se pronuncia en el mismo sentido la Audiencia Provincial de Bilbao respecto de la prisión provisional: "Con esos condicionantes,[59] se añade, en tercer lugar, un requisito que atañe a la actividad judicial. La prisión provisional ha de acordarse por medio de un auto motivado. La suficiencia y razonabilidad de la motivación serán el resultado de la ponderación de los intereses en juego (la libertad de una persona

Algoritmización del Derecho y de la Justicia. De la Inteligencia Artificial a la Smart Justice, Tirant lo Blanch, Valencia, 2021, pp. 106-107.

58 Neira Pena, A. M.: "Inteligencia Artificial", cit., p. 1920.

59 Se refiere a la necesidad de "fumus boni iuris" y "periculum in mora".

cuya inocencia se presume, por un lado, la realización de la administración de la justicia penal y la evitación de hechos delictivos, por otro) a partir de toda la información disponible en el momento en que ha de adoptarse la decisión, de las reglas del razonamiento lógico y del entendimiento de la prisión como una medida de aplicación excepcional. La motivación, en definitiva, exige la expresión del fin constitucionalmente legítimo perseguido con la prisión provisional y el juicio de ponderación con el derecho a la libertad personal. Así lo indica ahora el artículo 506.1 LECrim., al señalar que las resoluciones que se dicten sobre la situación personal del imputado adoptarán la forma de auto y el que acuerde la prisión provisional o disponga su prolongación "expresará los motivos por los que la medida se considera necesaria y proporcionada respecto de los fines que justifican su adopción".[60] La jurisdiccionalidad de las medidas cautelares trae consigo, por tanto, la necesidad de motivar tras un juicio de ponderación entre libertad y seguridad. Este juicio debe ser realizado por el juzgador tras recibir el resultado del algoritmo pues éste solamente hace una valoración del riesgo de reincidencia pero no incluye las variables de la presunción de inocencia y el "in dubio pro reo". Son estas variables las que deberá incluir el juez en su argumentación motivada para, valorando conjuntamente el resultado del algoritmo junto con el resto de diligencias practicadas, motivar qué medida cautelar adoptar.

Además, los algoritmos pueden ayudarnos, por un lado a sistematizar e interpretar contextualmente toda la información relevante para el caso[61] y, precisamente respecto de la variabilidad de las decisiones cautelares, "los sistemas de IA, como colectores de datos pueden servir para mantener actualizado el nivel de riesgo, o incluso como sistema de alerta ante cambios en las circunstancias iniciales que motivaron la decisión cautelar, siempre que los datos de que se nutren se mantengan actualizados y el algoritmo sea utilizado con esta funcionalidad con los órganos jurisdiccionales"[62] tras su oportuna motivación del cambio de circunstancias.[63] A este respecto, para que el algoritmo funcionase correctamente, el juzgador debería tener acceso al sistema de volcado de datos para poder ir modificando las respuestas a las preguntas dependiendo de la variabilidad de las circunstancias.

Por último, disponemos de las preguntas que se hacen a VIOGEN, pero no del valor que se otorga a cada una. Si transformamos el sistema de ser un protocolo para la seguridad de las víctimas para convertirse en un integrante directo del

60 AAP BI 26 Junio 2021 (ECLI:ES:APBI:2021:1172A), p. 3

61 Neira Pena, A. M.: "Inteligencia Artificial", cit., 1913

62 Ibidem, 1918.

63 Para ejemplo un botón, en el propio auto donde la AP de Madrid deniega la concesión de una orden de protección, ésta indica que: "Lo anterior no obsta para que, llegado el caso, y ante nuevos datos, y/o sobrevenidas circunstancias, pudieran ser incluso solicitadas, de conformidad con lo previsto en el art. 544 TER 11 LECRIM, las oportunas medidas de protección.", AAP M 8 marzo 2023 (ECLI:ES:APM:2023:689A) p. 5

"periculum in mora" cautelar penal urge más si cabe la transparencia del algoritmo para poder entender por qué ha tomado la decisión así como poder atacar la decisión si no estamos de acuerdo ya que, en la actualidad, desconocemos el valor ponderado que el sistema otorga a cada una de sus variables y cómo interactúan entre sí.

BIBLIOGRAFÍA

Barona Vilar, S.: "Prisión provisional: 'solo' una medida cautelar (Reflexiones ante la doctrina del TEDH y del TC, en especial de la STC 46/2000, 17 febrero)", *Actualidad Penal,* 2000, núm. 42, pp. 891-911.

Barona Vilar, S.: *Algoritmización del Derecho y de la Justicia. De la Inteligencia Artificial a la Smart Justice*, Tirant lo Blanch, Valencia, 2021.

Barona Vilar, S.: *Medidas cautelares en el proceso penal,* Prontuario de Derecho Procesal 3, Honduras, 2015.

Barona Vilar, S.: "¿Una nueva concepción expansiva de las medidas cautelares en el proceso penal?", *Revista del Poder Judicial,* 2006, núm. especial 19, pp. 237-264.

Borges Blázquez, R.: "Obligaciones estatales positivas de prevención y medidas de protección civiles para víctimas de violencia doméstica y de género. Una apuesta a favor de su regulación", *Actualidad Jurídica Iberoamericana,* 2020, núm. 13, pp. 898-929.

Borges Blázquez, R.: "La inteligencia artificial en el proceso penal y el ¿regreso? de Lombroso", en AA. VV.: *Justicia algorítimica y neuroderecho. Una mirada multidisciplinar,* (coord. por S. Barona Vilar), Tirant lo Blanch, Valencia, 2021, pp. 157-182.

Borges Blázquez, R.: "Inteligencia artificial y perspectiva de género: programar, investigar y juzgar con filtro morado", *Revista General de Derecho Procesal,* 2021, núm. 55, pp. 1-41.

Bueno De Mata, F.: "Macrodatos, Inteligencia Artificial y Proceso: Luces y Sombras", *Revista General de Derecho Procesal,* 2020, núm. 51, pp. 1-31.

Cotino Hueso, L.: "Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales", *DILEMATA*, 2017, núm. 24, pp. 131-150.

De Urbano Castillo, E.: "El alejamiento del agresor, en los casos de violencia familiar", *La Ley,* 2001, núm. 5248.

Éticas, *Auditoría Externa del Sistema VioGén,* Fundación Ana Bella, 2022.

González Álvarez, J. L.: "Sistema de seguimiento integral en los casos de violencia de género (sistema viogén)", *Cuadernos de la Guardia Civil,* 2018, núm. 56, pp.83-102.

González Álvarez, J. L., López-Ossorio, J. J., Urruela, C., Rodríguez-Díaz, M.:"Integral Monitoring System in Cases of Gender Violence VioGén System", *Behavior & Law Journal*, 2018, num. 4(1), pp. 29-40.

González Álvarez, J. L., López-Ossorio, J. J., Muñoz Rivas, M.: "La valoración policial del riesgo de violencia contra la mujer pareja en España- Sistema Viogén", 2018.

González Álvarez, J. L., Santos Hermoso, J., Camacho-Collados, M.: "Policía predictiva en España. Aplicación y retos futuros", *Behavior & Law Journal,* vol. 6, núm. 1, 2020, pp. 26-41.

López-Ossorio, J. J., Lonaiz, I., González Álvarez, J. L.: "Protocol for the police gender violence risk assessment (VPR4.0): Review of its performance", *Rev Esp Med Legal*, 2019, núm. 45(2), pp. 52-58.

López-Ossorio, J. J., González Álvarez, J. L.; Andrés Pueyo, A.: "Eficacia predictiva de la valoración policial del riesgo de la violencia de género", *Psychosocial Intervention,* 2016, núm. 25, pp. 1-7.

Martínez Garay, L.: "Peligrosidad, Algoritmos y Due Process: el Caso State v Loomis", *Revista de Derecho Penal Y Criminología*, 2018, núm. 20, pp. 485-502.

Martínez Garay, L., Montes Suay, F.: "El uso de valoraciones del riesgo de violencia en Derecho Penal: algunas cautelas necesarias", *InDret*, 2018, núm. 2.

Mcgregor, L., Murray D., NG, V., "International Human Rights Law as a Framework for Algorithmic Accountability", *ICLQ*, 2019, vol. 68, pp. 309-343.

Neira Pena, A. M.: "Inteligencia Artificial y tutela cautelar. Especial referencia a la prisión provisional", *Rev. Bras. de Direito Processual Penal,* Porto Alegre, 2021, vol. 7, num. 3, pp. 1897-1933.

Planchadell Gargallo, A.: "Inteligencia Artificial y medidas cautelares", en AA. VV.: *Justicia algorítimica y neuroderecho. Una mirada multidisciplinar,* (coord. por S. Barona Vilar), Tirant lo Blanch, Valencia, 2021, pp. 389-419.

Serrano Hoyo, G.: "Algunas cuestiones procesales que plantea la Orden de Protección de las víctimas de la violencia doméstica", *Anuario de la Facultad de Derecho*, 2004, pp. 69-104.

Van Der Aa, S., Niemi, Johanna; S., Lorena; Ferreira, A., Baldry, A., "Mapping the legislation and assessing the impact of Protection Orders in the European member states", *Daphne,* 2015.

WASHINGTON, A. L.: "How to argue with an algorithm: lessons from the Compas-Propublica debate", *Colo. Tech. L.J.,* 2019, vol. 17, núm. 1, pp. 131-160.

EL CASO DE LA NEGOCIACIÓN ASISTIDA EN EL ÁMBITO DEL DERECHO DE CONSUMO PARA UN MEJOR ACCESO A LA JUSTICIA EN CHILE: LECCIONES APRENDIDAS EN EL DESARROLLO DE SOFTWARE CON TECNOLOGÍAS DE INTELIGENCIA ARTIFICIAL*

THE CASE OF ASSISTED NEGOTIATION IN THE FIELD OF CONSUMER LAW FOR BETTER ACCESS TO JUSTICE IN CHILE: LESSONS LEARNED IN THE DEVELOPMENT OF SOFTWARE WITH ARTIFICIAL INTELLIGENCE TECHNOLOGIES

Actualidad Jurídica Iberoamericana Nº 21, agosto 2024, ISSN: 2386-4567, pp. 408-433

* Este trabajo forma parte del proyecto de investigación Fondecyt Regular Nº 1220735 titulado "Digitalización y algoritmos en la solución de conflictos en materia de Consumo en Chile. Propuesta de mejora del acceso a la justicia del consumidor individual a la luz de los sistemas comparados", financiado por la Agencia Nacional de Investigación y Desarrollo de Chile (ANID). Además, forma parte del Módulo Jean Monnet IA y Derecho Privado Europeo de la Universidad Autónoma de Chile, financiado por el Programa Erasmus plus perteneciente a la Unión Europea.

Sebastián
BOZZO HAURI
y Juan Carlos
VIDAL ROJAS

ARTÍCULO RECIBIDO: 29 de mayo de 2023
ARTÍCULO APROBADO: 1 de julio de 2024

RESUMEN: Las nuevas tecnologías de negociación asistida y resolución de conflictos en el derecho tienen relación con el uso de plataformas digitales y herramientas en línea para facilitar y mejorar la comunicación y la colaboración entre las partes de un conflicto. Estas tecnologías incluyen —entre otras— la mediación en línea, las salas virtuales de negociación, el intercambio de información y documentos a través de plataformas seguras, y el uso de Inteligencia Artificial para analizar datos y generar opciones de solución. Es importante destacar que si bien estas tecnologías pueden ofrecer beneficios significativos, también plantean desafíos importantes. La privacidad y la seguridad de los datos, la imparcialidad de los algoritmos y la posible falta de acceso a estas tecnologías por parte de ciertos grupos de la población son aspectos críticos que deben abordarse de manera cuidadosa y reflexiva. El objetivo de este trabajo es proporcionar una visión clara y equilibrada de las oportunidades y desafíos asociados con las nuevas tecnologías en la resolución de conflictos legales. Con esto, se espera contribuir al desarrollo de estrategias efectivas y éticas para su implementación en el ámbito del derecho, fomentando así una justicia más accesible. De esta forma el trabajo se divide en dos partes, en la primera, se revisa el marco teórico de la negociación y resolución de disputas en línea (ODR), y en una segunda parte, a través del desarrollo de tres prototipos se intentará demostrar una solución práctica, donde utilizaremos tecnología al servicio de las personas y sus consultas judiciales.

PALABRAS CLAVE: Inteligencia Artificial, ODR, consumidor, prototipo.

ABSTRACT: *New technologies for assisted negotiation and conflict resolution in law refer to the use of digital platforms and online tools to facilitate and improve communication and collaboration between parties in conflict. These technologies include, among others, online mediation, virtual negotiation rooms, the exchange of information and documents through secure platforms, and the use of Artificial Intelligence to analyze data and generate settlement options. It is important to note that while these technologies can offer significant benefits, they also pose significant challenges. Data privacy and security, the fairness of algorithms, and the potential lack of access to these technologies by certain population groups are critical issues that need to be carefully and thoughtfully addressed. The objective of this paper is to provide a clear and balanced view of the opportunities and challenges associated with new technologies in legal dispute resolution. With this, it is hoped to contribute to the development of effective and ethical strategies for their implementation in the field of law, thus promoting a more accessible justice. In this way, the work is divided into two parts: in the first part, the theoretical framework of online negotiation and dispute resolution (ODR) is reviewed, and in the second part, through the development of three prototypes, we will try to demonstrate a practical solution where we will use technology to serve people and their judicial consultations.*

KEY WORDS: *Artificial Intelligence, ODR, consumer, prototype.*

SUMARIO.- I. INTRODUCCIÓN. II. RESOLUCIÓN DE CONFLICTOS: DESDE LO ANÁLOGO A LO DIGITAL. 1. Origen y desarrollo de la negociación como método de resolución de conflictos. 2. Resolución de disputas online (ODR). *A) Experiencia pública de ODR: plataforma europea online de justicia. B) Experiencia privada de ODR: el caso Kleros. C) Experiencias chilenas de MASC.* III. EXPERIENCIA EN EL DESARROLLO DE PROTOTIPOS DE SOFTWARE CON TECNOLOGÍA DE IA. 1. Cuestiones previas. 2. Desarrollo de prototipos. *A) Prototipo N°1. B) Prototipo N°2. C) Prototipo N°3. D) Resultados.* IV. CONCLUSIONES.

I. INTRODUCCIÓN.

Las exigencias del siglo XXI, en un mundo cada día más acelerado y conectado, obligan a incorporar la tecnología en todos los ámbitos, aún más en un área tan relevante como lo es el derecho. Facilitar el acceso a la justicia es una exigencia para todos los Estados, los cuales deben entregar y asegurar —de manera eficiente y hábil— justicia para todos. Por esto, es básico que se lleven a cabo procesos claros, sencillos y al alcance de todos los ciudadanos, con rapidez y seguridad, permitiendo el ingreso a mediaciones y asesorías antes de llegar al tribunal de justicia. En este sentido, el impulso de la transformación digital en materia de justicia ha obligado a proponer iniciativas tecnológicas que tengan como objetivo principal aprovechar el potencial de innovación que ofrece la tecnología para poner al servicio de la ciudadanía del siglo XXI —cada vez más exigente y conectada— la justicia[1].

Así, la incorporación de la Inteligencia Artificial (en adelante, IA) a las negociaciones asistidas en el contexto del derecho resulta indispensable en la búsqueda de alternativas de resolución de conflictos[2], pues a partir de ella es posible entregar herramientas al alcance de todos, desarrollar tecnologías que contribuyan a mejorar la atención, acortar los tiempos de espera en la atención y lograr negociaciones asistidas exitosas; todo ello puede mejorar el acceso a la justicia de las personas y en especial para los consumidores, dado que disminuye el coste de administración y —por ende— bajan las barreras de acceso por el menor precio que significaba iniciar una disputa[3]. Así, la tecnología en el ámbito del derecho es una realidad que puede significar un avance importante en democratizar el acceso a la justicia de las personas.

1 Boucier, D.: *Inteligencia Artificial y Derecho*, Editorial UOC, Pompeu, 2003.

2 Martín Diz, F.: "Modelos de aplicación de Inteligencia Artificial en justicia asistencial o predictiva versus decisoria", en AA.VV.: *Justicia algorítmica y neuroderecho* (edit. por S. Barona Vilar), Tirant lo Blanch, Valencia, 2021, p. 66.

3 Bozzo Hauri, S.: "El uso de las nuevas tecnologías como forma de disminuir las barreras de acceso a la justicia del consumidor en Chile", *Vniversitas Jurídica*, 2023, vol. 72, p. 1.

• Sebastián Bozzo Hauri
Profesor titular del Módulo Jean Monnet IA y Derecho Privado Europeo e integrante del grupo de investigación IA y Derecho de la Universidad Autónoma de Chile: sebastian.bozzo@uautonoma.cl

• Juan Carlos Vidal Rojas
Profesor y miembro del grupo de investigación ingeniería informática y computación de Universidad Autónoma de Chile: juan.vidal@uautonoma.cl

Por ello, la intención medular es dar atención rápida y de calidad a los ciudadanos[4], siendo necesario destacar la importancia de las tecnologías de IA integradas en el proceso de desarrollo de software, las que en un principio han sido de forma experimental pero cada día son más habituales.

La tecnología es una aliada al momento de innovar para contribuir en mediaciones, negociaciones, arbitrajes y resoluciones judiciales, el alcance en información y la prontitud en las soluciones a los conflictos. Ello, pues estamos viviendo un crecimiento exponencial y vertiginoso de herramientas de internet, digitales, virtuales, sincrónicas, asincrónicas, IA, aplicaciones, algoritmos, 4G, 5G, wifi, Wireless, nube, etc. Por lo tanto, de una u otra manera, no hay forma de vivir en la sociedad actual sin estar conectado de algún modo[5].

Así las cosas, resulta imprescindible mejorar el tiempo de respuesta y dar soluciones a las consultas realizadas por los consumidores, ya sea en mediaciones o en negociaciones asistidas en los diferentes ámbitos del derecho. Por tanto, es relevante indagar e interiorizar sobre la importancia de los avances tecnológicos y comunicacionales a la hora de resolver conflictos, con el fin de simplificar procesos y mejorar la calidad de vida[6].

En consecuencia, el alcance de las nuevas tecnologías se torna crucial para dar una mejor cobertura de atención, toda vez que se necesita mayor interoperabilidad entre los servicios públicos y privados, motivación por el cambio y una reducción de la burocracia para alcanzar mejores estándares de sistemas de respuestas y resolución de conflictos[7]. Por lo mismo es que —desde la mirada más propiamente administrativa— los mecanismos de negociación asistida se conciben de manera más clara como alternativas al proceso legal, en el sentido de constituirse simplemente como formas de descongestionar el sistema y así dejar las causas más relevantes para el sistema judicial[8].

En este trabajo aportamos conocimiento para evidenciar la evolución de nuevas prácticas tecnológicas basadas en la IA que han permitido al derecho disponer de herramientas para mejorar la calidad de servicio de los tribunales, ayudando así no solo a las personas que necesitan de este sino también a jueces, abogados y todos los entes involucrados. Asimismo, analizamos el impacto y las implicaciones

4 "En la resolución y administración de controversias cada vez más desarrolladas para responder al crecimiento de la conflictividad en las sociedades contemporáneas interconectadas, a la congestión judicial y al surgimiento de nuevas controversias en el ámbito privado y público en la era digital". Centro de Estudios de Justicia de las Américas, C.: *Resolución de Conflictos en línea*, Equipo Editorial y Gráfico CEJA, Santiago, 2022, p. 10.

5 Elisavetsky, A.: *La mediación a la luz de las nuevas tecnologías,* Errelus, Buenos Aires, 2019, p. 74

6 Elisavetsky, A.: "La mediación"*,* cit., p. 75

7 Contini, F. y Velicogna, M.: "Del acceso a la información al acceso a la justicia: diez años de e-justice en Europa", *El rol de las Nuevas Tecnologías en el Sistema de Justicia,* 2021, núm. 16, p. 44.

8 Díaz, A.: *Mecanismos Alternativos de Solución de Conflictos*, Academia Judicial, Santiago, 2019, pp. 61-63.

de las nuevas tecnologías de negociación asistida y sistemas de ODR. Por último, demostramos a través de tres prototipos desarrollados que es posible entregar soluciones factibles con la ayuda de la tecnología de IA disponible actualmente.

II. RESOLUCIÓN DE CONFLICTOS: DESDE LO ANÁLOGO A LO DIGITAL.

1. Origen y desarrollo de la negociación como método de resolución de conflictos.

Para determinar el origen de la negociación de conflictos, debemos considerar no solo un punto de partida histórico específico sino la naturaleza misma de las interacciones humanas a lo largo del tiempo. Aunque la antigua Grecia se destaca por sus aportes en muchos campos, incluida la retórica y el arte de la persuasión, la práctica de negociar conflictos es probablemente tan antigua como la existencia de las relaciones entre grupos humanos. Ya en el siglo VI a.C., los oradores elocuentes en comunidades de diversas culturas asumían roles similares a los de negociadores, defendiendo causas y fomentando la cooperación entre los pueblos. Así, el emperador Constantino —quien fomentó el desarrollo de métodos de negociación— se preocupó de que sus enviados adquirieran capacidad negociadora para asegurarse la posición en el imperio.

Con posterioridad, al inicio de la Edad Media, los negociadores eran los enviados de la Iglesia Católica; y —mucho después—, en el siglo XX, a partir de la Primera Guerra Mundial, las negociaciones dejaron de depender de las relaciones familiares entre monarcas, de modo que aparecieron las negociaciones públicas conducidas por funcionarios especializados, quienes eran mandatados por sus respectivos gobiernos para lograr acuerdos[9].

Según el autor del libro "El Arte de Negociar", esta práctica consiste en establecer acuerdos, constituyendo un quehacer ineludible capaz de implicar a todos y cada uno de los seres humanos, y la importancia de los intereses en juego es prácticamente inconmensurable si se tiene en cuenta que afecta a casi todas nuestras actividades[10]. De esta manera, la negociación asistida se podría conceptualizar como el proceso mediante el cual dos o más partes, con intereses comunes y opuestos, confrontan sus intereses, a través de una comunicación dinámica, donde intercambian bienes y servicios, tratando de resolver sus diferencias en forma directa, para lograr una solución que genere mutua satisfacción de las partes[11]; se trata de un proceso estructurado que se destina a la identificación

9 Gonzalbo Aizpuru, P.; Mayer Celis, L.: *Conflicto, resistencia y negociación en la historia*, Colegio de México, México, 2016, p. 102.

10 De las Alas Pumariño, E.: *El Arte de Negociar*, AIIM, Madrid, 2014, p. 13.

11 Vargas Correa, A.: *Creación de Valor en Procesos de Negociación Asistida*, Editorial Académica Española, España, 2018, p. 73

y el análisis de las tendencias de los conflictos con la finalidad de determinar la respuesta más adecuada[12].

Parte importante del desarrollo de estos sistemas se debe al trabajo de las plataformas digitales en la intermediación y arbitraje entre vendedores y consumidores dentro de los "Marketplaces". Así, empresas del ámbito privado como Amazon, eBay y Mercado Libre lideran la integración de algoritmos para la resolución de disputas en línea. Estas plataformas utilizan la IA como un instrumento crucial para dirimir controversias, constituyendo este enfoque una parte integral de su estructura de negocio. Ofrecen a los consumidores un entorno seguro, donde tienen la garantía de que una entidad imparcial intervendrá para resolver los problemas, buscando soluciones legítimas y justas[13].

En términos generales, la negociación electrónica se fundamenta en el soporte de las tecnologías de la información y las comunicaciones (en adelante, TICs), lo que posibilita una interacción directa entre los participantes de una disputa, ya sea de manera sincrónica o asincrónica. Dicha negociación electrónica se aplica en variados sectores como el familiar, civil, pero primordialmente en el comercial y de consumo[14].

Los sistemas que automatizan la negociación electrónica se basan en un software estructurado para recabar datos del usuario mediante formularios, los cuales frecuentemente incorporan los principios de la Escuela de Harvard (Intereses, opciones, alternativas, compromisos). Estas tecnologías disminuyen la tendencia natural hacia una conducta competitiva o distributiva de los negociadores, privilegiando en cambio el empleo de la tecnología para un diálogo facilitado entre las partes por medio de un proceso automatizado[15].

De esta forma, a través de un programa informático se ofrece a las partes la posibilidad de coordinar la comunicación, elaborar la agenda, alcanzar soluciones potenciales e incluso la confección de un acuerdo, centrando la controversia mediante formularios prediseñados e inteligentes que varían según la información proporcionada por las partes, marcando el ámbito de acuerdos posibles o reformulando sus intervenciones para que sean más constructivas[16].

12 Vargas Correa, A.: "Creación de Valor", cit., p. 73.

13 Bozzo Hauri, S.: "Plataformas, algoritmos y su rol en la resolución de conflictos en el ámbito de consumo", en AA.VV.: *Justicia Poliédrica en periodo de mudanza* (dir. por S. Barona Vilar), Tirant lo Blanch, Valencia, 2022, p. 314.

14 Arley Orduña, A.: *Resolución electrónica de disputas (ODR): acceso a justicia digital,* Tirant Lo Blanch, Valencia, 2021, p. 96.

15 Arley Orduña, A.: "Resolución electrónica", cit., p. 96.

16 Montesinos García, A.: "Inteligencia Artificial y ODR", en AA.VV.: *Justicia algorítmica y neuroderecho* (edit. por S. Barona Vilar), Tirant lo Blanch, Valencia, 2021, p. 518.

Estos sistemas brindan apoyo desde el comienzo de la mediación o en puntos donde los involucrados no consiguen alcanzar sus metas mediante esfuerzos individuales, intercambio de datos, propuestas y razonamientos, y se enfrentan a la incapacidad de gestionar tareas mutuamente dependientes o alcanzar acuerdos que conduzcan a compromisos sólidos[17]. Por ende, existen dos categorías principales de negociación electrónica: aquellas que automatizan el proceso negociador y aquellas que ofrecen asistencia en la toma de decisiones[18].

La incorporación de la tecnología en negociaciones asistidas y evaluación de conflictos en el ámbito del Derecho tiene como propósito central disponer de la información necesaria para comprender el problema y dar solución apoyándose en el ordenamiento jurídico y en la jurisprudencia[19]. Así, al unirse derecho y tecnología se consigue una comunicación optimizada, mayor accesibilidad a la información y una mejor capacidad de análisis[20].

En el ámbito del consumo, el uso de software para la negociación asistida previa es crucial para promover acuerdos tempranos entre consumidores y proveedores, previniendo la escalada de conflictos. Las plataformas de ODR que se limitan a proporcionar solamente vías de comunicación digital entre las partes subestiman el valor de estas herramientas. Al no aprovechar plenamente la capacidad del software de asistencia en la negociación, se pierde la oportunidad de resolver disputas de manera eficiente desde sus etapas iniciales, evitando complicaciones futuras[21].

En cuanto a la finalidad del uso de nuevas tecnologías de IA en la negociación y evaluación de conflictos al servicio del derecho, podemos encontrar las siguientes: en primer lugar, busca facilitar la accesibilidad a la información jurídica; y, en segundo lugar, pretende simplificar y automatizar todo o parte del proceso de razonamiento jurídico. Actualmente, dicha tecnología está presente en: la mediación en línea; la negociación por videoconferencia y en el uso de la IA en la resolución de disputas. A su vez, la información que las personas habitualmente requieren es: cómo resolver los problemas; cuáles son sus derechos y obligaciones y cómo llevar un caso a un tribunal[22].

17 Arley Orduña, A.: "Resolución electrónica", cit., p. 97.

18 Arley Orduña, A.: "Resolución electrónica", cit., p. 97.

19 En este caso cobra mucha relevancia la implementación de tecnologías de IA en negociación asistida y evaluación de conflictos en el ámbito del Derecho. Díaz, L.: *La Mediación y Negociación para Resolver Conflictos Legales,* 2019, p. 223.

20 Centro de Estudios de Justicia de las Américas, C.: "Resolución de Conflictos", cit., p. 22.

21 Catalán Chamorro, M.: *El acceso a la justicia de consumidores: los nuevos instrumentos del ADR y ODR de Consumo*, Tirant Lo Blanch, Valencia, 2019, p. 337.

22 Reiling, D: "Comprendiendo las tecnologías de la información para la resolución de conflictos", *El rol de las Nuevas Tecnologías en el Sistema de Justicia,* 2021, núm. 16, p. 28.

Existen distintos modos de integrar la tecnología de IA en el ámbito del derecho. En la actualidad se utilizan frecuentemente las siguientes:

Chatbot: Esta tecnología sirve para orientar, derivar y entregar respuestas básicas a los usuarios que desconocen los procedimientos judiciales como un primer acercamiento a la asistencia en torno a dudas legales; proporcionando una herramienta efectiva, rápida y segura para la entrega de información básica e iniciar la búsqueda de asesoría legal necesaria para cada caso y su propia complejidad y desarrollo. En el ámbito de consumo puede ser de gran relevancia, pues gracias a la respuesta que entregue el software "chatbot" se podría orientar al consumidor sobre el porcentaje de posibilidad de obtener o no una solución favorable y, por otra parte, cuál es el medio idóneo para solucionar su conflicto[23].

Sistemas que utilizan IA: Generalmente para el reconocimiento facial, sin embargo, también existen aplicaciones que están siendo utilizadas en el ámbito público como en los tribunales de justicia[24]. La incorporación de tecnología de reconocimiento facial en el proceso judicial puede resultar útil en el tratamiento de los metadatos de las grabaciones y registros audiovisuales judiciales. Nos referimos a la comunicación no verbal que se presenta en los actos judiciales, como la que ocurre en la vista de un juicio oral o en una declaración judicial, y que resulta imposible de verbalizar o transcribir. Esta tecnología de reconocimiento facial puede resultar también de utilidad para proceder a la identificación o acreditación de la identidad de las personas que declaran en el juzgado, siempre que previamente figuren en una base de datos judiciales.

Software de gestión: Se han desarrollado herramientas digitales que logran facilitar el trabajo de los operadores jurídicos, agilizando el mismo, ya sea en el ámbito del ejercicio profesional, tribunales, notarías, registro de propiedades, entre otros.

Antes de existir estas tecnologías, el profesional jurídico tenía que enfrentarse diariamente a procesos poco eficientes y con altos márgenes de error. Por ello, las tecnologías que se han incorporado a las distintas áreas del derecho han impactado de forma positiva a todos los actores de un proceso judicial, desde el abogado, cliente, juez, documentación, audiencias, agendas, almacenamiento de datos, etc.

2. Resolución de disputas online (ODR).

En cuanto a los sistemas ODR, estos se refieren al diseño e implementación de sistemas de resolución de conflictos, dentro y fuera de las cortes y juzgados, que

23 Marcos Francisco, D.: "Sistema arbitral de consumo: algunas propuestas 'inteligentes' de lege ferenda", *InDret*, 2024, núm. 1, p. 120.

24 Pérez Estrada, M. J.: *Fundamentos jurídicos para el uso de la inteligencia artificial en los órganos judiciales*, Tirant Lo Blanch, Valencia, 2022, p. 107.

operan en internet y que usan TICs[25]. Se relacionan con la conferencia en 1976 del profesor de Harvard, Frank Sander[26], quien ofreció un enfoque absolutamente novedoso a fin de reducir la demanda del usuario sobre los tribunales de justicia. Para ello, propuso el "Tribunal Multipuertas", pues consideraba injustificada la resolución de los jueces en temas que podían ser atendidos a través del diagnóstico y la derivación de los casos al método de solución más adecuado[27].

Así, dentro del sistema de administración de justicia, los ODR son un tipo de mecanismo alternativo de solución de conflictos (en adelante, MASC) que —como ya se dijo— se diferencia de este último porque funciona a través de TICs.[28] Por lo general funcionan a través de una plataforma digital que permite a los consumidores avanzar en la resolución de controversias de baja cuantía, desde el inicio de una reclamación o demanda hasta la decisión final, totalmente en línea. Este proceso puede implicar diferentes metodologías, entre ellas la utilización de la información suministrada por "vías guiadas", la licitación a ciegas, la solución híbrida alternativa de controversias (incluida la negociación facilitada y la evaluación neutral temprana, ya sea con aportaciones humanas o con algoritmos de inteligencia artificial), la comunicación digital (como la participación a distancia o por video en audiencias y la mensajería asincrónica) y la carga y respuesta a las pruebas en línea.[29]

Siguiendo el trabajo de la profesora Catalán[30] "es posible entender la negociación online como el método que utiliza múltiples softwares o prácticas, en ocasiones muy diferentes, que ofrecen una salida o una respuesta a un problema concreto a través de una serie de opciones limitadas para ello. En el cual se distinguen dos tipos de negociaciones online por antonomasia: el blind bidding o negociación automática, y la denominada negociación asistida".

El blind bidding es un método de oferta oculta donde cada parte presenta una oferta inicial y un límite mínimo aceptable para un arreglo. Este procedimiento

25 Centro de Estudios de Justicia de las Américas, C.: "Resolución de Conflictos", cit., p. 14.

26 Centro de Estudios de Justicia de las Américas, C.: "Resolución de Conflictos", cit., p. 34.

27 Catalán Chamorro, M.: "El acceso", cit., p. 270.

28 Montesinos García, A.: "Inteligencias Artificial", cit., p., 507. Señala al respecto: "En la década de los noventa asistimos al nacimiento de los denominados mecanismos de resolución de conflictos on line, ODR ('online dispute resolution'), una nueva modalidad de ADR ('alternative dispute resolution'), que estructura y permite resolver las controversias a través de medios electrónicos, si no en todas las fases del procedimiento, si en gran parte del mismo. Se combina así la eficiencia de la resolución alternativa de conflictos con el poder de Internet y las tecnologías de la información y de la comunicación, ofreciendo numerosas ventajas".

29 Bozzo Hauri, S.; Remeseiro Reguero, R.: "Resolución de conflictos en consumo: ¿Una solución a través de la inteligencia artificial?, en AA.VV.: *Justicia algorítmica y neuroderecho* (edit. por S. Barona Vilar), Tirant lo Blanch, Valencia, 2021, p. 614.

30 Catalán Chamorro, M.: "Una plataforma ODR europea ¿Una solución?, en AA.VV.: *Derecho del consumo y protección del consumidor sustentable en la sociedad digital del siglo XXI* (edit. por S. Barona Vilar), Edición Universidad Autónoma de Chile, Santiago, 2023, p. 365.

es útil para resolver reclamaciones monetarias relacionadas con consumo o compensaciones por daños y perjuicios. La parte que reclama especificará una cantidad inicial y un porcentaje o suma menor —que se mantiene confidencial y no se revela a la otra parte— que estaría dispuesta a aceptar en última instancia para resolver la disputa rápidamente. De igual manera, la parte demandada propone una suma inicial que está dispuesta a abonar, junto con un límite mínimo menor. Si el programa identifica un punto de encuentro posible dentro de estos límites, se cerrará el trato por el monto que más se aproxime a las cifras propuestas por ambos. Si no se logra un acuerdo, el programa permite a las partes continuar intentándolo hasta un número preestablecido de veces, generalmente no más de tres[31].

Por otro lado, la negociación asistida se podría conceptualizar como el proceso mediante el cual dos o más partes, con intereses comunes y opuestos, confrontan tales intereses a través de una comunicación dinámica, donde intercambian bienes y servicios, tratando de resolver sus diferencias en forma directa, para lograr una solución que genere mutua satisfacción de las partes. Se trata de un proceso estructurado que se destina a la identificación y el análisis de las tendencias de los conflictos con la finalidad de determinar la respuesta más adecuada[32].

Las plataformas de ODR se posicionaron a partir de la necesidad de entregar una solución —principalmente— al comercio electrónico, bajo la premisa de que los tribunales eran insuficientes, los procesos largos, los costos de justicia y abogados elevados, en contraposición al valor de la disputa que se produce en las relaciones de consumo, que son por lo general de baja cuantía.

Ahora bien, entre las plataformas que usan algoritmos con el objetivo de lograr resoluciones justas y eficientes para dar respuesta a diversos conflictos, podemos mencionar "Smartsettle ONE", el cual permite que —desde un servidor neutral que, en estricto rigor, es un mediador automático—, a través de algoritmos se puedan conseguir que las partes en conflicto logren el mejor acuerdo, sugiriendo variadas propuestas y posibilidades que se ajusten a sus requerimientos[33].

Entre las ventajas de la utilización de IA se puede mencionar que las tecnologías permiten investigar, monitorear, almacenar datos, comprobar, entregar pruebas y respuestas inmediatas, acelerando los procesos judiciales; mientras que, entre las desventajas cabe mencionar la vulnerabilidad de la privacidad y la inseguridad digital, para el ámbito del derecho aspecto imprescindible y la vulnerabilidad de información fundamental para los procesos. Por lo tanto, la seguridad es un tema

31 Catalán Chamorro, M.: "Una plataforma" cit., p. 365.

32 Vargas Correa, A.: "Creación de Valor", cit. p. 74.

33 Dobratinich, A.: "Inteligencia Artificial y Justicia: Aplicabilidad de la tecnología en las decisiones judiciales en Argentina", *Revista Direitos Culturais,* 2022, vol. 17, núm. 42, p. xx.

central, así como lo es el respeto por la privacidad de las personas: cada caso impacta a un ser humano, por lo que reviste de suma importancia el resguardo de los datos, los cuales podrían ser manipulados o mal usados[34].

A) Experiencia pública de ODR: plataforma europea online de justicia.

El 21 de mayo de 2013, el Parlamento Europeo y el Consejo establecieron las bases normativas para la resolución alternativa de litigios en el ámbito del consumo mediante la adopción de la Directiva 2013/11/UE, que se hizo efectiva el 8 de julio del mismo año. Paralelamente, se emitió el Reglamento (UE) Nº524/2013, que rige la resolución de litigios online en materia de consumo y comenzó a aplicarse directamente en los Estados miembros desde el 9 de enero de 2016, sin requerir transposición a la legislación nacional. Este marco legal busca asegurar que los Estados cuenten con entidades adecuadas para la resolución alternativa de disputas de consumo (entidades ADR) conforme a las normas europeas.

La implementación de esta normativa involucra a la Comisión Europea, a los Estados miembros y a los empresarios. La Comisión es responsable de lanzar y gestionar la plataforma online destinada a resolver estos litigios, mientras que los Estados miembros deben asegurar la disponibilidad de entidades ADR certificadas que ofrezcan cobertura amplia para tratar los conflictos surgidos de transacciones comerciales y servicios entre consumidores y empresarios dentro de la UE. Además, se impone a los empresarios la obligación de informar a los consumidores sobre la existencia de este MASC online[35].

La plataforma europea de resolución de conflictos sirve como un medio que proporciona a los consumidores una vía accesible hacia la justicia, ofreciéndoles información vital sobre la solución extrajudicial de disputas, un compendio de entidades de resolución alternativa, guías para presentar quejas, contactos nacionales, y análisis sobre su rendimiento. Su eficacia depende de la capacidad de los Estados miembros para establecer y mantener entidades de resolución alternativa que se alineen con los estándares y procedimientos del derecho europeo, así como de asegurar que los empresarios informen adecuadamente sobre estas opciones a los consumidores[36].

34 Vargas Correa, A.: "Creación de Valor", cit., p. 74.

35 Esteban de la Rosa, F.: "Tecnología de la información y de la comunicación y resolución de litigios: el modelo europeo de promoción del ODR en el ámbito de los litigios de consumo", *Revista iberoamericana de derecho internacional y de la integración,* 2019, núm. 10, p. 90.

36 Como señala Catalán Chamorro, M.: "Una plataforma", cit., p. 358 al indicar: "Sin duda la idea de esta plataforma suponía un antes y un después en la protección del consumidor dentro de la Unión Europea. Hasta ese momento, la Unión Europea había protegido al consumidor de una manera preferente en diversas leyes sustantivas, otorgándole así derechos sobre diversas materias controvertidas y protegiéndole frente a diversos atropellos constantes por parte del amplio mercado europeo. Sin embargo, la ejecución o, más bien, el ámbito procedimental para hacer realidad estos derechos ante juzgados y tribunales se había convertido en un camino realmente tortuoso para cualquier consumidor que quisiera reivindicarlos. Por ello, esta plataforma venía a solventar ese gran agujero en el que los consumidores perdían la posibilidad de

Aunque estas entidades pueden gestionar los conflictos en línea mediante una plataforma específica, hasta ahora, la plataforma no ha maximizado el potencial de las tecnologías avanzadas para mediar entre las partes directamente a través de software. A pesar de la implementación de módulos como el de conversación directa y autoevaluación desde junio de 2019, que buscan mejorar la comunicación entre consumidores y empresarios y guiar a los usuarios hacia la mejor opción de resolución, se queda corta en aprovechar completamente las herramientas de negociación en línea asistida o automatizada. Esto refleja una oportunidad perdida para fortalecer la mediación y facilitar una resolución de conflictos más eficiente y accesible mediante el uso de tecnologías digitales avanzadas[37].

B) Experiencia privada de ODR: el caso Kleros.

Antes de explicar la plataforma "Kleros", es necesario entender que la blockchain es una tecnología conexa que funciona como un sistema de registro distribuido y seguro que, por sus características, es capaz de crear confianza y transparencia en las transacciones digitales sin la necesidad de una autoridad central[38]. Esta tecnología funciona como un libro de contabilidad inmutable y compartido que es esencial para registrar y rastrear activos y transacciones en muchos sectores, desde finanzas, propiedad intelectual y administración de justicia por medio de plataformas de ODR[39].

La blockchain actúa como una infraestructura subyacente que soporta varias aplicaciones, incluidas criptomonedas como Bitcoin, contratos inteligentes y sistemas de votación, entre otros. Es una tecnología que está revolucionando la forma en que se intercambia la información y se garantiza su integridad, facilitando así

reivindicar sus derechos, debido a los altos costes procesales no solo de tiempo, sino también del dinero y esfuerzo que suponía acudir a los tribunales ordinarios".

37 Barrientos Camus, F.; Bozzo Hauri, S. y Jequier Lehuedé, E.: "Nuevas tecnologías para acceder a la justicia del consumidor", *Revista chilena de derecho y tecnología*, vol. 12, 2023, p. 22.

38 Ibáñez Jiménez, J.: *Derecho de Blockchain, y de la tecnología de registros distribuidos*, Aranzadi, Navarra, 2018, p. 31, indica que: "Se denomina cadena de bloques o Blockchain al resultado de aplicar una tecnología digital criptográfica que permite crear bases de datos almacenadas y compartidas en una comunidad o red no jerárquica o 'inter pares' ('peer to peer'), construida sobre grupos, bloques o eslabones de datos, ligados o vinculados entre sí, por códigos alfanuméricos llamados 'hashes'. Tecnología conocida como registro distribuido o DLT que, además de servir para crear un registro compartido y de enlace entre datos anotados, produce el efecto de identificar a estos de manera inequívoca, inalterable y transparente. Quedando los datos accesibles para quienes los compartan accediendo a una red o sistema multilateral donde todos pueden interactuar".

39 Polanco Medina, J.: "Internet y otras tecnologías disruptivas", en AA.VV.: *Tratado de Derecho digital* (coord. por E. M. Valpuesta Gastaminza y J. C. Hernández Peña), Wolter Kluwer, Madrid, 2021, p. 123, señala que la cadena de bloques tiene una serie de características, entre ellas la réplica distribuida de los bloques, es decir "…el conjunto de todos los bloques se descarga en todos los 'nodos' que participan en la cadena. Esto es lo que caracteriza a las redes de blokchain como 'distribuidas' o 'descentralizadas'. La información no se halla en un terminal central a la que acceden los usuarios, como pasa en otros muchos sistemas (entre ellos los bancarios), sino que se replica en todos los ordenadores que utilizan el programa. Esto hace que no exista el peligro de un ataque informático al sistema central que bien robe, bien manipule la información, pues cualquier ataque sólo afectará a uno o varios ordenadores, y el acervo de todas las transacciones sigue incólume en la mayoría de los operadores".

procesos más seguros y eficientes en distintas industrias, haciéndola una tecnología conexa fundamental para el desarrollo de soluciones innovadoras en la era digital. Dada su capacidad para asegurar la autenticidad y la trazabilidad de la información, la tecnología blockchain se considera una pieza clave en la transformación digital y en el desarrollo de nuevos modelos de negocio que requieren un alto nivel de seguridad en las transacciones digitales.

"Kleros" es una entidad internacional liderada por un grupo de expertos en matemáticas que lidera el cambio digital mediante el aprovechamiento del "crowdsourcing" para impartir justicia. Su propuesta es un mecanismo para dirimir controversias menores surgidas en el contexto del comercio electrónico, seguros o telecomunicaciones, ofreciendo soluciones seguras, rápidas y de bajo costo a las disputas.

La plataforma se destaca por su robustez, operando sobre la tecnología de blockchain y aprovechando la inteligencia colectiva, además de incorporar un sistema de recompensas que motiva a los jurados a participar en la resolución de conflictos. "Kleros" no aspira a suplantar al sistema judicial tradicional, sino que busca intervenir en aquellos espacios donde la justicia formal no llega.

El origen de "Kleros" se inspira en el sistema de justicia de la antigua Grecia donde los juicios eran llevados a cabo por ciudadanos. Así, a través de un sistema regulado que facilitaba la selección de jurados por medio de la "kleroterion" —una piedra con ranuras donde se colocaban fichas identificatorias (pinakion)—, en donde, un sistema aleatorio de dados blancos y negros determinaba la participación de los jurados, previniendo la corrupción en su elección.

Este enfoque de justicia entre iguales, en el que los ciudadanos ejercían como jueces, contrasta con el modelo posterior del siglo XVIII, donde solo los abogados conocían la ley. En el mundo actual, caracterizado por transacciones globales instantáneas, la justicia todavía opera bajo las limitaciones de las fronteras y tecnologías del siglo XVIII, lo que resulta en procesos judiciales prolongados.

"Kleros" opera mediante múltiples cortes (tribunales populares especiales), incluyendo las áreas de finanzas, seguros y comercio electrónico, todas las cuales se ocupan de disputas de pequeñas cantidades.

Por ejemplo, si Pedro y Ana acuerdan la creación de un sitio web por $500, pero surge un conflicto debido a la distancia geográfica entre ellos, "Kleros" ofrece una alternativa viable, toda vez que, en lugar de recurrir a un juicio tradicional, "Kleros" actúa como un sistema de arbitraje internacional. En este proceso, el dinero se deposita en una criptomoneda en un fondo de garantía, evitando así

que Ana pague directamente a Pedro, manteniendo el dinero seguro durante la resolución de la disputa.

Posteriormente, "Kleros" selecciona un jurado de expertos en sitios web de todo el mundo para analizar el caso y emitir un veredicto. Si el jurado determina que Ana tiene razón, el fondo de garantía le devuelve el dinero. En última instancia, el jurado es responsable de resolver la disputa. Los individuos interesados en ser jurados deben utilizar una moneda denominada "Pinakion", un criptoactivo que se deposita en una corte y que les otorga la posibilidad de ser seleccionados aleatoriamente entre otros postulantes. Una vez que se completan las postulaciones, "Kleros" elige cinco candidatos que actuarán como jurados en la disputa. Además, el sistema se basa en blockchain, lo que garantiza la transparencia en la selección de jurados, ya que ni siquiera el fundador de la empresa puede modificar el proceso.

Para fomentar la honestidad y un análisis informado, "Kleros" emplea la teoría de juegos de Thomas Schelling. Este enfoque busca que los jurados elijan la opción que creen que será elegida por la mayoría, promoviendo así la convergencia hacia la verdad en la resolución de disputas. Cada jurado que vote en línea con la mayoría recibe la moneda perdida por aquellos que votaron en contra, incentivando así la imparcialidad. A largo plazo, los jurados deshonestos que voten al azar perderán sus monedas, mientras que aquellos que actúen de manera honesta serán recompensados económicamente por sus decisiones basadas en la evidencia[40].

C) Experiencias chilenas de MASC.

En primer lugar, cabe destacar el reciente ajuste normativo en Chile de la Ley N°19.496 sobre protección de los derechos de los consumidores que permite el desarrollo de los ODR. Esto, ya que el nuevo artículo 3, letra g, promueve el uso de MASC, tales como la mediación, la conciliación y el arbitraje, facilitando su realización a través de medios electrónicos. Así, con la inclusión de esta disposición se reconoce el derecho del consumidor a acceder a los MASC, admitiendo la posibilidad del arbitraje en línea, lo que representa la apertura hacia nuevas herramientas tecnológicas, incluyendo el uso de la IA[41].

Ahora bien, antes de la reforma señalada con anterioridad ya se apreciaban en el modelo chileno innovaciones destacadas en esta área con la implementación de una plataforma de resolución de disputas en línea por parte de la Cámara de

40 Bozzo Hauri, S.: "Plataformas, algoritmos", cit., pp. 323-324.

41 Barrientos Camus, F; Bozzo Hauri, S y Jequier Lehuedé, E.: "Nuevas tecnologías", cit., p. 9.
Sobre una mirada crítica de las tecnologías y ODR en el caso chileno ver Martínez-Cárdenas, B.: "La online dispute resolution, acceso a la justicia y protección de los derechos del consumidor en el comercio electrónico: el caso chileno", *Revista de internet, derecho y política*, 2023, núm. 38, p. 10.

Comercio de Santiago, en el contexto de la promoción de los ODR. Esta plataforma, denominada "Resolución en línea", ofreció durante el último trimestre del año 2021 una alternativa para resolver disputas de manera gratuita para el cliente, con un plazo máximo de 10 días. Su objetivo es generar soluciones mediante el uso de algoritmos y mediación en línea. Es evidente que esta plataforma fomenta la negociación mediante el uso de IA, y también reconoce la necesidad de incorporar elementos de mediación cuando sea necesario[42].

La plataforma en cuestión, que es de uso gratuito para los consumidores, apunta a dirimir disputas en un período no mayor a 10 días consecutivos. Sin embargo, este lapso puede prolongarse hasta 15 días si es necesario entrar en una etapa de mediación. El proceso para iniciar un reclamo es sencillo y se puede realizar en cuatro pasos. Se emplea un sistema de negociación asistida que facilita el entendimiento directo entre empresas y consumidores mediante el uso de algoritmos, permitiendo alcanzar resoluciones sin mediadores externos. No obstante, la plataforma también tiene la capacidad de identificar situaciones que podrían beneficiarse de una mediación online opcional, ofreciendo esta alternativa y asignando un mediador de forma automática si se elige. La eficacia del proceso se ha demostrado en la rapidez de las respuestas iniciales de los proveedores, que suelen ocurrir en menos de 72 horas.[43]

Podemos observar que las compañías se están uniendo para ofrecer iniciativas que integran MASC con tecnología de IA. Utilizan algoritmos que buscan proporcionar soluciones en no más de 10 días. A pesar de ser un enfoque innovador, esta iniciativa parece ser parte de una estrategia de autorregulación del sector, que fomenta la negociación y la mediación sin tener claridad en cuanto a cómo se lleva a cabo la operación de los mediadores o su proceso de selección[44]. Por tanto, es crucial tener en cuenta los procedimientos de acreditación para las entidades que se encargan de la resolución alternativa de conflictos de consumo, tal como lo dicta la Directiva 2013/11/UE del Parlamento Europeo y del Consejo, de 21 de mayo de 2013. Dicha Directiva, en sus artículos 26 y subsiguientes, estipula los criterios que estas entidades deben cumplir para ser acreditadas, garantizando así que satisfacen los estándares de calidad exigidos por la legislación europea en relación con la resolución extrajudicial de conflictos de consumo. Esto les permite

42 Barrientos Camus, F. y Bozzo Hauri, S.: "Las dificultades de acceso a la justicia del consumidor en Chile y propuestas para incorporar IA en los métodos de resolución de conflictos", en AA.VV.: *Actualidad y Futuro del Derecho de Consumo*, Editorial Grupo Ibáñez, Bogotá, 2023, p. 309 y ss.

43 Barrientos Camus, F. y Bozzo Hauri, S.: "Las dificultades", cit., p. 309 y ss.

44 El Decreto Nº 84 que aprueba el reglamento que regula la mediación, conciliación y arbitraje en materia de consumo, de conformidad con lo dispuesto por la ley 19.496, sobre protección de los derechos de los consumidores, no aborda procesos de acreditación o de sistemas de aseguramiento de la calidad. Sobre este punto se puede ver Bozzo Hauri, S.: "Mediación y arbitraje de consumo en Chile: hacia un modelo de aseguramiento de la calidad", en AA.VV.: *Estudios de Derecho del Consumidor V, XI Jornadas Nacionales de Derecho de Consumo Universidad Alberto Hurtado* (dir. por F. Barrientos Camus y C. Santelices Vergara), Tirant lo Blanch, Valencia, 2023, pp. 571.

formar parte de un registro nacional de entidades acreditadas y de la Plataforma Europea de Resolución de Disputas en Línea (ODR)[45].

En el ámbito de la defensa de los derechos de los clientes financieros, existe en Chile una Defensoría del Cliente Bancario; no obstante, en sus métodos de resolución de conflictos no utilizan nuevas tecnologías que permitan automatizar el proceso y ofrecer así una mayor agilidad y menor coste en su administración.

Este mecanismo, que se asemeja a un arbitraje y permite realizar múltiples intentos de conciliación, tiende a ser un proceso más extenso que los sistemas como el de la Cámara de Comercio. Comienza con la presentación de una queja, seguida de un análisis inicial que puede derivar en tres posibilidades: en el primero, si la queja cumple con los requisitos y los documentos necesarios y es por un monto menor o igual a 3,5 Unidad de Fomento (UF), se envía directamente al banco en busca de una solución expedita; en el segundo, si el reclamo excede las 3,5 UF, se admite para asignación a un defensor; en el tercero, la queja puede ser rechazada y devuelta al cliente para completar información o documentación faltante. Si el reclamo es completo, se procede con el banco para encontrar una solución. Si el cliente rechaza la propuesta del banco, se asigna un defensor al caso. Este defensor revisa y decide si acepta el reclamo, y solo si lo acepta, se procede a su resolución. De este sistema se desconocen las estadísticas o datos de eficacia.

III. EXPERIENCIA EN EL DESARROLLO DE PROTOTIPOS DE SOFTWARE CON TECNOLOGÍA DE IA.

1. Cuestiones previas.

El desarrollo de software prototípico se caracteriza por la creación acelerada de un modelo inicial que refleja las funcionalidades clave del programa para su visualización y manipulación por parte del usuario. Esto facilita la evaluación práctica y permite recabar comentarios acerca de diversos factores como la usabilidad, la funcionalidad y el desempeño, entre otros.

El prototipo se puede modificar cuando sea necesario y todos los resultados obtenidos de las presentaciones ayudarán en el desarrollo del producto final. Para ello, se usaron prototipos con la finalidad de evaluar ideas de manera tangible, entregando ejemplos de soluciones que se pueden obtener en el ámbito del derecho con la tecnología que tenemos a disposición hasta la fecha. De esta misma manera, podemos identificar problemas y proponer mejoras futuras.

45 Barrientos Camus, F. y Bozzo Hauri, S.: "Las dificultades", cit., p. 309 y ss.

El modelo de prototipo desechable es útil cuando los requisitos del proyecto no están definidos totalmente. Los proyectos desechables se utilizan principalmente con fines de retroalimentación, ya que, cuando se completa el uso del prototipo, se descarta; pudiendo, los desarrolladores crear prototipos desechables para un solo aspecto de un proyecto.

Las fases de un modelo prototipo "usar y botar" son las siguientes:

Identificación de requerimientos: En esta etapa recopilamos los requerimientos iniciales del proyecto a través de encuestas o entrevistas para comprender las expectativas del cliente. En relación con nuestro proyecto, mediante reuniones semanales, se llega a algunos requerimientos del prototipo, como lo son funcionalidades, áreas que abarcar, la idea general y cómo está enfocado.

Planificación: La segunda etapa implica crear un diseño preliminar y planificar cómo desarrollar el proyecto. Para nuestro proyecto se realiza un bosquejo de cómo se verá la aplicación, se hace la elección de la paleta de colores a utilizar y se consideran las funcionalidades básicas como responder las preguntas solicitadas y tener una interfaz simple.

Prototipo: Se crea un prototipo real, utilizando la información recopilada en las etapas anteriores. El prototipo es una representación a pequeña escala que luego será presentada a los usuarios para su testeo y evaluación. A continuación, se desarrolla el prototipo N°1, el cual es construido en corto tiempo y utilizando mínimos recursos.

Mejoras de prototipos: Luego de que el usuario pruebe y evalúe el prototipo, se recopilan sus comentarios para refinar el prototipo hasta que el cliente esté satisfecho. De esta manera, permite comprender mejor el problema y sus posibles soluciones y así llegar a la idea de realizar dos prototipos más, con diferentes enfoques para el mismo problema y así analizar cada uno de ellos y su integración.

Finalización: Llegado a este punto, tendremos la base gráfica y funcional para desarrollar el producto final.

A continuación, se presentan los tres prototipos desarrollados para que el usuario pueda probar sus funcionalidades y así tenga diferentes alternativas de solución de consulta.

Se utiliza el modelo de prototipo "usar y botar", debido a que en este caso no necesariamente llegará a convertirse en un producto final, solo es usado como muestra para perfeccionar requerimientos y demostrar su funcionalidad.

Se realizaron tres prototipos, que llamaremos N°1, N°2 y N°3, los cuales se desarrollaron con el objetivo de entregar respuestas específicas a las consultas jurídicas chilenas, con diferentes modos y enfoques para demostrar la variedad de opciones que podemos manejar para ayudar en el ámbito del derecho.

Desarrollo de prototipos.

A) Prototipo N°1.

Este prototipo se ha realizado con NodeJS y el framework Express. Aquí no se utilizó ninguna biblioteca en particular para la interfaz del usuario; solo se hizo uso de Javascript y Bootstrap para el diseño de la aplicación. Este prototipo se nutre de la información recabada por nosotros mismos, por lo tanto, el entrenamiento parte desde cero, creando una serie de preguntas y respuestas a modo de ejemplo solo para mostrar el funcionamiento.

Se crea un arreglo donde se especifica el mensaje y respuesta a este mensaje, a través de la lógica de programación con Javascript y a través de palabras claves se logran las respuestas pertinentes.

Se realizaron pruebas ingresando una serie de preguntas establecidas en el arreglo mencionado anteriormente. También se probó solo escribiendo una palabra clave sin la pregunta completa, detectándola igualmente y entregando la respuesta pertinente. Al realizar preguntas que no están en el arreglo, el bot responde: "Lo siento, no entiendo tu pregunta".

B) Prototipo N°2.

El desarrollo del prototipo N°2 fue realizado con ReactJS, utilizando la biblioteca Chat UI Kit, la cual permite crear la interfaz de usuario en simples pasos. Las respuestas a las dudas de los usuarios se extraen mediante llamadas a la API Chat GPT. Cabe recalcar que usamos la versión gpt-3.5-turbo que aporta información que recopiló desde internet hasta el año 2021.

Se realizó un filtro a través de un prompt, el cual indica el contexto en el que el bot estará trabajando; en este caso se le indicó responder solo a dudas de ámbito legal basado en las leyes chilenas, como si este fuera un abogado especializado. Esto permite tener un gran abanico de respuestas a todas las temáticas del derecho de manera general. El bot discrimina si las preguntas no corresponden al tema establecido. Es importante recalcar que el bot está preparado para mantener una conversación extensa manteniendo el contexto a través de las preguntas, pudiendo tener cada vez respuestas más concretas.

Se realizan algunas pruebas en este prototipo donde se pudo verificar que, al iniciar la conversación, el bot nos entrega un mensaje predeterminado. Luego, se realizó una consulta relacionada al ámbito del derecho, dando una respuesta acorde a la consulta. A continuación, se probó al enviar letras aleatorias, donde también nos entregó una respuesta coherente pidiendo reformular la pregunta, ya que es ilegible, y por último se consultó por un tema que no tiene que ver con el derecho, la respuesta entregada es que no tiene la capacidad de responder consultas de otra índole.

C) Prototipo N°3.

El prototipo se realizó con ReactJS utilizando la biblioteca react-simple-chatbot para crear la interfaz de usuario, en este caso creamos una matriz de pasos a seguir. Cada paso contiene básicamente una ID, un mensaje, un validador u opciones para elegir.

Esto funciona como un árbol de decisiones, partiendo por ejemplo con el requerimiento de tu nombre, para luego preguntar si quieres consultar por un finiquito o pensión alimenticia. Así se escala, según las elecciones del usuario, hasta llegar a una pregunta más concreta. Permite guiar al usuario con una estructura predeterminada y generar derivación a un enlace de contacto según el requerimiento.

Se realizan pruebas seleccionando las respuestas del árbol de preguntas programado con la biblioteca de react-simple-chatbot. En primer lugar, solicita el nombre del usuario para personalizar la consulta. Luego comienza con la serie de preguntas, de las cuales se debe seleccionar la que interprete la inquietud y ahondar en el tema.

D) Resultados.

Análisis de prototipos. En relación con el prototipo N°1 podemos mencionar, como debilidad de este tipo de prototipos, que la base de datos debe ser creada por un especialista en la materia, lo que conllevará bastante tiempo para que sea lo suficientemente robusta y pueda dar respuesta a todas las consultas y sus complejidades; pero al mismo tiempo, gana en eficacia y será más específica contribuyendo al enfoque que le dará el dueño de la aplicación, personalizándola de acuerdo con sus necesidades y propuestas.

En el prototipo N°2 la debilidad radica en que las respuestas pueden llegar a ser muy generales y que no se tiene tanto control sobre ellas, más que el contexto mismo que se le da en un comienzo, pero ahí en más la IA es quien decide qué responder y cómo. El beneficio de este tipo de prototipo es que permite

acceder a mucha información debido a que la base de entrenamiento de la IA es muy grande, e irá en asenso con el tiempo lanzando nuevas versiones más potentes, como la última (versión GPT-4) que ya es diez veces más potente que su predecesora. Por lo tanto, se espera que en un futuro cercano las respuestas serán aún más específicas acercándose a la perfección.

En el prototipo N°3, al tener opciones desde un comienzo tan cerradas, puede que el usuario no encuentre similitud con su verdadera problemática. Este tipo de Chatbot se puede utilizar como un filtro que permite clasificar a los usuarios según sus problemáticas y así derivarlos a una página u contacto que sea especialista en su consulta; de esta manera, el especialista tendrá un conocimiento previo del cliente.

Validación de prototipos. En primer lugar, se comenzó con la elaboración de preguntas específicas en el ámbito laboral, proporcionadas por la abogada Katherine Romero Riquelme, quien se desempeña en el Tribunal de Cobranza Laboral y Previsional de San Miguel. Estas preguntas y respuestas están validadas al ser realizadas por un experto en la materia. Luego estos datos se usaron en los prototipos. Por otra parte, la profesional antes mencionada probó los tres prototipos, siendo validados exitosamente.

En segundo lugar, se realizó una encuesta a cinco abogados, quienes tuvieron acceso a probar los tres prototipos y contestar una encuesta a través de Google Forms. Esta herramienta nos permite obtener una conclusión respecto a la funcionalidad y necesidad de la aplicación de nuevas tecnologías en el ámbito del Derecho.

Entre las preguntas realizadas se encuentran las siguientes:

¿Está de acuerdo con la incorporación de nuevas tecnologías en el ámbito del derecho? ¿Cree que el uso de estas tecnologías (Chatbot de consulta, prototipos expuestos), contribuiría a reducir los tiempos de consulta y resolución de los casos? ¿Por qué? ¿Cree que estos prototipos son necesarios en el ámbito del derecho en la actualidad? ¿Cuál o cuáles le parecieron más interesantes?

El cien por ciento de las personas encuestadas está de acuerdo en la incorporación de nuevas tecnologías en el ámbito del Derecho.

En relación con el prototipo N°1, este requiere de un trabajo de parte de expertos en derecho para poder generar la base de datos, por lo que resulta engorroso debido a la alta demanda de trabajo de estos profesionales, por lo que el proceso sería lento y no inmediato. En cuanto al prototipo N°2, la IA aún provoca incertidumbre por muchos motivos: el resguardo de la privacidad,

el desconocimiento, miedo por no tener el control de la información emitida, entre otros, haciendo inviable su utilización por ahora. Por último, con respecto a las opiniones obtenidas en las encuestas a profesionales, se identifica el interés en el prototipo N°3, el que podría ser implementado de forma inmediata, proporcionando asesoría y derivación simultánea a los usuarios y permitiendo al cliente como al profesional tener una base de información previa, ahorrando tiempo y entregando una mejor atención.

De igual manera se debe mencionar que la reacción a los prototipos fue alentadora y se demostró interés en la factibilidad de implementación para ayudar a mejorar los servicios de atención, en este caso en un servicio público.

Algunas reflexiones acerca del desarrollo. El trabajo desarrollado cumplió con el objetivo general, en el sentido que permitió analizar el impacto y las implicaciones de las nuevas tecnologías de negociación asistida y evaluación de conflictos en el ambiente del Derecho, lo cual fue logrado al evidenciar con la recopilación de datos y ejemplos de la gran evolución a la hora de implementar las nuevas tecnologías. Como segundo punto, el desarrollo de los tres prototipos permite demostrar que se pueden entregar soluciones concretas con la tecnología disponible, lo cual fue comprobado con el correcto funcionamiento de los tres.

En relación con los objetivos específicos se puede afirmar lo siguiente:

- Al efectuar la investigación correspondiente, como se refleja en el marco teórico del proyecto, se logró recopilar diferentes herramientas tecnológicas que se implementan actualmente en el ámbito del Derecho, permitiendo reconocer y ampliar las opciones de solución.

- Se logra demostrar con diferentes ejemplos las nuevas tecnologías implementadas actualmente en el ámbito del Derecho, mediante la investigación descriptiva, y se exponen variados ejemplos para verificar que en varios lugares del mundo el avance es significativo y prometedor. La exposición de estos casos permite visualizar soluciones a problemáticas que en otros países ya tienen resueltas y que darían mejoras a nuestros sistemas.

- El desarrollo de los tres prototipos permitió mantener una conversación asertiva en el ámbito judicial, en dos casos en temas específicos (pensión de alimentos y finiquitos) y en otro abarcar el amplio espectro del derecho en Chile. Se observa la cantidad de maneras que hay para llegar a un objetivo similar con diferentes enfoques y para diferentes necesidades con la tecnología existente.

En relación con el desarrollo de los tres prototipos nos permite demostrar que se pueden entregar diferentes soluciones, en este caso a través de Chatbots para diferentes contextos de una misma problemática. Con la tecnología en constante evolución, podemos esperar avances significativos y cada vez más sofisticados en el ámbito del derecho, logrando digitalizar procedimientos legales. Estas nuevas tecnologías de negociación asistida se pueden ya implementar dando un paso hacia un mejor acceso a la justicia de los consumidores. Esto gracias a que los métodos de resolución de conflictos serán más económicos para los consumidores, quitando así la barrera del coste oportunidad que significaba iniciar una disputa.

IV. CONCLUSIONES.

El presente trabajo nos permite constatar que la negociación asistida a través de desarrollo de software es una herramienta que permite facilitar los acuerdos de manera temprana entre proveedores y consumidores. Además, es posible advertir que esta es una herramienta dentro de otras varias que, si se integran a los MASC y en especial a los ODR y sus plataformas, el coste de administración de la mismas disminuye gracias a que es posible agilizar los procesos, reduciendo tiempos y, sobre todo, se puede prescindir del trabajo humano, lo que en general es uno de los elementos que eleva el coste de administración.

En Chile existe una oportunidad gracias a la reforma de la Ley N° 19.496 sobre protección de los derechos de los consumidores, a partir de lo incorporado en la letra g de su artículo 3, en el sentido de que hace posible avanzar en mecanismos de solución de conflictos alternativos a través de medios online; es decir, sistemas ODR. No obstante, es necesario fortalecer la regulación con un modelo que se centre en el aseguramiento de la calidad de dichos procesos.

Con relación a las distintas experiencias, se puede apreciar iniciativas de índole pública como lo es la plataforma europea online de justicia. Si bien esta plataforma significa un avance importante en el desarrollo de TICs en el ámbito de los ODR, no se aprecia una utilización intensa en herramientas tecnológicas que permitan obtener todo el beneficio que significa su uso y que, como se ha mostrado en este trabajo, están disponibles. En el ámbito privado se advierte el trabajo de Kleros, la cual se apoya en el desarrollo de Blockchain; es decir, en un modelo descentralizado a través de la colaboración de privados expertos.

Por último, cabe destacar que este trabajo implicó un significativo esfuerzo metodológico en el uso de prototipos, que iba más allá de una mera revisión bibliográfica de los avances reportados en la literatura jurídica. Se realizó una comprobación práctica de la viabilidad de estos prototipos, validándolos a través de su aplicación en escenarios reales, como lo sugieren diversos textos del campo.

Esta validación empírica no solo confirmó su aplicabilidad, sino que también evidenció su potencial como herramientas efectivas en el ámbito jurídico.

BIBLIOGRAFÍA

Arley Orduña, A.: *Resolución electrónica de disputas (ODR): acceso a justicia digital*, Tirant lo Blanch, Valencia, 2021.

Barrientos Camus, F. y Bozzo Hauri, S.: "Las dificultades de acceso a la justicia del consumidor en Chile y propuestas para incorporar IA en los métodos de resolución de conflictos", en AA.VV.: *Actualidad y Futuro del Derecho de Consumo*, Editorial Grupo Ibáñez, Bogotá, 2023.

Barrientos Camus, F.; Bozzo Hauri, S. y Jequier Lehuedé, E.: "Nuevas tecnologías para acceder a la justicia del consumidor", *Revista chilena de derecho y tecnología*, vol. 12, 2023, pp. 1-35.

Boucier, D.: *Inteligencia Artificial y Derecho*, Editorial UOC, Pompeu, 2003.

Bozzo Hauri, S.: "Mediación y arbitraje de consumo en Chile: hacia un modelo de aseguramiento de la calidad", en AA.VV.: *Estudios de Derecho del Consumidor V, XI Jornadas Nacionales de Derecho de Consumo Universidad Alberto Hurtado* (dir. por F. Barrientos Camus y C. Santelices Vergara), Tirant lo Blanch, Valencia, 2023, pp. 571-584.

Bozzo Hauri, S.: "El uso de las nuevas tecnologías como forma de disminuir las barreras de acceso a la justicia del consumidor en Chile", *Vniversitas Jurídica*, 2023, vol. 72.

Bozzo Hauri, S.: "Plataformas, algoritmos y su rol en la resolución de conflictos en el ámbito de consumo", en AA.VV.: *Justicia Poliédrica en periodo de mudanza* (dir. por S. Barona Vilar), Tirant lo Blanch, Valencia, 2022, pp. 313-330.

Bozzo Hauri, S. y Remeseiro Reguero, R.: "Resolución de conflictos en consumo: ¿Una solución a través de la inteligencia artificial?, en AA.VV.: *Justicia algorítmica y neuroderecho* (edit. por S. Barona Vilar), Tirant lo Blanch, Valencia, 2021, pp. 611-631.

Catalán Chamorro, M.: *El acceso a la justicia de consumidores: los nuevos instrumentos del ADR y ODR de Consumo*, Tirant lo Blanch, Valencia, 2019.

Catalán Chamorro, M.: "Una plataforma ODR europea ¿Una solución?, en AA.VV.: *Derecho del consumo y protección del consumidor sustentable en la sociedad digital del siglo XXI* (edit. por S. Barona Vilar), Edición Universidad Autónoma de Chile, Santiago, 2023, pp. 357-376.

Centro de Estudios de Justicia de las Américas, C.: *Resolución de Conflictos en línea*, Equipo Editorial y Gráfico CEJA, Santiago, 2022.

Contini, F. y Velicogna, M.: "Del acceso a la información al acceso a la justicia: diez años de e-justice en Europa", *El rol de las Nuevas Tecnologías en el Sistema de Justicia,* 2021, núm. 16, pp. 30-47.

De las Alas Pumariño, E.: *El Arte de Negociar*, AIIM, Madrid, 2014.

Díaz, A.: *Mecanismos Alternativos de Solución de Conflictos*, Academia Judicial, Santiago, 2019.

Díaz, L.: *La Mediación y Negociación para Resolver Conflictos Legales,* 2019.

Dobratinich, A.: "Inteligencia Artificial y Justicia: Aplicabilidad de la tecnología en las decisiones judiciales en Argentina", *Revista Direitos Culturais,* 2022, vol. 17, núm. 42, pp. 203-216

Elisavetsky, A.: *La mediación a la luz de las nuevas tecnologías*, Errelus, Buenos Aires, 2019.

Esteban de la Rosa, F.: "Tecnología de la información y de la comunicación y resolución de litigios: el modelo europeo de promoción del ODR en el ámbito de los litigios de consumo", *Revista iberoamericana de derecho internacional y de la integración,* 2019, núm. 10, pp. 86-107.

Gonzalbo Aizpuru, P.; Mayer Celis, L.: *Conflicto, resistencia y negociación en la historia*, Colegio de México, México, 2016.

Ibáñez Jiménez, J.: *Derecho de Blockchain y de la tecnología de registros distribuidos*, Aranzadi, Navarra, 2018.

Marcos Francisco, D.: "Sistema arbitral de consumo: algunas propuestas 'inteligentes' de lege ferenda", *InDret*, 2024, núm. 1, pp. 114-150.

Martín Diz, F.: "Modelos de aplicación de Inteligencia Artificial en justicia asistencial o predictiva versus decisoria", en AA.VV.: *Justicia algorítmica y neuroderecho* (edit. por S. Barona Vilar), Tirant lo Blanch, Valencia, 2021, pp. 65-85.

Martínez-Cárdenas, B.: "La online dispute resolution, acceso a la justicia y protección de los derechos del consumidor en el comercio electrónico: el caso chileno", *Revista de internet, derecho y política*, 2023, núm. 38, pp. 1-13.

Montesinos García, A.: "Inteligencia Artificial y ODR", en AA.VV.: *Justicia algorítmica y neuroderecho* (edit. por S. Barona Vilar), Tirant lo Blanch, Valencia, 2021, pp. 507-531.

Pérez Estrada, M. J.: *Fundamentos jurídicos para el uso de la inteligencia artificial en los órganos judiciales*, Tirant lo Blanch, Valencia, 2022.

Polanco Medina, J.: "Internet y otras tecnologías disruptivas", en AA.VV.: *Tratado de Derecho digital* (coord. por E. M. Valpuesta Gastaminza y J. C. Hernández Peña), Wolter Kluwer, Madrid, 2021.

Reiling, D: "Comprendiendo las tecnologías de la información para la resolución de conflictos", *El rol de las Nuevas Tecnologías en el Sistema de Justicia,* 2021, núm. 16, pp. 18-29.

Vargas Correa, A.: *Creación de Valor en Procesos de Negociación Asistida*, Editorial Académica Española, España, 2018.

LA ALGORITMIZACIÓN DEL DICTAMEN PERICIAL: ¿PUERTA DE ENTRADA PARA LA APARICIÓN DEL "PERITO-ROBOT"?*

THE ALGORITHMISATION OF THE EXPERT OPINION: A GATEWAY TO THE EMERGENCE OF THE "ROBOT EXPERT"?

Actualidad Jurídica Iberoamericana Nº 21, agosto 2024, ISSN: 2386-4567, pp. 434-467

* Este trabajo ha sido redactado en el marco del Proyecto de investigación "Bases para la modernización y mejora del régimen de propiedad industrial e intelectual ante los desafíos de la agenda digital y las exigencias de sostenibilidad (INNOPI)" (expediente: PID2022-136567NB-I0) financiado por MCIN/AEI/10.13039/501100011033/ FEDER, UE.

Marta CANTOS PARDO

ARTÍCULO RECIBIDO: 29 de mayo de 2023
ARTÍCULO APROBADO: 1 de julio de 2024

RESUMEN: La algoritmización del proceso judicial constituye uno de los mayores retos de futuro para la justicia. Este trabajo analiza la relación entre algoritmos y prueba. Concretamente, estudia la valoración de la prueba pericial por medio de sistemas algorítmicos auxiliadores y la posibilidad de que los dictámenes periciales puedan ser elaborados por algoritmos con inteligencia artificial generativa, identificando algunos de sus problemas y desafíos.

PALABRAS CLAVE: Inteligencia artificial, algoritmización de la prueba; prueba pericial; valoración de la prueba.

ABSTRACT: *The algorithmisation of the judicial process constitutes one of the largest challenges for the future of justice. This work analyzes the relationship between algorithms and evidence. Specifically, it studies the evaluation of expert evidence through auxiliary algorithmic systems and the possibility that expert opinions can be done by algorithms with generative artificial intelligence, identifying some of their problems and challenges.*

KEY WORDS: *Artificial intelligence; evidence algorithmisation; expert evidence; evaluation of evidence.*

SUMARIO.- I. LA PRUEBA PERICIAL COMO MEDIO DE PRUEBA POR EXCELENCIA EN MUCHOS PROCESOS CIVILES.- II. ALGORITMIZACIÓN DE LA PRUEBA. III. VALORACIÓN DE LA PRUEBA PERICIAL POR ALGORITMOS.- 1. Valoración de la cualificación y experiencia del perito.- 2. Valoración del contenido del informe pericial.- 3. Valoración de la imparcialidad y objetividad de un perito.- 4. Valoración de la comparecencia del perito en el juicio o la vista.- 5. A modo de conclusión.- IV. ELABORACIÓN DE DICTÁMENES PERICIALES POR ALGORITMOS.- 1. Inteligencia artificial generativa para la elaboración de dictámenes.- 2. Múltiples dudas desde la óptica legal actual.- V. RETOS DE FUTURO.

I. LA PRUEBA PERICIAL COMO MEDIO DE PRUEBA POR EXCELENCIA EN MUCHOS PROCESOS CIVILES.

La prueba pericial es un medio de prueba en concreto que se regula principalmente en los arts. 335 a 352 LEC. Mediante el dictamen pericial[1] se aportan al proceso los conocimientos científicos, artísticos, técnicos o prácticos que permiten al juez valorar la existencia de hechos y sus condiciones, así como conocer el contenido o interpretación de otras pruebas prácticas[2], como podría ser documental de tipo técnico o contable. En este sentido, el perito actúa como un auxiliador del órgano jurisdiccional, pues complementa la capacidad de juicio del juez, proporcionándole unas máximas de experiencia que le resultan desconocidas o no sabe aplicar adecuadamente[3], de modo que el perito le ilustra sobre las circunstancias del caso objeto de debate[4].

Para su admisión, el art. 335.1 LEC exige que estos conocimientos especializados (científicos, artísticos, técnicos, etc.) sean necesarios para valorar hechos o circunstancias relevantes en el asunto o para adquirir certeza sobre ellos.

Esta prueba puede resultar crucial en muchos casos. Al respecto, afirma Picó i Junoy que «la prueba pericial es la "regina probationum" en aquellos procesos en los que para resolver el conflicto son realmente imprescindibles saberes

1 Aunque en este trabajo se utilizarán de forma sinónima, téngase en cuenta la diferencia entre informe pericial y dictamen pericial. En palabras de Izquierdo Blanco, P.: "¿Qué espera un juez de un buen dictamen para ser convincente?", en AA.VV.: *La prueba pericial a examen. Propuestas de lege ferenda* (dir. por J. Picó i Junoy), Bosch, Barcelona, 2020, p. 217, un informe pericial "puede obrar en los autos en forma de prueba documental, o trabajo de un tercero o testigo o, incluso de una parte demandada, pero sin el contenido legal de dictamen de peritos y sin la posibilidad de ser valorada como tal por el Juez al amparo del art. 348 LEC", y un dictamen pericial es la "conclusión del trabajo o estudio que hace un perito sometido a las limitaciones técnicas del art. 335.1 de la LEC".

2 Cortés Domínguez, V.: "El dictamen de peritos", en V. Cortés Domínguez, V. y V. Moreno Catena, *Derecho Procesal Civil, Parte General*, Tirant lo Blanch, Valencia, 2021, p. 273.

3 Gómez Colomer, J. L.: "Los medios de prueba en concreto", en AA.VV.: *Proceso Civil, Derecho Procesal II* (coord. por J. L. Gómez Colomer y S. Barona Vilar), Tirant lo Blanch, Valencia, 2023, p. 262.

4 Picó i Junoy, J.: "La prueba pericial civil en la literatura procesal española", en AA.VV.: *La prueba pericial a examen. Propuestas de lege ferenda* (dir. por Picó i Junoy, J.), Bosch, Barcelona, 2020, p. 35.

• Marta Cantos Pardo
Profesora Ayudante Doctora, Universitat de València. Correo electrónico: marta.cantos@uv.es

científicos, técnicos o especializados»[5]. Esto es, sin duda, uno de los atributos que caracterizan a muchos de procesos civiles y que intuimos caracterizará a muchos más en el futuro, derivados del creciente protagonismo de la tecnología en todos los ámbitos de nuestra vida. Un ejemplo de ello son los procesos en materia de propiedad industrial en los que los aspectos técnicos resultan claves para enjuiciar el asunto[6].

Dada su relevancia, es común que las partes envueltas en un proceso de estas características encarguen a expertos la elaboración de dictámenes periciales, pues su contenido les resulta esencial para poder articular su estrategia procesal. Así, podemos encontrarnos con dictámenes de perito designados por las partes o el tribunal a solicitud de las partes (art. 339 LEC)[7].

Asimismo, e íntimamente relacionado con la importancia de esta prueba, es muy frecuente que las partes intenten apurar los plazos legales de presentación de los dictámenes, a fin de que las contrapartes dispongan de estos el mínimo tiempo posible y tengan menos margen de maniobra para plantear su estrategia defensiva. Esto les lleva a valerse de las excepciones legales a la regla general, que es la aportación de los dictámenes de parte junto con la demanda y la contestación con efectos preclusivos (arts. 336.1, 3 y 4 LEC).

Una de las vías excepcionales de las que suele abusarse en la práctica para la aportación tardía del dictamen consiste en la posibilidad de dejar anunciado el informe en la demanda o contestación para evitar presentarlo en ese momento. No obstante, la ley requiere su aportación en cuanto dispongan de este y, en todo caso, cinco días antes de iniciarse la audiencia previa al juicio ordinario o en treinta días desde la presentación de la demanda o contestación en el juicio verbal (art. 337.1 LEC)[8]. También, en virtud del art. 338 LEC, es posible la posterior aportación

5 Izquierdo Blanco, P.: "¿Qué espera", cit., p. 216.

6 De hecho, Vázquez Pizarro, M. T.: "Especialidades de la práctica de la prueba pericial en los procedimientos sobre patentes", *Diario La Ley*, 2020, núm. 9568 (LA LEY 900/2020), que es magistrada del Juzgado de lo Mercantil núm. 9 de Madrid, juzgado especializado en patentes y otros derechos de propiedad industrial, lo califica como "el medio más eficaz para que puedan analizarse los elementos de la patente y decidir la controversia".

7 En la práctica, normalmente es más frecuente acudir a informes periciales de parte. Por ejemplo, en los procesos en materia de propiedad industrial es muy habitual que cada parte cuente con su propio informe pericial, siendo mucho menos común que las partes soliciten el nombramiento de perito judicial. Lo que obedece a razones como las elevadas provisiones de fondos que los peritos suelen solicitar y el riesgo que existe de que se nombre a un perito que, aun teniendo la formación técnica, no tenga los conocimientos específicos que requiere la evaluación técnica de la cuestión. A lo que necesariamente se añade la incertidumbre que supone que se pueda designar un perito que pueda emitir un informe de contenido desconocido y que pueda resultar perjudicial para la parte. Vázquez Pizarro, M. T.: "Especialidades de", cit. (LA LEY 900/2020).

8 No obstante, existen salvedades a esta excepción. Por ejemplo, en los procesos en materia de propiedad industrial, el art. 119.2 Ley de Patentes amplía el plazo de contestación a la demanda a dos meses, por lo que restringe la aplicación de lo previsto en el art. 337 LEC para la aportación tardía de los dictámenes, que no será de aplicación para el demandado, salvo que la demandada justifique cumplidamente la imposibilidad de aportar el informe. Igualmente, Massaguer Fuentes pone de relieve una de las cuestiones que se han planteado en la práctica y que se desprende del hecho de que existan conflictos paralelos en diversos

de dictámenes (al menos cinco días antes del juicio o vista) cuando su necesidad o utilidad se ponga de manifiesto a causa de las alegaciones del demandado en la contestación a la demanda o de las alegaciones o pretensiones complementarias admitidas en la audiencia previa, a tenor del art. 426 LEC.

Así, se pone de manifiesto como ya el legislador es consciente de la relevancia de esta prueba, tanto respecto del contenido como del momento de su presentación.

Pese a la importancia de estos informes, el juez no podrá acordar de oficio la elaboración de dictamen pericial, salvo los casos previstos en la ley sobre procesos sobre declaración o impugnación de la filiación, paternidad y maternidad, capacidad de las personas y matrimoniales (art. 339.5 LEC)[9]. No obstante, en la audiencia previa, si el juez considerase que las pruebas propuestas por las partes son insuficientes para el esclarecimiento de determinados hechos controvertidos, sí podrá ponerlo de manifiesto a las partes, pudiendo señalar las pruebas que considere convenientes y necesarias, como una prueba pericial al respecto de alguna cuestión particular, de modo que las partes puedan completar o modificar sus proposiciones de prueba (art. 429.1 LEC)[10].

En otro orden de cosas, todo perito debe actuar bajo las máximas de independencia, imparcialidad y objetividad. No obstante, cada parte tiene la posibilidad de designar al perito que considere a los efectos de emitir su informe de parte y ello resulta en que en la práctica estos informes prácticamente siempre son favorables a los intereses de quienes los presentan —lo que resulta evidente, pues en caso contrario, si cuentan con ellos antes de la presentación de la demanda o contestación, no los aportarían—. Es innegable que "de facto" se perjudica la independencia del perito de parte a través de cuestiones como el control de la información que se le proporciona o las condiciones de pago que se le imponen[11].

países, de modo que si en esos procesos extranjeros el tribunal encarga la elaboración de informes a peritos, estos informes puedan ser traídos al proceso español y ser aportados en cuanto se disponga de ellos, aplicando las previsiones de los arts. 270 y 286 LEC, que permiten la presentación de documentos "a posteriori". En este sentido, SAP de Barcelona (Sección 15ª) 22 mayo 2017 (AC 2017, 1027), y Massaguer Fuentes, J.: *Acciones y procesos de infracción de Derechos de Propiedad Industrial*, Civitas Thomson Reuters, Cizur Menor, 2020, p. 313.

9 También, existen algunas excepciones a la regla general, por ejemplo, el art. 120.7 LP establece que en los procesos de nulidad de las patentes, de oficio o a petición de parte, pueda acordarse que se emita un informe pericial de la OEPM sobre aquellos extremos concretos en los que los informes aportados por las partes resulten contradictorios. Algunos autores, cuya opinión compartimos, han cuestionado esta potestad del juez de acordar, sin petición de parte, la emisión de este dictamen, teniendo en cuenta que se hace referencia a la LEC y que esta norma, salvo excepciones expresas, no permite que el juez proponga y acuerde prueba de oficio. Montañá Mora, M.: "La Nueva Ley de Patentes y el sector farmacéutico", *Cuadernos Derecho Farmacéutico*, 2015, núm. 55, p. 19.

10 Escalada López, M. L.: "El dictamen de peritos en el proceso de patentes", *Revista de Derechos de la Competencia y Distribución*, 2011, núm. 9/2011 (versión electrónica).

11 Váquez Rojas, C.: "La imparcialidad, la independencia y la objetividad pericial. Los factores humanos de los expertos", en AA.VV.: *La prueba pericial a examen. Propuestas de lege ferenda* (dir. por J. Picó i Junoy), Bosch, Barcelona, 2020, p. 130.

Así, se pueden formular tachas contra los peritos, cuestionando su vinculación con las partes, especialmente por las relaciones profesionales que puedan haber existido entre el perito y quien le realiza el encargo[12].

Creemos que no nos equivocamos si afirmamos que en el futuro es posible que la inteligencia artificial desarrolle un papel fundamental en relación con la prueba pericial, pues los sistemas algorítmicos podrían ofrecernos una mejor solución a muchas de las cuestiones que aquí se han planteado.

En estos casos, los algoritmos podrían resultar de gran utilidad pues podrían arrojar resultados más exactos y fiables desde el punto de vista de la técnica, que los que puede ofrecer un humano por muchos conocimientos y experiencia que acumule, ya que puede tener en cuenta un mayor volumen de datos. Además, y teniendo en consideración que "la máquina no descansa", la utilización de estos algoritmos podría favorecer la rápida emisión de informes lo que podría acabar con las excepciones procesales que permiten el uso (y abuso) de la presentación tardía de los informes con el único propósito de entorpecer la defensa de la contraparte. También, la objetivización que ofrecen estos sistemas podría reducir los problemas que pueden surgir sobre la posible independencia, objetividad e imparcialidad del perito.

Partiendo de las citadas ventajas, un sistema algorítmico podría auxiliar a un perito en la elaboración de su informe, incluso en algunos casos emitir un resultado concluyente. De hecho, en el futuro un sistema algorítmico avanzado podría llegar a emitir (redactar) un dictamen pericial, lo que nos podría llevar a hablar de la aparición de la figura del "perito-robot"[13].

Estas son solo algunas muestras de las posibilidades que ofrece la introducción de los algoritmos en este ámbito. Así, el objeto de este artículo es analizar las posibilidades que podría ofrecer la implementación de los algoritmos en relación con la prueba pericial en particular. Para ello, en los siguientes apartados se estudia, en primer lugar, la algoritmización de la prueba en general, para, a continuación, tratar las posibilidades que pueden ofrecer estas herramientas algorítmicas en la valoración de la prueba pericial y, por último, analizar las cuestiones que podrían surgir si es la propia máquina la que elabora el dictamen pericial.

12 Sin embargo, la jurisprudencia no ha considerado que la colaboración profesional entre el perito o la agencia de propiedad industrial en la que este presta servicios y la parte que le encomienda el informe sean motivos suficientes para considerar perjudicada su independencia (SJMe núm. 10 de Barcelona 18 octubre 2015 (JUR 2015, 150192).

13 El término "perito-robot" ya ha sido previamente acuñado en lengua inglesa como "expert robot", por ejemplo, por Katz, P.: "Expert robot: using artificial intelligence to assist judges in admitting scientific expert testimony", *Albany Law Journal of Science & Technology*, 2014, vol. 24, Issue 1, pp. 1-46.

Como se verá en este trabajo, son incontables los retos que se plantean pues la implementación de este tipo de sistemas requiere de una regulación que deberá tener en cuenta cuestiones muy complejas, como la fiscalización de los algoritmos o la adecuada selección e introducción de los datos utilizados para su "alimentación".

II. ALGORITMIZACIÓN DE LA PRUEBA.

El uso masivo de las nuevas tecnologías en prácticamente todos los aspectos de nuestras vidas ha dado lugar a la aparición de multitud de nuevas fuentes de prueba vinculadas con la tecnología[14], como son las redes sociales; las nuevas formas de transmisión de información (WeTransfer, OneDrive, etc.); las plataformas de comercio electrónico (Amazon, Ebay…) y las nuevas formas de contratación electrónica; los múltiples dispositivos electrónicos que utilizan el "internet de las cosas"; la aparición de archivos de páginas web, como "The Wayback Machine", que permite acreditar que una determinada información estaba publicada en una concreta página web en una fecha y hora exactas[15]; incluso la sustitución de las palabras por "emojis", lo que ya se está admitiendo por los tribunales como prueba de lo que representan[16], entre otras muchas.

La inteligencia artificial es sin duda el siguiente escalón y, como en el caso anterior, se aplica cada vez a más ámbitos de nuestra vida[17], por lo que, en línea con lo anterior, también podría constituir fuente de prueba en el futuro[18]. Siguiendo la definición de inteligencia artificial dada por Nieva Fenoll: "podría decirse que [la inteligencia artificial]

14 Picó i Junoy, J.: "Retos del derecho probatorio ante las nuevas tecnologías", en AA.VV.: *Inteligencia artificial legal y administración de justicia* (dir. por S. Calaza López y M. Llorente Sánchez-Arjona), Thomson Reuters Aranzadi, Cizur Menor, 2022, pp. 440-441.

15 Cantos Pardo, M.: "The Wayback Machine: origen, retos y utilización como fuente de prueba en materia de propiedad industrial", *ADI*, 2022, núm. 42, pp. 265-280.

16 El uso de los "emojis" con efectos probatorios se ha admitido por los tribunales españoles, pese a que no ha sido admitido en todos los casos. Abel Fabregó, A.: "Los emojis como fuente de prueba", *Revista Jurídica de Catalunya*, 2021, núm. 4-2021, pp. 127-136.

17 No obstante, algunos expertos en la materia, como Nieva Fenoll, J.: "Inteligencia artificial y proceso judicial: perspectivas ante un alto tecnológico en el camino", en AA.VV.: *Inteligencia artificial legal y administración de justicia* (dir. por S. Calaza López y M. Llorente Sánchez-Arjona), Thomson Reuters Aranzadi, Cizur Menor, 2022, p. 419, han percibido un parón tecnológico, que supone que su desarrollo se encuentra en estos momentos ralentizado respecto a tiempos anteriores.

18 De Hoyos Sancho, M.: "El libro blanco sobre inteligencia artificial de la Comisión Europea: reflexiones desde las garantías esenciales del proceso penal como "sector de riesgo"", *Revista Española de Derecho Europeo*, 2020, núm. 76, p. 22, explica que: "Cuando hablamos de sistemas IA que pueden ser, primero fuente de prueba y, en su caso, posteriormente aportados al proceso como medios de prueba, estamos pensando en las posibilidades que para formar la convicción del juzgador ofrecen herramientas tan dispares como las que se engloban bajo los conceptos de domótica, de asistencia a la conducción, los sistemas de compra conectados a la información que recogen los smart phones, los relojes inteligentes con sensores biológicos que registran multitud de datos, prevén y sugieren pautas de conducta o, en general, el llamado internet de las cosas. […] En definitiva, como puede suponerse a la vista de estos y otros muchísimos ejemplos que ya son realidad actualmente, todos estos sistemas IA pueden proporcionar información muy valiosa para una investigación y, en su caso, son susceptibles de llegar a acceder como medio de prueba […]".

describe la posibilidad de que las máquinas, en alguna medida, "piensen", o más bien imiten el pensamiento humano a base de aprender y utilizar las generalizaciones que las personas usamos para tomar nuestras decisiones habituales"[19].

Este protagonismo creciente de la inteligencia artificial afecta a múltiples aspectos de la esfera jurídica[20]. Concretamente, la inteligencia artificial tiene un largo camino que recorrer en el ámbito del Derecho procesal y puede reportar múltiples beneficios al proceso, como son la reducción de tiempos y la simplificación de trámites[21], pudiendo incluso mejorar la calidad de la justicia en términos generales, pues, por ejemplo, podría disponerse de herramientas que ayuden a las partes y al juez a encontrar mejores fundamentos legales, jurisprudenciales o doctrinales[22]. En este sentido, ya se han desarrollado multitud de estudios que analizan su posible incorporación y los grandes retos que implica su implementación, entre otros muchos, la afectación y menoscabo de principios procesales esenciales o el respeto a los derechos fundamentales[23]. Por tanto, su desarrollo y su regulación deben tener en cuenta estos límites para garantizar que no se vean perjudicados los principios y derechos referidos[24].

Esta algoritmización del proceso judicial de la que tanto se habla puede realizarse con diferentes grados de intensidad, que van desde la mera automatización de tareas procesales sencillas como es la verificación de requisitos básicos respecto de la presentación de documentos dentro de plazo[25]; al uso de sistemas algorítmicos

19 Nieva Fenoll, J.: *Inteligencia artificial y proceso judicial*, Marcial Pons, Madrid, 2018, p. 20.

20 Barona Vilar, S.: "Cuarta revolución industrial (4.0.) o ciberindustria en el proceso penal: revolución digital, inteligencia artificial y el camino hacia la robotización de la justicia", *Revista Jurídica Digital UANDES*, 2019, vol. 3, núm. 1, p. 7.

21 Montesinos García, A.: "Reflexiones sobre la algoritmización del proceso judicial civil", en AA.VV.: *Sistemas predictivos en la justicia civil* (ed. por A. I. Blanco García), Tirant lo Blanch, Valencia, 2024, p. 24.

22 De hecho, si suponemos que en el futuro estas herramientas algorítmicas estarán incorporadas a la práctica jurídica ordinaria, la formación de los juristas también debe adaptarse a este nuevo escenario. Khatniuk, N.; Shestakovska, T.; Rovnyi, V.; Pobiianska, N. y Surzhyk, Y.: "Legal principles and features of artificial intelligence use in the provision of legal services", *SDG Journal of Law ans sustainable development*, 2023, vol. 11, núm. 5, p. 12, afirman que: "Therefore, there is an urgent need to develop new methods of acquiring knowledge and practical skills for future lawyers in the field of innovative technologies and artificial intelligence".

23 Barona Vilar, S.: *Algoritmización del Derecho y de la Justicia: De la Inteligencia Artificial a la Smart Justice*, Tirant lo Blanch, Valencia, 2021, pp. 390-415; De Luis García, E.: "Sistemas predictivos y tutela civil: impacto sobre los derechos y garantías procesales", en AA.VV.: *Sistemas predictivos en la justicia civil* (ed. por A. I. Blanco García), Tirant lo Blanch, Valencia, 2024, pp. 239-245, y Montesinos García, A.: "Afectación de los derechos y garantías procesales por el empleo de algoritmos predictivos", en AA.VV.: *El proceso como garantía*, (dir. por J. M. Asensio Mellado), Atelier, Barcelona, 2023, pp. 703-714.

24 En esta línea, resulta destacable el acuerdo provisional entre el Consejo de la UE y el Parlamento Europeo sobre la propuesta relativa a las normas armonizadas en materia de inteligencia artificial, el denominado "Reglamento de Inteligencia Artificial".

25 Bonet Navarro, J.: "La tutela judicial de los derechos no humanos. (De la tramitación electrónica al proceso con robots autónomos)", *Revista Ceflegal*, 2018, núm. 208, pp. 80-81. Asimismo, téngase en cuenta que actualmente ya se utilizan en los tribunales españoles herramientas asistenciales de tipo algorítmico para la realización de ciertas tareas, algunas de ellas en su formato definitivo y otras como proyectos piloto. Es el caso de VioGen, Sistema de Comparecencias Apud Acta en Remoto, Carpeta justicia, Escritorio Virtual de Inmediación Digital, etc. Las referencia y explica: Catalán Chamorro, M. J.: *La justicia digital en España, retos y desafíos*, Tirant lo Blanch, Valencia, 2023, pp. 139-162.

que auxilien al juzgador a tomar determinadas decisiones, verbigracia, ayudándole a valorar el "periculum in mora" respecto de una medida cautelar[26]; llegando incluso a la sustitución del juez por la máquina, lo que algunos llaman el "juez-robot". Esta posibilidad cuenta con multitud de obstáculos advertidos por la doctrina[27].

Téngase en cuenta que la inteligencia artificial, en realidad, se concreta en modelos estadísticos complejos capaces de autoajustarse según la nueva información que reciben[28], por lo que para su adecuado funcionamiento y desarrollo resultan claves los datos que se utilicen para el denominado proceso de entrenamiento. En este sentido, el "Machine Learning" es una de las estrategias que puede usar la inteligencia artificial para poder simular la cognición humana. Así, se desarrollan algoritmos que analizan la información datificada, reconocen patrones (relaciones entre los datos) y, a partir de ahí, elaboran predicciones. Esto es precisamente lo que se ha denominado como proceso de "entrenamiento", que puede ser supervisado, no supervisado o por refuerzo[29]. En resumen, la inteligencia artificial parte de un gran

26 Blanco García, A. I.: "El periculum in mora de las medidas cautelares reales. La ¿utilidad? De la Inteligencia Artificial en su detección", en AA.VV.: *Sistemas predictivos en la justicia civil* (ed. por A. I. Blanco García), Tirant lo Blanch, Valencia, 2024, p. 87, afirma que la inteligencia artificial podría resultar útil para valorar y predecir riesgos específicos que la tutela cautelar trata de evitar; puntualizando que precisamente en este punto la inteligencia artificial no solo puede servir para la elaboración de patrones de comportamiento sobre la base casuística anterior, sino también para la identificación y clasificación de riesgos y factores que deben ser analizados por los tribunales.

27 Entre otros, podemos referir: (i) La confrontación con preceptos constitucionales básicos (art. 117 Constitución Española), Gómez Colomer, J. L.: "Unas reflexiones sobre el llamado "juez-robot", al hilo del principio de la independencia judicial", en AA.VV. *Justicia algorítmica y neuroderecho, Una mirada multidisciplinar* (ed. por S. Barona Vilar), Tirant lo Blanch, Valencia, 2021, pp. 243-263; (ii) el incumplimiento de principios procesales esenciales y la vulneración de los derechos dentro del proceso, Montesinos García, A.: "Afectación de", cit., pp. 703-714, (iii) el vínculo al precedente, Battelli, E.: "La decisión robótica, algoritmos, interpretación y justicia predictiva", *Revista de Derecho Privado*, 2020, núm. 38, p. 62, (iv) el estancamiento de la jurisprudencia, Montesinos García, A.: "Empleo de la inteligencia artificial en algunas fases del proceso judicial civil: prueba, medidas cautelares y sentencia", *Actualidad civil*, 2022, núm. 11, p. 8; Bueno De Mata, F.: "Macrodatos, Inteligencia Artificial y Proceso: Luces y sombras", *Revista General de Derecho Procesal*, 2020, núm. 51, p. 28, (v) el riesgo de contar con algoritmos sesgados, Borges Blázquez, R.: "La inteligencia artificial en el proceso penal y el ¿regreso? de Lombroso", en AA.VV.: *Justicia algorítmica y neuroderecho, Una mirada multidisciplinar* (ed. por S. Barona Vilar), Tirant lo Blanch, Valencia, 2021, p. 180. También, en ese sentido, Soriano Arnanz, A. y Simó Soler, E.: "Machine learning y Derecho: aprendiendo la (des)igualdad", en AA.VV.: *Justicia algorítmica y neuroderecho, Una mirada multidisciplinar* (ed. por S. Barona Vilar), Tirant lo Blanch, Valencia, 2021, pp. 194-197, (vi) la atribución de responsabilidades civiles a la máquina, Grimm, P. W.; Grossman, M. R. y Cormack, G V.: "Artificial intelligence as evidence", *Northwestern Journal of Technology and Intellectual Property*, 2021, vol. 19, núm. 1, pp. 65-71, etc.

28 Simó Soler, E. y Rosso, P.: "La destrucción algorítmica de la humanidad", *Diario La Ley*, 2022, núm. 9982, p. 2.

29 Simó Soler, E. y Rosso, P.: "La destrucción", cit., p. 2, explican los tres tipos de procesos de aprendizaje: supervisado, no supervisado y aprendizaje por refuerzo: "En el aprendizaje supervisado los algoritmos necesitan ayuda externa para realizar las tareas de predicción o clasificación. Se proporciona un conjunto de datos de entrada y de salida etiquetados para que un modelo puede aprender algún tipo de patrón que permita predecir o clasificar la variable de salida correctamente. En el caso del aprendizaje no supervisado, a diferencia del anterior, no hay etiquetado. Se proporciona un conjunto de datos de entrada sin clasificar y se le pide a la máquina que busque patrones subyacentes y prediga el resultado. Cuando se introducen nuevos datos, se emplean las características aprendidas previamente para reconocer la clase de los datos. Se utiliza principalmente para la agrupación y la reducción de características. Por último, en el aprendizaje por refuerzo, los algoritmos aprenden a reaccionar a un entorno por sí mismos, a través de un proceso de recompensa acumulada en casos de éxito. Se busca un equilibrio entre la explotación (la maximización de la recompensa) y la exploración (la búsqueda de mejores resultados). Este tipo de aprendizaje se encuentra en el ámbito de la robótica y la industria de los videojuegos". También, en este sentido, Mahesh, B.: "Machine Learning Algorithms-A Review", *International Journal of Science and Research*, 2020, núm. 9, pp. 381-383, y Ullah, Z.;

volumen de datos para, a través de sus redes neuronales, por sí misma encontrar relaciones entre los datos, identificar patrones y tomar decisiones.

En este punto reside precisamente una de las limitaciones técnicas de estos sistemas algorítmicos, pues los algoritmos recopilan una enorme cantidad de datos que contrastan entre ellos, pero siempre mirando al pasado, a los datos que tienen registrados[30]. Esto impide que puedan ofrecerse soluciones creativas que permiten avanzar respecto de lo que ya existe y que sí pueden ser ideadas por personas[31]. Además, encuentran otras limitaciones como es que por medio de estas herramientas de inteligencia artificial se pudieran introducir hechos no alegados por las partes, lo que vulneraría el principio dispositivo y de aportación de parte, y el riesgo que pudiera suponer que estos sistemas utilizaran datos obtenidos con vulneración del derecho a la intimidad y protección de datos[32].

Partiendo de lo anterior, los algoritmos podrían resultar muy provechosos en el ámbito probatorio tanto para las partes como para los tribunales. A continuación, se refieren algunos ejemplos, aunque podrían desarrollarse otros[33].

Por lo que se refiere a las partes, podrían auxiliarles en la elección de los medios de prueba que más convienen a sus pretensiones o estrategia procesal[34]. Asimismo, los algoritmos podrían, analizando casos previos y la prueba con que cuenta una de las partes, por ejemplo, el demandante, informarle sobre la

Al-turjman, F.; Mostarda, L. y Gagliardi, R.: "Applications of artificial intelligence and machine learning in smart cities", *Computer Communications*, 2020, Vol. 154, p. 315.

30 La doctrina ha identificado otras muchas limitaciones técnicas como la falta de pruebas sólidas de validez y confiabilidad de muchos de los algoritmos que se están utilizando; fallos en la monitorización de la fluencia de la función; ausencia de transparencia y explicabilidad, falta de rendición de cuentas, ausencia de resiliencia… Grimm, P. W.; Grossman, M. R. y Cormack, G V.: "Artificial intelligence", cit., pp. 41-78.

31 Nieva Fenoll, J.: "Inteligencia artificial", cit., pp. 425-429. Aunque el Deep Learning y la inteligencia artificial generativa podrían superar esta barrera.

32 Castillo Felipe, R.: "Proceso civil e inteligencia artificial", en AA.VV.: *Proceso civil y nuevas tecnologías* (dir. por J. Sigüenza López), Aranzadi, Cizur Menor, 2021, p. 289.

33 Otra posibilidad que apunta Martín Diz, F.: "Herramientas de inteligencia artificial y adecuación en el ámbito del proceso judicial, en AA.VV.: *Derecho Procesal, Retos y Transformaciones* (dir. por L. M. Bujosa Vadell), Atelier, Barcelona, 2021, p. 296, es que algorítmicamente se pudiera analizar la posible ilicitud de una prueba en relación con su obtención y práctica.

34 En esta línea, téngase en cuenta que los abogados ya están usando la jurimetría para predecir las posibilidades de éxito de una pretensión y auxiliarse en el desarrollo de su trabajo. Planchadell-Gargallo A.: "Inteligencia Artificial y medidas cautelares", en AA.VV.: *Justicia algorítmica y neuroderecho. Una mirada multidisciplinar* (ed. por S. Barona Vilar), Tirant lo Blanch, Valencia, 2021, p. 399, describe la jurimetría como la definición de la estrategia procesal más idónea para el éxito del caso o una propuesta de resolución, basada en el análisis cognitivo de millones de decisiones judiciales. Barona Vilar, S.: *Algoritmización del,* cit., p. 371, enfatiza el carácter asistencial de la jurimetría, que no sustituye la mente humana, sino que ofrece a los abogados información que puede interesarles en el ejercicio de su trabajo. La realidad nos muestra que con una simple búsqueda en internet encontramos ofertas de estas herramientas de analítica, como Jurimetría La Ley, disponible en https://jurimetria.laleynext.es/content/Inicio.aspx (consultado el 2 de febrero de 2024), o Tirant Analitycs, disponible en: https://analytics.tirant.com/analytics/ (consultado el 2 de febrero de 2024).

suficiencia o insuficiencia probatoria respecto de los hechos en que se basa su pretensión, a efectos de que este pueda replantearse su estrategia[35].

Desde la perspectiva del juzgador, la inteligencia artificial podría auxiliar a los jueces en tres aspectos, para lo que seguiremos los postulados de NIEVA FENOLL[36]:

(i) La valoración de la prueba, lo que se estudiará con detalle en el siguiente apartado.

(ii) La elaboración de hipótesis, es decir, pueden desarrollarse herramientas que tras la introducción de los elementos probatorios de un proceso extraigan la hipótesis más plausible de los hechos probados[37]. De esta manera, el juez podría introducir los datos extraídos de las pruebas y el algoritmo elaboraría la o las hipótesis que han podido acontecer. De hecho, existen algunas herramientas que funcionan de esta manera[38]. El problema que presentan, como se ha advertido, es que, pese a basarse en un volumen inmenso de casos, el algoritmo se basaría siempre en experiencias pasadas, las cuales además pudieron no ser juzgadas adecuadamente en el pasado, lo que supondría arrastrar esos errores, perjudicando el enjuiciamiento de casos actuales[39].

(iii) La concreción con menor subjetividad de los llamados "estándares probatorios", que, indica Nieva Fenoll, es consecuencia del descrito segundo campo, la elaboración de hipótesis. El establecimiento de estos estándares probatorios en principio genera seguridad, aunque son en esencia intuitivos y se desprenden de las elaboraciones de hipótesis referidas anteriormente, por lo que arrastran sus errores y no pueden ser calificados de infalibles[40]. No obstante,

35 Sanchis Crespo, C.: "Inteligencia artificial y decisiones judiciales: crónica de una transformación anunciada", *Scire*, 2023, vol. 29, núm. 2, p. 76.

36 Nieva Fenoll, J.: "Inteligencia artificial", cit., pp. 419-420.

37 Sanchis Crespo, C.: "Inteligencia artificial", cit., p. 76. También, Ariza Colmenarejo, M. J.: "Impugnación de las decisiones judiciales dictadas con auxilio de inteligencia artificial", en AA.VV.: *Inteligencia artificial legal y administración de justicia* (dir. por S. Calaza López y M. Llorente Sánchez-Arjona), Thomson Reuters Aranzadi, Cizur Menor, 2022, p. 39, afirma que el empleo de la inteligencia artificial en la actividad probatoria facilitaría la labor de razonamiento del probatorio del juez, con el fin de declarar la existencia de los hechos probados.

38 Ya existen en la actualidad algunas herramientas que trabajan de esta manera, Nieva Fenoll, J.: *Inteligencia artificial*, cit., pp. 26-27, cita las siguientes: (i) "Stevie", un programa que construye historias coherentes partiendo de los datos existentes; (ii) "Echo y Peirce-IGTT", una aplicación que realiza hipótesis y estrategias de acusación y defensa, o (iii) "Alibi", que ante un determinado delito hace un pronóstico de las diferentes explicaciones que pueda tener el comportamiento del reo, a los efectos de comprobar esas explicaciones, incluso aunque el reo decidiera no ofrecerlas.

39 Nieva Fenoll, J.: "Inteligencia artificial", cit., p. 428.

40 Explica Nieva Fenoll, J.: "Inteligencia artificial", cit., p. 428, que: "En su versión a mi juicio más depurada, parten precisamente de la elaboración de hipótesis propia de la probabilidad inductiva, arrojando conclusiones más o menos seguras en función de si las hipótesis alternativas a la que va alcanzando mayor sustento probatorio, se van descartando, logrando así por fin un grado de confirmación que pretende otorgar más seguridad al juez que toma la decisión".

afirma este mismo autor que "la mayor utilidad de los estándares (es) la de servir de pauta probatoria a los jueces, la inteligencia artificial sería útil para conseguir guiar aún mejor el uso de esa pauta, ampliando incluso su rango de observación al ser más probable que elabore bastantes más hipótesis que las que se le puedan ocurrir a un juez tomando como única ayuda su imaginación y la de las partes"[41].

En este sentido, puede resultar ventajoso que un algoritmo (presuntamente objetivo[42]) y no un juez (marcado por la subjetividad humana) sea quien determine la veracidad de los datos aportados al proceso y pueda precisar qué datos requieren de prueba. Al respecto, algunos autores, advierten que podrían reconfigurarse las reglas sobre el objeto y necesidad de prueba, como es el caso de la prueba de derecho extranjero, que bien podría ser sustituida por un algoritmo que ofreciera al juez estos datos, sin necesidad de prueba de parte[43].

Todo lo anterior, en palabras de NIEVA FENOLL nos permitiría "escapar definitivamente de la intuición y de la pura filosofía, acercándose mucho más al empirismo, disponiendo la aplicación del derecho en función de la "voluntas legislatoris" tras una determinación de los hechos que sea correcta desde el punto de vista empírico, [...]"[44].

III. VALORACIÓN DE LA PRUEBA PERICIAL POR ALGORITMOS.

Afirma ORTELLS RAMOS que por valoración de la prueba "se entiende la operación intelectual que realiza el juzgador para determinar la eficacia de los medios de prueba en orden a, según el sistema de valoración que el ordenamiento establezca, originar convicción en el juzgador o permitirle fijar formalmente el hecho como establecido a los efectos de la resolución sobre el objeto del proceso"[45].

Nuestra LEC ha optado por un sistema mixto de valoración. En unos casos se inclina por la valoración legal de la prueba, lo que implica que es la ley la que proporciona la valoración si se acredita el hecho recogido en la norma. Esta forma de valoración se aplica a casos expresamente previstos en la norma, como los documentos públicos (art. 317.1°-6° LEC), entre otros. En el resto de supuestos no referidos expresamente en la ley, opta por la valoración libre de la prueba, que

41 NIEVA FENOLL, J.: "Inteligencia artificial", cit., p. 429.

42 Sin obviar los sesgos que pueden contener estos algoritmos y que debieran ser mitigados por los procesos de supervisión correspondientes, como las evaluaciones de impacto. SANCHIS CRESPO, C.: "Inteligencia artificial", cit., pp. 76-77.

43 CASTILLO FELIPE, R.: "Proceso civil", cit., pp. 286-287.

44 NIEVA FENOLL, J.: "Inteligencia artificial", cit., p. 426.

45 ORTELLS RAMOS, M.: «Capítulo 14», en AA.VV.: *Derecho Procesal Civil* (dir. por M. ORTELLS RAMOS), Aranzadi Thomson Reuters, Cizur Menor, 2022, p. 252-253.

implica que el juzgador realiza esta operación intelectual basándose en las reglas de la sana crítica, por lo que debe fundamentarse en criterios de razonamiento común derivados de máximas de experiencia o de reglas científicas y técnicas (sobre psicología, física, biología, etc). Asimismo, la LEC exige que la valoración de cada medio de prueba se encuentre motivada, por lo que deben expresarse los razonamientos fácticos y jurídicos que conducen a la apreciación y valoración de las pruebas.

Montesinos García estudia la cuestión y entiende que los supuestos de valoración legal podrán ser fácilmente realizados por un programa de inteligencia artificial, ya que consiste en constatar que efectivamente se cumplen los presupuestos previstos en la ley para que se produzca la fijación de los hechos[46]. Sin embargo, esta misma autora advierte que la valoración de las pruebas de manera libre no cuenta con estándares que orienten al juez, lo que puede dificultar la objetivización en un lenguaje algorítmico de los criterios que orientan al juzgador para valorar las pruebas[47]. Además, para valorar un dictamen pericial que es escrito, el algoritmo debiera conocer el lenguaje natural, pero también el técnico empleado por el perito, lo que requeriría de un adecuado etiquetado de los términos científicos, para su traducción al lenguaje numérico, esto es, un desarrollo técnico de cierta complejidad.

Por su parte, Bonet Navarro vislumbra el futuro uso de esta valoración libre por medio de algoritmos con mayor nitidez, pues entiende que en realidad se produciría "la sustitución de la convicción y la subjetividad (del juez) por un porcentaje numérico, el que se estime suficiente y adecuado para considerar fijado el hecho y que ya lleva implícita la coherencia en el contexto'[48]. Lo que no resta que alcanzar una herramienta de auxilio en la valoración de la prueba para el juez que presente determinadas garantías requiera de un proceso de desarrollo muy complejo.

Otra cuestión relevante a tener en cuenta sería la concreta regulación y articulación procesal que debiera darse al uso de estos algoritmos[49]. Así, podría ser conveniente que al menos en un primer momento la introducción de estos instrumentos fuera progresiva, de manera que se previera su utilización sólo en determinados aspectos procesales menos relevantes, como podría ser el de valorar la capacidad de un perito frente al resto de peritos intervinientes en el

46 También, Nieva Fenoll, J.: *Inteligencia artificial*, cit., p. 79.

47 Montesinos García, A.: "Empleo de", cit., pp. 2-3.

48 Bonet Navarro, J.: "Valoración de la prueba y resolución mediante inteligencia artificial", en AA.VV.: *Derecho Procesal: retos y trasformaciones* (dir. por L. Bujosa Vadell), Atelier, Barcelona, 2021, p. 324.

49 Montesinos García, A.: "Reflexiones sobre", cit., p. 49, apunta que: "resulta necesaria una regulación que prevea cuándo, cómo, y bajo qué condiciones pueden utilizarse los modelos algorítmicos en un proceso civil".

proceso. Ello permitiría ponderar en la realidad sus resultados y efectividad y valorar su ampliación a otras cuestiones.

Igualmente, debiera regularse si, una vez desarrollados estos sistemas computacionales con las debidas garantías, podrían utilizarse como herramientas judiciales disponibles para todos los justiciables, de modo que las partes pudieran solicitar su aplicación o el juez pudiera emplearlas de oficio[50]. No obstante, su uso de oficio por el juez podría contravenir los principios dispositivos y de aportación de parte que rigen en el proceso civil. Cosa distinta sería que la norma regulase su uso en todo caso por el juez, de manera que el juez siempre contara con el auxilio del algoritmo, aunque después pudiera apartarse de su resultado.

Asimismo, teniendo en cuenta la regulación actual, en el caso de aplicarse estas herramientas computacionales, las partes deberían tener la posibilidad de conocer el funcionamiento de estos algoritmos, es decir, se tendría que garantizar la transparencia e incluso se debería prever la posibilidad de que las partes cuestionaran el propio algoritmo (su configuración, su proceso de entrenamiento, la existencia de sesgos…), por ejemplo, a través de una pericial informática[51]. Además, si los sistemas algorítmicos se emplearan de oficio o en todo caso por el juez, el resultado arrojado por estos no debería conocerse directamente en la sentencia, lo que perjudicaría el derecho de defensa de las partes, por lo que sería necesario articular trámites de alegaciones posteriores a su aplicación.

Partiendo de lo anterior, estos algoritmos podrían asistir al juez en múltiples aspectos de la valoración de la prueba pericial. A continuación, se exponen de forma separada, advirtiéndose que aún podrían desarrollarse otras aplicaciones.

1. Valoración de la cualificación y experiencia del perito.

La cualificación y especialización del perito deben ser adecuadas para el objeto de la pericia, lo que dotará de mayor credibilidad a la prueba[52]. Su valoración

50 Al respecto, Montesinos García, A.: "Empleo de", cit., p. 4, manifiesta que: "Las partes podrían proponerlas como instrumentos de ayuda a la valoración del juez de determinados medios de prueba, como complemento a las pruebas propuestas, o incluso podrían ser acordadas por el juez cuando considere que las pruebas propuestas por las partes resultan insuficientes (art. 429.1 LEC). Convendría, en todo caso, que esta posibilidad se contemplara en la ley".

51 De Hoyos Sancho, M.: "El libro", cit., pp. 23-14: "si no fuera posible acceder y conocer el "código fuente" del algoritmo que gobierna el sistema IA, generalmente protegido por el derecho de propiedad intelectual y creado para fines ajenos al enjuiciamiento penal, sería casi imposible cuestionar o impugnar los resultados/datos que proporciona el sistema y que se podrían utilizar como prueba en una causa penal. […] En definitiva, si no hay suficiente transparencia –acceso al código fuente, inputs y outputs del software- no podrá asegurarse la necesaria y suficiente paridad de armas entre acusación y defensa, el justo equilibrio procesal entre ambas posiciones. Incluso suponiendo que se tuviera acceso a tal información, sería preciso además que las partes pudieran disponer de peritos en la materia que certificaran –o no- la fiabilidad del sistema IA y de sus resultados en ese concreto supuesto".

52 Pellicer Ortiz, B.: "¿Cuándo un juez deja de creer en un dictamen pericial?", en AA.VV.: *La prueba pericial a examen. Propuestas de lege ferenda* (dir. por J. Picó i Junoy), Bosch, Barcelona, 2020, p. 130.

puede partir del curriculum del perito, analizando su formación, pero también su experiencia profesional y académica en el campo objeto de peritaje[53]. Así, un perito puede tener una formación universitaria superior, por ejemplo, ser ingeniero superior industrial, pero no haberse dedicado al campo técnico concreto al que se refiere su dictamen pericial. De manera que, si la parte contraria presentara un informe elaborado por un ingeniero técnico, pero que ha trabajado durante un largo periodo temporal en el ámbito técnico objeto de informe, su capacidad técnica para emitir dictamen podría considerarse superior a la del primero. Una herramienta algorítmica podría ponderar estas cuestiones para realizar una valoración acertada.

2. Valoración del contenido del informe pericial.

El contenido del informe deviene fundamental y debe ser objeto de valoración por el juzgador. Por un lado, debe contar con algunos aspectos formales básicos, como son la identificación del perito y de la parte que le contrata, manifestación de no hallarse incurso en causa de tacha legal, juramento o promesa de decir verdad, conclusiones alcanzadas y fecha del informe[54]. El algoritmo podría detectar fácilmente la efectiva inclusión de estos aspectos formales esenciales y también extraer algunas conclusiones al respecto, por ejemplo, cuando la fecha de emisión del informe se encuentre especialmente alejada de los hechos controvertidos y pueda haber acontecido una alteración del objeto de la pericial por la concurrencia de determinadas circunstancias, o en algunos casos por el mero transcurso temporal. Este sería el caso de una pericial médica cuando el paciente ya se encuentra recuperado de la dolencia, por lo que pueden estudiarse los informes médicos previos pero el reconocimiento médico puede tener en ese momento escaso valor.

Otra cuestión fundamental son las fuentes que ha tenido en consideración el perito para realizar su informe y que un sistema algorítmico podría analizar. Así, no es lo mismo que el perito solo haya tenido acceso a la documentación que le ha facilitado el abogado que le ha realizado el encargo o que, también, haya podido tener en cuenta los escritos de las partes, el informe de la otra parte, etc. Además, tampoco tiene el mismo valor que el perito haya podido examinar personalmente la cosa, objeto o lugar que son objeto de la pericial[55], verbigracia, visitando un

53 Advierte la doctrina que los algoritmos podrían detectar plagios en las publicaciones o trabajos que aleguen los peritos para acreditar su experiencia o descubrir méritos aparentes, incluso identificar la creatividad y originalidad de estas. Montesinos García, A.: "Empleo de", cit., p. 3; Simón Castellano, P.: "Inteligencia artificial y valoración de la prueba: las garantías jurídico-constitucionales del órgano de control", *THĒMIS-Revista de Derecho*, 2021, núm. 79, pp. 289-290. También, en relación con la valoración del currículo del perito, Nieva Fenoll, J.: *Inteligencia artificial*, cit., pp. 94-95.

54 Izquierdo Blanco, P.: "¿Qué espera", cit., pp. 220-222.

55 Pellicer Ortiz, B.: "¿Cuándo un", cit., p. 210.

edificio para comprobar los vicios de la construcción, que que solo haya tenido acceso a fotografías del edificio proporcionadas por la parte[56].

También, resulta esencial el método científico empleado para alcanzar sus conclusiones, así como el cumplimiento de los estándares técnicos[57]. Respecto de la valoración de la prueba pericial, conviene traer a colación los criterios de "Daubert", que fueron establecidos por el Tribunal Supremo de los Estados Unidos de América[58] para determinar si una prueba podía ser considerada como científica y que posteriormente fueron recogidos en parte en el art. 702 de las "Federal Rules of Evidence"[59]. Así, explica Nieva Fenoll, que pese a haber sido concebidos estos criterios para la admisión de la prueba, también se pueden utilizar para su valoración[60]. El algoritmo podría realizar una función similar, analizando los criterios que le permitan valorar si concurren o no estos parámetros mínimos.

Además, las herramientas algorítmicas pueden detectar contradicciones o inconsistencias dentro del propio dictamen. Incluso estos sistemas podrían detectar los argumentos contrarios entre los diferentes dictámenes aportados a un proceso. En esta línea, podrían considerar otras cuestiones como que el perito haga referencia a aspectos que exceden del objeto del informe o que aporte multitud de anexos que tienen una relación tangencial con la pericial requerida, lo que en muchas ocasiones solo genera (deliberadamente) confusión respecto de las cuestiones a las que debe dar respuesta que no se le han pedido.

Por último, estos algoritmos también podrían analizar las conclusiones alcanzadas por el perito, su rotundidad, claridad y precisión, así como la fundamentación de cada uno de ellas.

3. Valoración de la imparcialidad y objetividad de un perito.

56 Al respecto, Pellicer Ortiz, B.: "¿Cuándo un?", cit., p. 211, afirma que: "Por el contrario, una debida inspección por parte del perito de aquello que es objeto de la pericia, con una rápida personación en el lugar objeto de examen, o tomando las muestras que sean precisas o con seguimiento de la evolución de las lesiones de la víctima de un accidente de tráfico, dotarán al informe pericial de una mayor robustez".

57 Katz, P.: "Expert robot", cit., pp. 38-39, explica que: "The Expert Robot will be able to evaluate the expert testimony under its rules and compare it with vast stores of existing literatura and studies to determine whether the expetiment´s design has been subject to review within the relevant scientific community".

58 Estas sentencias fueron: (i) Daubert v. Merrell Dow Pharmaceuticals, 509 U.S. 579 (1993), (ii) General Electric Co. v. Joiner, 522 U.S. 136 (1997), y (iii) Kumho Tire Co. v. Carmichael, 526 U.S. 137 (1999).

59 Vázquez Rojas, C.: *De la prueba científica a la prueba pericial*, Marcial Pons, Madrid, 2015, pp. 137-148. Nieva Fenoll, J.: "Repensando Daubert: la paradoja de la prueba pericial", en AA.VV.: *Peritaje y prueba pericial* (dir. por J. Picó i Junoy), Atelier, Barcelona, 2017, p. 90.

60 Según concreta Nieva Fenoll, J.: "Un cambio generacional en el proceso judicial: La inteligencia artificial", en AA.VV.: *Derecho Procesal: retos y transformaciones* (dir. por L. M. Bujosa Vadell), Atelier, Barcelona, 2021, pp. 288-289, se trata de los siguientes criterios: "1. Que la técnica haya sido elaborada siguiendo el método científico, en el sentido de que haya sido verificada empíricamente con intentos de falsificación y refutación. 2. Que la técnica empleada haya sido objeto de revisión por parte de otros expertos y haya sido publicada. 3. Indicación del grado de error de la técnica. 4. Existencia del mantenimiento de estándares y controles sobre la fiabilidad de la técnica. 5. Consenso en la comunidad científica sobre la técnica empleada (estándar Frye)".

La imparcialidad y objetividad de un perito resultan esenciales. Por un lado, la LEC establece la posibilidad de recusar a los peritos a fin de evitar que un perito nombrado por designación judicial emita un dictamen (arts. 124 a 128, y 343.1 LEC). En este caso, las causas son (i) haber dictado con anterioridad sobre el mismo asunto dictamen contrario a la parte recusante, ya sea dentro o fuera del proceso, (ii) haber prestado servicios como tal perito al litigante contrario o ser dependiente o socio del mismo, y (iii) tener participación en sociedad, establecimiento o empresa que sea parte del proceso. Por otro lado, se prevé la posibilidad de tachar a los peritos de parte, de forma que el juez pueda tener en cuenta que concurren causas que ponen en duda su imparcialidad (condición de cónyuge o pariente por consanguinidad o afinidad, contar con interés directo o indirecto en el asunto, etc.), a tenor del art. 343 LEC.

Así, un sistema algorítmico podría valorar las causas previstas en el art. 125 LEC para la recusación del perito y que el juez se viera auxiliado para decidir sobre este incidente de recusación. Lo mismo podría ocurrir respecto de las circunstancias que pueden alegarse como tacha y la prueba que se aporte para su justificación a efectos de valorar su imparcialidad. Además, se debieran tener en consideración las alegaciones realizadas por las partes a fin de negar o contradecir la tacha, así como la documentación acreditativa de estas. Esta valoración de la tacha podría bien hacerse de forma independiente, para asistir al juez a valorar si concurren o no las circunstancias que perjudican su imparcialidad, realizándose la valoración de la pericial de forma "clásica" por el juez, o bien integrarse dentro de un algoritmo de valoración del dictamen pericial en su conjunto.

En otro orden de cosas, pese a que no concurran las causas previstas para la recusación y la tacha del perito, en algunos casos podemos hablar de la existencia de un cierto clientelismo entre el perito designado por las partes y quien le contrata. De hecho, en la práctica, lo normal es que el letrado adelante al perito la conclusión esperable de su dictamen[61], es decir, que el encargo se realice con indicación previa del resultado que se espera. En estos casos, el perito lo que hace es buscar la forma de dar explicación de forma técnica a la hipótesis que le solicitan, lo que le impide realizar su trabajo sin la "contaminación previa" que debiera concurrir. La dificultad se encuentra en acreditar que ha concurrido esta forma torcidera de trabajo (lo que, sin embargo, es bastante frecuente en la práctica)[62]. Al contrario, genera credibilidad que el perito de parte reconozca la veracidad de determinadas alegaciones de la parte contraria o del informe de

61 Izquierdo Blanco, P.: "¿Qué espera", cit., p. 130.

62 En este sentido, también, Nieva Fenoll, J.: "Repensando Daubert", cit., p. 95: "Ningún dictamen de parte es presentado sin antes haber sido revisado y adaptado profundamente por el abogado. De hecho, si el perito se niega a hacer el dictamen que le pide el abogado, el experto es sustituido por otro profesional que sí se adapte a esos intereses".

la otra parte (art 335.2 LEC)[63]. Estas cuestiones también podrían ser tenidas en cuenta por un algoritmo a efectos de determinar la objetividad del perito, por ejemplo, valorando como más fiable el informe que no niegue de forma sistemática (e incluso infundada) todo lo expresado de contrario.

4. Valoración de la comparecencia del perito en el juicio o la vista.

El perito podrá comparecer en el juicio o vista a instancia de parte o de oficio, a los efectos de exponer o explicar su informe, contestar a las preguntas de las partes, objeciones o propuestas de rectificación que se le hagan, responder a cuestiones ampliatorias que se le puedan formular, criticar otros dictámenes periciales, etc. En definitiva, realizar cualquier intervención que pueda resultar de utilidad para entender y valorar el dictamen en relación con lo que sea objeto del pleito.

También, puede acordarse el denominado "careo de peritos", que consiste en la declaración conjunta de los peritos designados en un proceso, con su presencia simultánea en la sala de vistas.

La forma en la que se realiza la declaración, también, es valorada por el juzgador y podría verse auxiliada por algoritmos. Por ejemplo, el dominio de la oralidad, las expresiones faciales y demás lenguaje no verbal, los silencios, la emisión de respuestas dubitativas, poco precisas o incluso deliberadamente complejas desde el punto de vista técnico a efectos de evadir una determinada respuesta, restarán crédito a la declaración del perito. Estas cuestiones podrían ser analizadas de forma algorítmica para extraer conclusiones al respecto. No obstante, en la práctica, esto se podría traducir en la sustitución del subjetivismo del juez por el de la máquina.

Así, fundamentalmente para el análisis de la prueba testifical se ha estudiado ya la aplicación de la neurociencia, que ofrece mecanismos capaces de mesurar la veracidad de las declaraciones, por ejemplo, mediante imágenes de resonancia magnética –fMRI–. No obstante, su aplicación ha sido cuestionada por la doctrina, pues existen problemas que ponen en duda su fiabilidad[64] y la afectación de derechos fundamentales. Asimismo, para el análisis de las declaraciones se han desarrollado algoritmos de micro-expresiones faciales que analizan cómo determinadas zonas de la cara permiten saber cuándo una persona dice la verdad o está mintiendo[65]. De hecho, en España se ha admitido en algunos casos como

63 Pellicer Ortiz, B.: "¿Cuándo un?", cit., p. 212.

64 Picó i Junoy, J.: "La prueba del dolor", en AA.VV.: *Neurociencia y proceso judicial* (dir. por M. Taruffo y J. Nieva Fenoll), Marcial Pons, Madrid, 2013, pp. 91-92. Picó i Junoy, J.: "Retos del", cit., pp. 447-451.

65 Matsumoto, D. y Hwang, H. C.: "Microexpressions differentiate truths from lies about future malicious intent", *Frontiers in Psychology*, 2018, núm. 9, pp. 1-11, realizan un estudio empírico en la materia del que se desprende su utilidad en algunos supuestos, pero también algunas de sus limitaciones.

prueba un informe elaborado por esta técnica y en otros se ha rechazado de pleno[66]. Además, existen estudios que desacreditan estos "métodos de detección de la mentira"[67].

En todo caso, entendemos que estas herramientas, si llegaran a desarrollarse con las suficientes garantías, podrían tener un mayor recorrido y aplicación para la valoración de las testificales y las declaraciones de parte, pues es menos común que un perito falte a la verdad de forma consciente y deliberada. No obstante, podría resultar de utilidad cuando exista la relación de clientelismo antes apuntada, el perito esté intentando ocultar la existencia de una causa de tacha o este se pudiera ver "acorralado" en un careo entre peritos y pudiera llegar a mentir para mantener su postura. En estos casos estos sistemas sí podrían llegar a resultar de utilidad.

5. A modo de conclusión.

De esta valoración de la prueba pericial se podrán extraer conclusiones esenciales para la resolución de los asuntos. Así, el algoritmo debiera poder mostrar cuáles son los motivos que le llevan a un determinado resultado para que sea, en todo caso, el juez el que tome la decisión de acoger las conclusiones de un informe en concreto, pudiendo justificarlo debidamente en la sentencia.

Además, por medio de estos sistemas algorítmicos se podrían valorar los diferentes dictámenes aportados a un proceso para determinar cuál alcanza un resultado más fiable[68]. En estos casos, la valoración de los diferentes dictámenes

66 En concreto, la STS (Sala 2ª) 6 de marzo 2019 (RJ 2019, 868), parece que sí da credibilidad a un informe pericial admitido en primera instancia de Micro-expresiones faciales y lenguaje corporal inconsciente, basándose en que las partes no se oponen al mismo y la existencia de avales de distintos organismos oficiales y universitarios que reconocen dicha prueba de utilidad tanto en procedimientos civiles como penales. Sin embargo, otras sentencias se pronuncian de forma contraria, como la SAP de Barcelona (Sección 18ª) 18 diciembre 2020 (JUR 2021, 28295), que remite a la SAP de Barcelona (Sección 18ª) 8 de mayo 2019 (JUR 2019, 159229), en la que se afirma que: "no se ha aportado publicación científica que avale y contraste la técnica utilizada. […] No podemos considerar dicha técnica como válida para verificar la credibilidad de las manifestaciones vertidas por la menor. […] Es decir, se parte de una hipótesis a partir de la cual se diseña un interrogatorio dirigido a una persona sin tener en consideración otras variables como estado madurativo, formación, contexto social, etc. y sin tener en cuenta otras expresiones no verbales, con el riesgo de obtener respuestas sesgadas e interpretando determinados gestos a los que se vincula, sin margen de error, una emoción. La utilización de dicha metodología no está suficientemente contrastada, se desconoce la concreta formación de las personas que la han llevado a cabo y la forma en como ha sido aplicada a la menor se considera por la Sala totalmente inadecuada". También, en contra SAP de Barcelona (Sección 12ª) 17 enero 2020 (JUR 2020, 48385). Por otro lado, su uso podría tener mejor encaje en los ADR, como el arbitraje. Así lo apunta Marcos Francisco, D.: "Smart ODR y su puesta en práctica: el salto a la inteligencia artificial", *Revista General de Derecho Procesal*, 2023, núm. 59, p. 21, requiriendo para su uso que exista consentimiento expreso de las partes y de la persona implicada (por ejemplo, el testigo cuya declaración va a analizarse algorítmicamente).

67 Denault, V., et altri: "The analysis of nonverbal communication: The dangers of pseudoscience in security and justice contexts", *Anuario de Psicología Jurídica*, 2020, núm. 30, pp. 1-12.

68 Ariza Colmenarejo, M. J.: "Impugnación de las decisiones", p. 47, pone como ejemplo de aplicación de la inteligencia artificial, la posibilidad de alcanzar una fórmula para establecer el mayor peso probatorio entre varios dictámenes periciales.

vendrá respaldada por porcentajes, de modo que a uno de ellos se le atribuya mayor fiabilidad que a los demás[69].

En esta línea, la implantación de algoritmos viene a objetivar la valoración de la prueba pericial en detrimento de la subjetividad que concurre por naturaleza en un juez. Lo que se traduce en palabras de Nieva Fenoll en la objetivización de "la intuición o percepción humana, incluso perfeccionándola"[70]. Lo que requiere del avanzado y garantista desarrollo de estos sistemas, para evitar que la subjetividad humana se sustituya por la algorítmica.

En todo caso, en nuestra opinión, estos mecanismos debieran estar especializados, según el objeto de la pericial a desarrollar[71] y tener siempre una función auxiliadora del juez, debiendo ser el juzgador el que tome la decisión última de la valoración y exprese los motivos que le llevan a ella. Al igual que un juez puede apartarse de la opinión técnica de un perito[72], también debiera poder hacerlo de la valoración que hace el algoritmo de la prueba. Lo que requeriría, además, del establecimiento de trámites para que los resultados del algoritmo puedan ser cuestionados por las partes. En esta línea, Nieva Fenoll propone que: "En concreto, la herramienta podría ser diseñada, no como una especie de robot de funcionamiento automático, sino como una pauta de alertas para que el juez vaya introduciendo sus valoraciones al respecto, de manera que el resultado final no sea una especie de pronóstico de credibilidad, sino simplemente el resultado de un trabajo del juez guiado por la herramienta, que podría asistirle también en la motivación"[73].

El riesgo que puede suponer la generalización de la implantación de estos mecanismos algorítmicos de auxilio es que los jueces tomen directamente la conclusión que les arroja el algoritmo y para evitar tener que realizar una motivación suficiente que contraríe sus postulados caigan en el automatismo de dejar que sea la máquina la que tome la decisión y elija cuál es la solución técnica

69 Igualmente, podrían desarrollarse herramientas que evalúen cada uno de los medios de prueba aportados a los efectos de otorgar mayor credibilidad a algunos de ellos. Bonet Navarro, J.: "Valoración de", cit., p. 330.

70 Nieva Fenoll, J.: *Inteligencia artificial*, cit., p. 84.

71 Afirma Vázquez Rojas, C.: *De la prueba*, cit., p. 284-285, que: "La heterogeneidad de las muy diversas pruebas periciales desborda cualquier intento de unificación en un criterio para valorar su calidad", es decir, para poder valorar las pruebas correctamente necesitamos que el algoritmo se encuentre especializado en ese campo técnico. Difícilmente podremos desarrollar un sistema computacional que sirva para todos los casos, pues las especificidades de cada ámbito son muchas. En esta línea, pero en términos generales, se pronuncian Grimm, P. W.; Grossman, M. R. y Cormack, G V.: "Artificial intelligence", cit., p. 97, afirmando que: "The problem that the AI was developed to resolve-and the output it produces-must "fit" with what is at issue in the litigation".

72 Pellicer Ortiz, B.: "¿Cuándo un?", cit., p. 215, afirma que: "aunque el juez no viene obligado a someterse al dictamen pericial, no puede sustituir el criterio técnico del perito por su propio criterio subjetivo y viene obligado a explicar suficientemente y motivadamente las razones que le llevan a apartarse de las conclusiones de la pericia".

73 Nieva Fenoll, J.: "Inteligencia artificial", cit., p. 427.

más adecuada, esto es, decida a qué dictamen pericial acogerse[74]. Lo anterior, como ha advertido la doctrina, supondría la vuelta a un sistema de valoración legal de la prueba[75], desvirtuando la función asistencial de la que no debieran apartarse. Por tanto, como advierte MARTÍN DIZ, la utilización de estos mecanismos de inteligencia artificial en materia probatoria debe realizarse desde el pleno respecto a los derechos humanos y a los derechos fundamentales procesales[76].

IV. ELABORACIÓN DE DICTÁMENES PERICIALES POR ALGORITMOS.

El siguiente escenario es aquel en que es el propio algoritmo el que emite el dictamen pericial, pues, si tenemos en cuenta que los sistemas de inteligencia artificial se basan en un conjunto de datos que los nutre, es razonable pensar que pueden tener los mismos o mayores conocimientos que los que poseería un perito humano[77]. Son muchas y de muy diverso tipo las incógnitas que se abren al respecto, por lo que en este apartado apuntaremos algunas de ellas, pese a que pueden plantearse otras.

Partimos de un ejemplo real que se está dando en el sector asegurador, que utiliza herramientas de inteligencia artificial para la valoración de siniestros y la contratación de riesgos, aunque los procesos no están automatizados al cien por cien y las compañías cuentan con expertos que validan su veracidad. Así, se están implementado algoritmos que para el proceso de entrenamiento emplean una gran cantidad de fotografías con variedad de siniestros en vehículos. De esta forma, para la valoración de un caso en concreto, el sistema analiza las fotografías del vehículo siniestrado, detecta los daños que existen en las piezas y realiza el proceso de cuantificación de los daños con su algoritmo previamente "alimentado" mediante unos parámetros necesarios (tipología, material, acabados, superficie, tiempos…). De hecho, quienes los están aplicando afirman que están obteniendo una alta fiabilidad y confían en su mejora progresiva, precisamente derivada de su uso cada vez mayor que va retroalimentado a sus bases de datos, así como la

74 En esta línea, también, Montesinos García, A.: "Empleo de", cit., p. 4, afirma que: "entendemos que la información que obtenga el juez a través del sistema de IA podrá servirle para formar su convicción, pero en ningún caso tendrá que aceptarla de forma automática, sino que podrá desmarcarse de ella cuando así lo considere. Advertimos con ello del riesgo que supone que el juez se conforme, de manera acrítica, con la decisión proporcionada por la máquina sin contrarrestar ni cuestionarse sus resultados y del peligro de automatismo que ello conlleva".

75 Borrás Andrés, N.: "La verdad y la ficción de la inteligencia artificial en el proceso penal", en AA.VV.: *La justicia digital en España y la Unión Europea: Situación actual y perspectivas de futuro* (dir. por J. Conde Fuentes y G. Serrano Hoyo), Atelier, Barcelona, 2019, p. 36.

76 Martín Diz, F.: "Justicia predictiva: inteligencia artificial y algoritmos aplicados al proceso judicial en materia probatoria", en AA.VV.: *El impacto de las tecnologías disruptivas*, (dir. por F. Bueno De Mata), Aranzadi, Cizur Menor, 2022, p. 148.

77 Bonet Navarro, J.: "Valoración de", cit., p. 330.

asistencia que realizan los peritos que van corrigiendo las desviaciones que van surgiendo[78].

Por tanto, en la práctica encontramos ejemplos en los que estas herramientas algorítmicas se están generalizando, aunque aún tienen un carácter auxiliar, pues sus resultados son supervisados por personas. Sin embargo, esto nos muestra que no es improbable que en el futuro estas compañías aseguradoras utilicen automáticamente los resultados algorítmicos y la labor de los peritos sea residual.

En esta línea, en el futuro podrían desarrollarse algoritmos que elaborasen dictámenes periciales, esto es, la sustitución del perito humano por el "perito-robot". Podemos realizar multitud de precisiones, objeciones y puntualizaciones a la anterior afirmación. De forma preliminar surge una primera cuestión relacionada con la multitud y diversidad de dictámenes periciales que pueden requerirse en los distintos tipos de procesos judiciales civiles, lo que se traduciría en la necesidad de crear algoritmos especializados para dar respuesta a cada caso. Piénsese en lo diferente que puede ser un informe que valore si las cuentas anuales de una sociedad reflejan la imagen fiel del patrimonio, a una pericial que valore si un motor hidráulico cumple con los requisitos técnicos que se establecieron en el contrato.

En este sentido, de entrada parece razonable pensar que cada tipo de informe pericial requerirá de un algoritmo especializado, que haya sido entrenado con unos datos concretos, propios del ámbito técnico en que se debe emitir el informe. Lo que puede complicar su desarrollo, teniendo en cuenta que unos pueden alimentarse con imágenes, otros con texto, otros con varios de ellos, etc. Además de que el tipo de cuestiones que se le pueden plantear al algoritmo pueden ser casi infinitas, si tenemos en cuenta la gran cantidad y diferente naturaleza de los procesos que pueden surgir, como: valorar si existen o no daños estructurales en un puente y cuantificar la posible indemnización, determinar si un médico cumplió con el protocolo médico, calcular la indemnización por clientela por la extinción anticipada del contrato de agencia, valorar los daños morales causados por el uso ilícito de una marca, etc. Esto nos puede llevar a la paradoja de tener que desarrollar infinidad de algoritmos para que sus resultados puedan resultar confiables.

1. Inteligencia artificial generativa para la elaboración de dictámenes.

Como se ha explicado, la inteligencia artificial, a través de sus redes neuronales, puede por sí misma encontrar relaciones entre un gran volumen de datos para identificar patrones y tomar decisiones.

78 Gómez Jiménez, Á.: "Verificación y valoración digital por Inteligencia Artificial (AI)", *CESVI*, 2022, núm. 120, pp. 36-40.

La inteligencia artificial generativa se considera una rama de la inteligencia artificial y hace referencia, según Casar Corredera, al conjunto de "métodos y aplicaciones capaces de generar contenidos (texto, imágenes, software o cualquier otra cosa) con características indistinguibles de las que produciría un ser humano. Para ello, esencialmente, las aplicaciones aprenden las características propias de los contenidos para las que han sido concebidas, a partir de una colección considerable de ejemplos reales, preferentemente de manera no supervisada, y terminan por ser capaces de producir nuevos contenidos con esas propiedades, con las instrucciones de generación que les pueda dar un usuario humano (instrucciones típicamente construidas en lenguaje natural o prompts)"[79].

En esta línea, en estos últimos años se han desarrollado "modelos de lenguaje masivos" (LLM, por sus siglas en inglés: *large language models*), que son modelos que a través de redes neuronales son entrenados para aprender y reproducir el lenguaje, lo que ha resultado en lo que se conoce como "GPT" (i) "G"enerativo, precide la siguiente palabra; ii) "P"re-entrenado, con grandes volúmenes de datos, y iii) "T"ransformador, codificador y decodificador basado en redes neuronales)[80].

El desarrollo de estos modelos puede llevarnos a pensar que es posible que se desarrollen algoritmos que respondan a las cuestiones que se les planteen desde el punto de vista técnico (lo que se traduce en porcentajes numéricos); pero que, además, emitan un informe pericial escrito en el que detallen sus conclusiones y sobre todo relaten la motivación de estas conclusiones[81]. De manera que casi podríamos hablar de la intervención del llamado "perito-robot".

Como apuntábamos al inicio, las dudas que se presentan son muchas y algunas tienen que ver con la técnica. Por un lado, se entiende por explicabilidad e interpretabilidad la necesidad de comprender las decisiones tomadas por los algoritmos de inteligencia artificial, pues cuando se emplean modelos de aprendizaje profundo basados en redes neuronales de varias etapas puede resultar imposible comprender el razonamiento seguido e interpretar la solución alcanzada por el algoritmo[82]. Esta limitación técnica no es en nada desdeñable, si tenemos en cuenta que un sistema de inteligencia artificial generativa podría emitir un informe

79 Casar Corredera, J. R.: "Inteligencia artificial generativa", *Anales de la Real Academia de Doctores de España*, 2023, Volumen 8, núm. 3–2023, p. 476.

80 Sánchez, M. y Carbajal, E.: "La inteligencia artificial generativa y la educación universitaria", *Perfiles Educativos*, 2023, vol. 45, número especial, p. 72.

81 En nuestra opinión, actualmente puede ser complicado técnicamente que los sistemas de inteligencia artificial generativa produzcan informes periciales de cierta calidad técnica, teniendo en cuenta la complejidad del lenguaje técnico, que requeriría del adecuado etiquetado de este lenguaje, entre otras muchas cuestiones.

82 Puntualiza Casar Corredera, J. R.: "Inteligencia artificial", cit., pp. 481-482, que: "Los términos de Explicabilidad e Interpretabilidad suelen usarse indistintamente, aunque el término Interpretabilidad se refiere a la propiedad de entender la relación entre los datos procesados y la solución propuesta, en una perspectiva causa-efecto; y la Explicabilidad a la capacidad de entender el razonamiento efectuado por la máquina para llegar a las conclusiones presentadas o a las acciones propuestas".

pericial, pero podría desconocerse desde el punto de vista técnico cómo se ha llegado a ese resultado.

Por otro lado, es ampliamente conocido que el desarrollo garantista de un sistema de inteligencia artificial requiere de un volumen de datos considerable. En este sentido, aparece lo que se denomina frugabilidad, que hace referencia a la condición de los algoritmos de aprendizaje de no necesitar tantos recursos (datos, energía, tiempo de entrenamiento…) para alcanzar unas prestaciones aceptables. Así, la frugabilidad en datos supone que el algoritmo con pocos datos con los que entrenarse puede, sin embargo, alcanzar resultados fiables[83]. Esta condición podría favorecer el desarrollo de algunos de los algoritmos especializados a los que se hacía referencia, respecto de los que no sea sencillo encontrar grandes cantidades de datos para su alimentación. La cuestión de nuevo es si esto pudiera garantizar la obtención de resultados fiables.

Otra vía que podría ayudar al desarrollo de algoritmos especializados para elaborar los diferentes tipos de algoritmos que hagan las funciones del "perito-robot" es el aprendizaje por transferencia ("Transfer Learning"), que es la posibilidad de valerse, al menos como punto de partida, de un modelo entrenado en una tarea para realizar otra, lo que podría favorecer el uso de determinados algoritmos desarrollados para elaborar un tipo de dictámenes periciales para elaborar otros[84]. Pongamos por caso, un algoritmo que evalúa si un fármaco infringe una patente, que podría ser el punto de partida para analizar si esa patente es nula.

2. Múltiples dudas desde la óptica legal actual.

La posibilidad de que el dictamen pericial emitido por un perito persona física sea sustituido por un informe pericial emitido por un sistema algorítmico con inteligencia artificial generativa o "perito-robot" plantea muchas dudas si lo analizamos desde la actual regulación de la LEC. De hecho, como se verá en las próximas líneas, la aplicación de los preceptos actuales a ese hipotético escenario genera situaciones artificiosas y que en algunos casos se apartan de toda lógica.

Por un lado, el art. 340 LEC permite que el dictamen pericial pueda ser emitido por una persona física o una persona jurídica, sin embargo, en este último caso, exige que la institución a la que se encargue el dictamen exprese a la mayor brevedad qué persona o personas se encargarán directamente de prepararlo, a las que se exigirá el juramento o promesa, ex art. 335.2 LEC. Por tanto, este precepto tendría difícil encaje con la elaboración de un informe pericial por un algoritmo, lo que podría solucionarse reformulando este precepto para dar cabida a este nuevo

83 Casar Corredera, J. R.: "Inteligencia artificial", cit., p. 482.

84 Casar Corredera, J. R.: "Inteligencia artificial", cit., p. 482.

sistema o exigiendo que uno de los desarrolladores o responsables del algoritmo aparezca como autor del dictamen, lo que podría generar muchos problemas, entre otros, relacionados con la atribución de responsabilidades.

Asimismo, difícilmente el algoritmo podría prestar juramento o promesa de actuar con objetividad, lo que como mucho podría exigirse a sus desarrolladores. Lo que ocurre es que, como se ha referido anteriormente en relación con la explicabilidad e interpretabilidad, en los casos de modelos de aprendizaje profundo basados en redes neuronales de varias etapas puede resultar muy complejo o incluso imposible conocer el razonamiento seguido por el sistema, por lo que su desarrollador tampoco podría emitir un juramento íntegro, sino sólo de lo que él alcanza a comprender.

En relación con el contenido del informe, este debiera ser similar al del informe emitido por un perito humano. Así, debería contar con algunos aspectos esenciales, como son la identificación del "perito-robot", es decir, el propio algoritmo, identificando quién es su titular, si es una empresa o una institución, quiénes han sido sus desarrolladores, etc. También, se debiera identificar la parte que le contrata, así como las fuentes que ha tenido en consideración para obtener ese resultado concreto. Siendo de especial importancia las conclusiones alcanzadas, que deben dar respuesta a las preguntas que se les planteen desde el punto de vista técnico, así como los argumentos que les llevan a estas. Igualmente, sería conveniente que se explicara el propio funcionamiento del sistema algorítmico y cuáles han sido los datos con quienes se ha entrenado el algoritmo (referencia a la base de datos, por ejemplo) para que se pudiera valorar si cumplen con los estándares técnicos mínimos.

Además, tendría que poder controlarse que el informe pericial no excede los límites que le son propios. Esto es, no debiera incorporar nuevos hechos o documentos que no constan en el proceso y que debieron aportarse con la demanda o la contestación (art. 265 LEC), no debería hacer referencia a cuestiones que exceden del objeto del informe, etc.

Todo lo anterior nos lleva a preguntarnos si sería posible que cada parte encargara un informe a una empresa desarrolladora de algoritmos y que en el proceso se aportaran informes elaborados con inteligencia artificial generativa que llegaran a resultados opuestos[85]. En estos casos, se debiera poder impugnar el resultado de estas periciales a los efectos de comprobar cuál ofrece un resultado

85 Esto puede ponerse en relación con lo advertido por Castillo Felipe, R.: "Proceso civil", cit., pp. 288-289, cuando afirmaba que "lo más probable es que, al tiempo que se redujese dicha necesidad de intervención (de los peritos) en algunos campos, se requiriese su presencia en otros. Por ejemplo, para practicar prueba sobre la prueba tendente a desacreditar aquellas propuestas de valoración emitidas por los algoritmos".

más fiable[86]. Lo anterior requeriría de la publicación de los códigos fuentes en abierto y de la transparencia absoluta de estos algoritmos, pues sin ello no podrían impugnarse sus resultados con base en un erróneo funcionamiento, incorrecto desarrollo técnico, existencia de sesgos derivados de un deficiente entrenamiento, etc[87]. Y, ello, a favor de principios procesales esenciales como es la igualdad de armas[88] o el derecho de recurso.

Por su parte, el art. 347 LEC regula la posible actuación de los peritos en el juicio o en la vista, lo que puede consistir en solicitar la exposición completa del dictamen, su explicación, dar respuesta a preguntas y objeciones, etc. En el caso de que el informe haya sido emitido por sistemas de inteligencia artificial, difícilmente el algoritmo podrá acudir a juicio a ratificarlo o a realizar un careo con el informe realizado por otro sistema[89]. En todo caso, que esta intervención en el juicio fuera realizada por miembros del equipo técnico desarrollador del algoritmo, nos llevaría al problema ya referido de la explicabilidad, pues es posible que estos no puedan comprender cómo se ha llegado a determinadas soluciones.

Por último, aunque podríamos tratar otras muchas más aristas, debiéramos plantearnos quién asumiría la responsabilidad civil deriva de la emisión de un

86 Como afirma Montesinos García, A.: "Empleo de", cit., p. 4: "si estas herramientas van a utilizarse como auxilio al juez en la valoración de la prueba, en la medida en que pueden influir en su decisión, las partes deben conocer con carácter previo los elementos y características esenciales del sistema de IA. Solo así podrá permitirse que puedan cuestionar su resultado; lo que no puede impedirse por el mero hecho de estar protegidos por el derecho de propiedad intelectual, pues se quebrantarían gravemente las garantías procesales que deben respetarse en el proceso y se pondría en peligro el derecho de defensa de las partes. A todo justiciable se le tiene que ofrecer la posibilidad de recurrir las decisiones adoptadas en la fase probatoria basadas en programas informáticos, de manera que puedan comprobar que se ha respetado la imparcialidad y se trata de una decisión no sesgada. Por todo ello, deviene imprescindible que se garantice la tan aclamada trasparencia algorítmica". También en ese sentido: De Hoyos Sancho, M.: "El libro", cit., pp. 23-25.

87 En todo caso, como proponen algunos autores, sería recomendable la creación de "un organismo público de control que supervise la creación de algoritmos orientados a la función jurisdiccional", lo que podría ampliarse a la emisión de informes periciales. Conde Fuentes, J.: "Inteligencia artificial y robotización judicial: su impacto en nuestro sistema de justicia, Derecho Digital e Innovación", *Derecho Digital e Innovación. Digital Law and Innovation Review*, 2022, núm. 13, pp. 6-7. Simón Castellano, P.: "Inteligencia artificial", cit., pp. 291-292, apunta que estas comisiones para el control de la algoritmización de este campo, debieran supervisar la publicidad y transparencia de todo el proceso, en concreto: "la trazabilidad del código de IAJVR –detalle de todas las acciones que llevan a cabo todos los agentes con poderes de gestión sobre el código o algoritmo, a modo de backlog o audit trail–, la explicabilidad –hacer fácil lo difícil, hacer comprensible para una persona lega las principales pautas y reglas lógicas que hacen que el algoritmo proyecte esas estimaciones– y auditabilidad –interna y externa, sometido al escrutinio y revisión periódica de ojos expertos ajenos, que puedan certificar eventuales vulnerabilidades o deficiencias en la configuración técnica del sistema–".

88 De Hoyos Sancho, M.: "El libro", cit., p. 23: "Se produciría así lo que Quattrocolo (2019, p. 12) califica en este punto de "asimetría o desequilibrio cognoscitivo", ya que generalmente una parte —la pública, el Ministerio Fiscal—, tendrá acceso a la tecnología más moderna y dispondrá de medios económicos que de forma habitual no estarán al alcance del particular investigado/acusado, quien por tanto no tendrá opciones reales de rebatir o impugnar los resultados que ofrezca la prueba algorítmica". Quattrocolo, S.: "Equitá del processo penale e automated evidence alla luce della Convenzione europea dei diritti dell'uomo", *Revista ítalo-española de Derecho Procesal*, 2019, vol. 2, pp. 118-120.

89 Sólo en los casos en los que estos algoritmos tuvieran asociados sistemas tipo Siri y Alexa vinculados al algoritmo podríamos hablar de ratificación o posible careo, lo que sin duda nos acerca casi a la ciencia ficción.

informe pericial erróneo por parte de un algoritmo con inteligencia artificial generativa.

De todo lo anterior se desprende claramente que la normativa actual no responde a ese hipotético nuevo panorama en que el perito humano fuera sustituido por un perito-robot, lo que nos lleva a afirmar que si se quiere implementar este hipotético sistema con estas condiciones sería necesaria una reflexiva y profunda reconfiguración de la regulación de la prueba pericial, que responda a la nueva lógica que está detrás de estos algoritmos, pero que no suprima los derechos y garantías procesales que amparan a las partes.

V. RETOS DE FUTURO.

Pese a los retos que se plantean y los riesgos para la concatenación de derechos que se generarían, la algoritmización de la prueba, en general, y la prueba pericial, en particular, puede tener un gran recorrido y ofrecer enormes ventajas. Así, puede resultar favorable que un algoritmo, del que se presume objetividad (aunque en determinados casos podría encontrarse sesgado) y no un juez, marcado por la subjetividad humana, sea quien determine la veracidad de los datos aportados al proceso.

Por lo que se refiere a la valoración de la prueba pericial, los algoritmos podrían resultar auxiliadores para valorar: (i) La cualificación, experiencia y capacidad del perito. (ii) El contenido del informe pericial. Empezando por sus aspectos formales, de los que se podrían extraer conclusiones, por ejemplo, en relación con la posible alteración del objeto de pericia por el transcurso temporal existente entre los hechos y la fecha de reconocimiento y examen del objeto para la elaboración de la pericial. Pero, también, se podría valorar la calidad, diversidad y objetividad de las fuentes consultadas, así como el método científico empleado, la existencia de contradicciones o inconsistencias en el dictamen, así como la rotundidad, claridad y precisión y fundamentación de las conclusiones alcanzadas, entre otras. (iii) La objetividad e imparcialidad del perito. A efectos de examinar si concurren las causas para su recusación o tacha, así como la prueba y alegaciones que se aporten para su justificación. Incluso podría valorarse la existencia de una hipotética relación de clientelismo. (iv) Y la comparecencia del perito en el juicio o vista, empleando herramientas similares a las de la valoración de la prueba testifical o la declaración de parte.

Asimismo, los algoritmos podrían utilizarse de forma conjunta para dar un resultado de valoración final o de forma parcial para valorar solo un aspecto en concreto, por ejemplo, la existencia de motivos para tachar al perito.

En todo caso, entendemos que, al menos en un primer momento, estos mecanismos debieran tener siempre una función auxiliadora del juez, que es quien debe tomar la decisión última de la valoración y expresar los motivos que le llevan a ella, pudiendo apartarse del resultado del algoritmo. No obstante, se deberían tomar medidas para evitar el riesgo de que los jueces caigan en el automatismo de dejar que sea la máquina la que tome la decisión y acojan siempre y en cualquier supuesto sus resultados. Así, en nuestra opinión, la introducción de estas herramientas debería ser progresiva, comenzando por la asistencia en algunas tareas para posteriormente ir utilizándose en más aspectos. Además, se debería estudiar cómo se articula dentro del procedimiento, permitiendo que las partes puedan conocer su funcionamiento, garantizando el principio de contradicción y la posibilidad de impugnar sus resultados. Llegado el caso, si su utilización se generalizara para muchos ámbitos, se debería estudiar si se mantiene el procedimiento tal cual está con ciertas adaptaciones o conviene reconfigurarlo por completo, teniendo en cuenta el nuevo paradigma.

El siguiente escenario sería la aparición del perito-robot, es decir, aquellos supuestos en que por medio de algoritmos con inteligencia artificial generativa se pudieran emitir dictámenes periciales como los que actualmente dicta un perito humano. Esto presenta múltiples dudas, tanto desde el punto de vista técnico, pues parece que lo razonable sería que se desarrollaran algoritmos especializados para cada tipo de pericial, como desde el punto de vista de nuestra legislación procesal actual, ya que la normativa no responde a ese hipotético nuevo panorama. En su caso, sería necesaria una reconfiguración de la regulación de la prueba pericial, siempre respetando los derechos y garantías procesales que amparan a las partes y evitando que lo que podría ser un avance se convierta en un retroceso.

BIBLIOGRAFÍA

Abel Fabregó, A.: "Los emojis como fuente de prueba", *Revista Jurídica de Catalunya*, 2021, núm. 4-2021, pp. 113-137.

Ariza Colmenarejo, M. J.: "Impugnación de las decisiones judiciales dictadas con auxilio de inteligencia artificial", en AA.VV.: *Inteligencia artificial legal y administración de justicia* (dir. por S. Calaza López y M. Llorente Sánchez-Arjona), Thomson Reuters Aranzadi, Cizur Menor, 2022, pp. 29-54.

Barona Vilar, S.: *Algoritmización del Derecho y de la Justicia: De la Inteligencia Artificial a la Smart Justice*, Tirant lo Blanch, Valencia, 2021.

Barona Vilar, S.: "Cuarta revolución industrial (4.0.) o ciberindustria en el proceso penal: revolución digital, inteligencia artificial y el camino hacia la robotización de la justicia", *Revista Jurídica Digital UANDES*, 2019, vol. 3, núm. 1, pp. 1-17.

Battelli, E.: "La decisión robótica, algoritmos, interpretación y justicia predictiva", *Revista de Derecho Privado*, 2020, núm. 38, pp. 45-86.

Blanco García, A. I.: "El periculum in mora de las medidas cautelares reales. La ¿utilidad? De la Inteligencia Artificial en su detección", en AA.VV.: *Sistemas predictivos en la justicia civil* (ed. por A. I. Blanco García), Tirant lo Blanch, Valencia, 2024, pp. 79-112.

Bonet Navarro, J.: "Valoración de la prueba y resolución mediante inteligencia artificial", en AA.VV.: *Derecho Procesal: retos y trasformaciones* (dir. por L. Bujosa Vadell), Atelier, Barcelona, 2021, p. 315-337.

Bonet Navarro, J.: "La tutela judicial de los derechos no humanos. (De la tramitación electrónica al proceso con robots autónomos)", *Revista Ceflegal*, 2018, núm. 208, pp. 55-92.

Borges Blázquez, R.: "La inteligencia artificial en el proceso penal y el ¿regreso? de Lombroso", en AA.VV.: *Justicia algorítmica y neuroderecho, Una mirada multidisciplinar* (ed. por S. Barona Vilar), Tirant lo Blanch, Valencia, 2021, pp. 157-181.

Borrás Andrés, N.: "La verdad y la ficción de la inteligencia artificial en el proceso penal", en AA.VV.: *La justicia digital en España y la Unión Europea: Situación actual y perspectivas de futuro* (dir. por J. Conde Fuentes y G. Serrano Hoyo), Atelier, Barcelona, 2019, pp. 31-39.

Bueno De Mata, F.: "Macrodatos, Inteligencia Artificial y Proceso: Luces y sombras", *Revista General de Derecho Procesal*, 2020, núm. 51 (versión online).

Cantos Pardo, M.: "The Wayback Machine: origen, retos y utilización como fuente de prueba en materia de propiedad industrial", *ADI*, 2022, núm. 42, pp. 265-280.

Casar Corredera, J. R.: "Inteligencia artificial generativa", *Anales de la Real Academia de Doctores de España*, 2023, Volumen 8, núm. 3–2023, p. 475-489.

Castillo Felipe, R.: "Proceso civil e inteligencia artificial", en AA.VV.: *Proceso civil y nuevas tecnologías* (dir. por J. Sigüenza López), Aranzadi, Cizur Menor, 2021, pp. 259-296.

Catalán Chamorro, M. J.: *La justicia digital en España, retos y desafíos*, Tirant lo Blanch, Valencia, 2023.

Conde Fuentes, J.: "Inteligencia artificial y robotización judicial: su impacto en nuestro sistema de justicia, Derecho Digital e Innovación", *Derecho Digital e Innovación. Digital Law and Innovation Review*, 2022, núm. 13 (versión online).

Cortés Domínguez, V.: "El dictamen de peritos", en V. Cortés Domínguez, V. y V. Moreno Catena, *Derecho Procesal Civil, Parte General*, Tirant lo Blanch, Valencia, 2021, pp. 273-286.

De Hoyos Sancho, M.: "El libro blanco sobre inteligencia artificial de la Comisión Europea: reflexiones desde las garantías esenciales del proceso penal como "sector de riesgo"", *Revista Española de Derecho Europeo*, 2020, núm. 76, pp. 9-43.

De Luis García, E.: "Sistemas predictivos y tutela civil: impacto sobre los derechos y garantías procesales", en AA.VV.: *Sistemas predictivos en la justicia civil* (ed. por A. I. Blanco García), Tirant lo Blanch, Valencia, 2024, pp. 239-245.

Denault, V., et altri: "The analysis of nonverbal communication: The dangers of pseudoscience in security and justice contexts", *Anuario de Psicología Jurídica*, 2020, núm. 30, pp. 1-12.

Escalada López, M. L.: "El dictamen de peritos en el proceso de patentes", *Revista de Derechos de la Competencia y Distribución*, 2011, núm. 9/2011 (versión electrónica).

Gómez Colomer, J. L.: "Los medios de prueba en concreto", en AA.VV.: *Proceso Civil, Derecho Procesal II* (coord. por J. L. Gómez Colomer y S. Barona Vilar), Tirant lo Blanch, Valencia, 2023, p. 262.

Gómez Colomer, J. L.: "Unas reflexiones sobre el llamado "juez-robot", al hilo del principio de la independencia judicial", en AA.VV.: *Justicia algorítmica y neuroderecho, Una mirada multidisciplinar* (ed. por S. Barona Vilar), Tirant lo Blanch, Valencia, 2021, pp. 243-263.

Gómez Jiménez, Á.: "Verificación y valoración digital por Inteligencia Artificial (AI)", *CESVI*, 2022, núm. 120, pp. 36-40.

Grimm, P. W.; Grossman, M. R. y Cormack, G V.: "Artificial intelligence as evidence", *Northwestern Journal of Technology and Intellectual Property*, 2021, vol. 19, núm. 1, pp. 9-106.

Izquierdo Blanco, P.: "¿Qué espera un juez de un buen dictamen para ser convincente?", en AA.VV.: *La prueba pericial a examen. Propuestas de lege ferenda* (dir. por J. Picó i Junoy), Bosch, Barcelona, 2020, pp. 215-232.

Katz, P.: "Expert robot: using artificial intelligence to assist judges in admitting scientific expert testimony", *Albany Law Journal of Science & Technology*, 2014, vol. 24, Issue 1, pp. 1-46.

Khatniuk, N.; Shestakovska, T.; Rovnyi, V.; Pobiianska, N. y Surzhyk, Y.: "Legal principles and features of artificial intelligence use in the provision of legal services", *SDG Journal of Law ans sustainable development*, 2023, vol. 11, núm. 5, pp. 1-18.

Mahesh, B.: "Machine Learning Algorithms-A Review", *International Journal of Science and Research*, 2020, núm. 9, pp. 381-386.

Marcos Francisco, D.: "Smart ODR y su puesta en práctica: el salto a la inteligencia artificial", *Revista General de Derecho Procesal*, 2023, núm. 59, pp. 1-41.

Martín Diz, F.: "Justicia predictiva: inteligencia artificial y algoritmos aplicados al proceso judicial en materia probatoria", en AA.VV.: *El impacto de las tecnologías disruptivas*, (dir. por F. Bueno De Mata), Aranzadi, Cizur Menor, 2022, pp. 131-154.

Martín Diz, F.: "Herramientas de inteligencia artificial y adecuación en el ámbito del proceso judicial, en AA.VV.: *Derecho Procesal, Retos y Transformaciones* (dir. por L. M. Bujosa Vadell), Atelier, Barcelona, 2021, pp. 295-304.

Massaguer Fuentes, J.: *Acciones y procesos de infracción de Derechos de Propiedad Industrial*, Civitas Thomson Reuters, Cizur Menor, 2020.

MATSUMOTO, D. y HWANG, H. C.: "Microexpressions differentiate truths from lies about future malicious intent", *Frontiers in Psychology*, 2018, núm. 9, pp. 1-11.

MONTAÑÁ MORA, M.: "La Nueva Ley de Patentes y el sector farmacéutico", *Cuadernos Derecho Farmacéutico*, 2015, núm. 55, pp. 6 y ss.

MONTESINOS GARCÍA, A.: "Reflexiones sobre la algoritmización del proceso judicial civil", en AA.VV.: *Sistemas predictivos en la justicia civil* (ed. por A. I. BLANCO GARCÍA), Tirant lo Blanch, Valencia, 2024, pp. 21-56.

MONTESINOS GARCÍA, A.: "Empleo de la inteligencia artificial en algunas fases del proceso judicial civil: prueba, medidas cautelares y sentencia", *Actualidad civil*, 2022, núm. 11, pp. 1-20.

MONTESINOS GARCÍA, A.: "Afectación de los derechos y garantías procesales por el empleo de algoritmos predictivos", en AA.VV.: *El proceso como garantía*, (dir. por J. M. ASENSIO MELLADO), Atelier, Barcelona, 2023, pp. 703-714.

NIEVA FENOLL, J.: "Inteligencia artificial y proceso judicial: perspectivas ante un alto tecnológico en el camino", en AA.VV.: *Inteligencia artificial legal y administración de justicia* (dir. por S. CALAZA LÓPEZ y M. LLORENTE SÁNCHEZ-ARJONA), Thomson Reuters Aranzadi, Cizur Menor, 2022, pp. 417-437.

NIEVA FENOLL, J.: "Un cambio generacional en el proceso judicial: La inteligencia artificial", en AA.VV.: *Derecho Procesal: retos y transformaciones* (dir. por L. M. BUJOSA VADELL), Atelier, Barcelona, 2021, pp. 281-294.

NIEVA FENOLL, J.: "Repensando Daubert: la paradoja de la prueba pericial", en AA.VV.: *Peritaje y prueba pericial* (dir. por J. PICÓ I JUNOY), Atelier, Barcelona, 2017, pp. 85-101.

ORTELLS RAMOS, M.: «Capítulo 14», en AA.VV.: *Derecho Procesal Civil* (dir. por M. ORTELLS RAMOS), Aranzadi Thomson Reuters, Cizur Menor, 2022, p. 237-260.

PELLICER ORTIZ, B.: "¿Cuándo un juez deja de creer en un dictamen pericial?", en AA.VV.: *La prueba pericial a examen. Propuestas de lege ferenda* (dir. por J. PICÓ I JUNOY), Bosch, Barcelona, 2020, pp. 209-216.

PICÓ I JUNOY, J.: "Retos del derecho probatorio ante las nuevas tecnologías", en AA.VV.: *Inteligencia artificial legal y administración de justicia* (dir. por S. CALAZA LÓPEZ y M. LLORENTE SÁNCHEZ-ARJONA), Thomson Reuters Aranzadi, Cizur Menor, 2022, pp. 439-455.

Picó i Junoy, J.: "La prueba pericial civil en la literatura procesal española", en AA.VV.: *La prueba pericial a examen. Propuestas de lege ferenda* (dir. por J. Picó i Junoy), Bosch, Barcelona, 2020, pp. 35-52.

Picó i Junoy, J.: "La prueba del dolor", en AA.VV.: *Neurociencia y proceso judicial* (dir. por M. Taruffo y J. Nieva Fenoll), Marcial Pons, Madrid, 2013, pp. 83-96.

Planchadell-Gargallo A.: "Inteligencia Artificial y medidas cautelares", en AA.VV.: *Justicia algorítmica y neuroderecho, Una mirada multidisciplinar* (ed. por S. Barona Vilar), Tirant lo Blanch, Valencia, 2021, pp.129-160.

Quattrocolo, S.: "Equitá del processo penale e automated evidence alla luce della Convenzione europea dei diritti dell'uomo", *Revista ítalo-española de Derecho Procesal*, 2019, vol. 2, p. 107-123.

Sánchez, M. y Carbajal, E.: "La inteligencia artificial generativa y la educación universitaria", *Perfiles Educativos*, 2023, vol. 45, número especial, pp. 70-86.

Sanchis Crespo, C.: "Inteligencia artificial y decisiones judiciales: crónica de una transformación anunciada", *Scire*, 2023, vol. 29, núm. 2, pp. 65-84.

Simó Soler, E. y Rosso, P.: "La destrucción algorítmica de la humanidad", *Diario La Ley*, 2022, núm. 9982 (versión online).

Simón Castellano, P.: "Inteligencia artificial y valoración de la prueba: las garantías jurídico-constitucionales del órgano de control", *TH□MIS-Revista de Derecho*, 2021, núm. 79, pp. 283-297.

Soriano Arnanz, A. y Simó Soler, E.: "Machine learning y Derecho: aprendiendo la (des)igualdad", en AA.VV.: *Justicia algorítmica y neuroderecho, Una mirada multidisciplinar* (ed. por S. Barona Vilar), Tirant lo Blanch, Valencia, 2021, pp. 183-207.

Ullah, Z.; Al-turjman, F.; Mostarda, L. y Gagliardi, R.: "Applications of artificial intelligence and machine learning in smart cities", *Computer Communications*, 2020, Vol. 154, pp. 313-323.

Vázquez Pizarro, M. T.: "Especialidades de la práctica de la prueba pericial en los procedimientos sobre patentes", *Diario La Ley*, 2020, núm. 9568 (LA LEY 900/2020).

Váquez Rojas, C.: "La imparcialidad, la independencia y la objetividad pericial. Los factores humanos de los expertos", en AA.VV.: *La prueba pericial a examen.*

Propuestas de lege ferenda (dir. por J. Picó i Junoy), Bosch, Barcelona, 2020, pp. 117-141.

Vázquez Rojas, C.: *De la prueba científica a la prueba pericial*, Marcial Pons, Madrid, 2015.

CONVERGENCIA INTERNACIONAL Y CAMINOS PROPIOS: REGULACIÓN DE LA INTELIGENCIA ARTIFICIAL EN AMÉRICA LATINA*

INTERNATIONAL CONVERGENCE AND OWN PATHS: REGULATION OF ARTIFICIAL INTELLIGENCE IN LATIN AMERICA

Actualidad Jurídica Iberoamericana Nº 21, agosto 2024, ISSN: 2386-4567, pp. 468-493

* Este trabajo es parte de la investigación financiada por Fondecyt Regular No. 1230895, por el proyecto I+D–2022 UCEN, No. CIP2022015, y por el proyecto financiado por Ministerio de Ciencia e Innovación (España), Expediente No. PID2021-123170OB-I00: "Claves para una justicia digital y algorítmica con perspectiva de género".

Pablo
CONTRERAS

ARTÍCULO RECIBIDO: 29 de mayo de 2023
ARTÍCULO APROBADO: 1 de julio de 2024

RESUMEN: El texto brinda una panorámica de los intentos de regulación de la inteligencia artificial en América Latina. Para ello, examina las obligaciones de tratados internacionales relacionados, los instrumentos de soft law sobre la materia y las estrategias o políticas nacionales de Estados latinoamericanos. A partir de la descripción de los distintos niveles regulatorios, se explica cómo, en ciertas materias, los Estados latinoamericanos convergen con estándares internacionales o europeos, confirmándose el efecto "Bruselas". Sin embargo, la región exhibe peculiaridades regulatorias como el reconocimiento de los neuroderechos y la normativa de neurotecnologías. Además, con la aprobación del Parlamento Europeo del Reglamento de Inteligencia Artificial, es posible que se intensifique el efecto "Bruselas" en los proyectos de ley que actualmente se encuentran en tramitación en los congresos latinoamericanos.

PALABRAS CLAVE: Inteligencia artificial; América Latina; regulación de tecnología; datos personales; efecto Bruselas.

ABSTRACT: *The paper provides an overview of AI regulatory attempts in Latin America. It examines the related international treaty obligations, the soft law instruments on the subject and the national strategies or policies of Latin American States. From the description of the different regulatory levels, it explains how, in certain matters, Latin American States converge with international or European standards, confirming the "Brussels" effect. However, the region exhibits regulatory peculiarities, such as the recognition of neuro-rights and the regulation of neurotechnologies. Furthermore, with the approval by the European Parliament of the Artificial Intelligence Regulation, it is possible that the "Brussels" effect will intensify in the bills currently being processed in Latin American congresses.*

KEY WORDS: *Artificial intelligence; technology regulation; Latin America; personal data, Brussels effect.*

I. INTRODUCCIÓN.

¿Cómo entender los intentos de regulación de la inteligencia artificial (IA) en América Latina? Si bien es un tema que se aborda desde la realidad europea, estadounidense o china, la región latinoamericana suele estar olvidada en los estudios sobre la materia. Este texto busca llenar ese vacío en la literatura, tomar distintas piezas regulatorias en curso –notando sus vacíos– y presentar las tensiones en el desarrollo de esquemas de gobernanza de la IA en América Latina[1]. Evidentemente, existen distintos instrumentos regulatorios para enfrentar estas tecnologías[2]. Este texto se sitúa en un plano general de la región y busca ilustrar el panorama latinoamericano relativo a tratados internacionales y soft law sobre la materia misma y aspectos conexos, como la protección de datos personales y la ciberseguridad. A partir de ello, se contrasta con las iniciativas domésticas que se encuentran en tramitación legislativa con indicadores de gobernanza elaborados por el Centro Nacional de Inteligencia Artificial (CENIA), durante 2023.

En primer término, el texto aborda la ausencia de un tratado internacional general sobre regulación de la IA y la falta de tratativas preliminares al respecto. Tampoco se estima que existe regulación internacional conexa que pudiere ser aplicable. Por ejemplo, el marco general de derechos humanos, a nivel interamericano, es limitado y con escasos pronunciamientos sobre el impacto de la tecnología en la garantía de los derechos. Asimismo, respecto de otros tratados, la convergencia con Europa es incipiente. Por un lado están las ratificaciones al Convenio 108+ del Consejo de Europa, por parte de Uruguay y Argentina, pero también cómo sigue pendiente el caso mexicano. Algo similar puede decirse respecto de la Convención de Budapest.

Sin embargo, a nivel de tratados, destaca el "Digital Economy Partnership Agreement" (DEPA). Se trata de un tratado entre Chile, Singapur y Nueva Zelandia que Busca generar un marco adecuado para fomentar la exportación

1 Sobre IA y el denominado "Sur Global", véase Arun, C.: "AI and the Gobal South: Designing for other Worlds", en AA.VV.: *The Oxford Handbook of Ethics of AI* (ed. por M. Dubber *et al*), Oxford University Press, Oxford, 2020.

2 Clarke, R.: "Regulatory alternatives for AI", *Computer Law & Security Review*, vol. 35, núm 4, 2019, pp. 398-409.

• Pablo Contreras
Profesor asociado de la Universidad Central de Chile, Director de la Cátedra Legal Tech UCentral. Correo electrónico: pablo.contreras@ucentral.cl

de productos y servicios, regulando los flujos de datos, la no discriminación a productos digitales, la identidad digital y privacidad, y la IA, entre otras materias. En su art. 8, el tratado obliga a los Estados partes a generar la adopción de marcos éticos y de gobernanza que apoyen el uso fiable, seguro y responsable de las tecnologías de la inteligencia artificial (marcos de gobernanza de la inteligencia artificial). Se trata de una norma de hard law que media a un soft law, generado domésticamente, pero que debe dialogar con estándares internacionales.

A nivel de soft law, el panorama interamericano nuevamente carece de instrumentos explícitos sobre IA. A nivel de la OEA, los instrumentos relevantes dicen relación con privacidad y protección de datos personales, por un lado, y con neurociencias y neuroderechos, por el otro. En el nivel de instituciones técnicas, la Red Iberoamericana de Protección de Datos ha elaborado unas Recomendaciones generales para el tratamiento de datos en inteligencia artificial y una Declaración sobre neurodatos, ambas en línea con la OEA.

Por último, a nivel doméstico, los países carecen de leyes generales de IA. Dado el índice de CENIA, es posible advertir que la mayoría de los países de Latinoamérica que forman parte de la OCDE sí tienen estrategias nacionales en IA, instituciones que pueden liderar la gobernanza en la materia pero que la regulación general o conexa de la IA es deficitaria y no existen entornos para la experimentación regulatoria (sandboxes, por ejemplo). Los proyectos de ley dialogan con Europa en algunos aspectos, pero parecen, más que nada, intentos fragmentarios que no desarrollan las estrategias generales de cada país.

II. EL CONTEXTO LATINOAMERICANO.

La revisión del panorama latinoamericano requiere dar cuenta de algunos factores que explican cómo se ha dado la relación entre los Estados que conforman la región. En términos sintéticos, existen tres factores que explican el tipo de relacionamiento y producción de normas a nivel regional: i) débiles lazos de integración, ii) baja densidad normativa en la regulación internacional y iii) estrategias unilaterales basadas en los intereses estratégicos de integración y comercio.

En esta sección se revisan los aspectos centrales de hard law y soft law en la gobernanza de la IA. Además, se revisan las estrategias nacionales y la normativa doméstica de los países latinoamericanos que forman parte de la OCDE para obtener un panorama de la regulación en la materia.

1. Tratados internacionales.

No existe un tratado internacional general o marco sobre IA a nivel global y el interés del derecho internacional público, en la literatura, es incipiente[3]. Los diversos instrumentos internacionales que se han desarrollado sobre la materia apuntan a cuestiones específicas[4]. Por ejemplo, existen las enmiendas a la Convención de Viena sobre la Circulación Vial de 1968[5], con el objeto de eliminar los obstáculos legales para incorporar los vehículos autónomos conforme a la tecnología vigente. Otro tanto se encuentra en el caso de la discusión sobre los sistemas de armas autónomos y las recomendaciones del Comité Internacional de la Cruz Roja para establecer normas internacionales jurídicamente vinculante[6].

Los intentos regulatorios sobre la IA, con carácter marco o general, provienen específicamente desde Europa. Desde el plano del derecho internacional, el Comité sobre IA del Consejo de Europa divulgó el "borrador cero" de su Convención sobre Inteligencia Artificial, Derechos Humanos, Democracia y Estado de Derecho[7]. En la misma senda de la protección de datos personales, el borrador del tratado tiene una pretensión de universalidad[8] y permite su ratificación por Estados que no son parte del Consejo de Europa, al igual que el Convenio 108 y 108+ sobre protección de datos personales[9]. En otros términos, a

3 Arvidsson, M. & Noll, G.: "Artificial Intelligence, Decision Making and International Law", *Nordic Journal of International Law*, vol. 92, 2023, pp. 1-2.

4 Contreras, P. & Trigo, P.: "La gobernanza de la inteligencia artificial. Esbozo de un mapa entre *hard law* y *soft law* internacional", en AA.VV.: *Inteligencia artificial y derecho* (ed. por M. Azuaje & P. Contreras), Tirant lo Blanch, Valencia, 2021, pp. 457-477; Lee, J.: *Artificial Intelligence and International* Law, Springer, Dordrecht, 2022, pp. 227.

5 Convención de Viena sobre la Circulación Vial. (1968). Viena, Austria. 8 de noviembre de 1968, entró en vigor el 21 de mayo de 1977.

6 Cicr: "Armas autónomas: el CICR insta a los Estados a avanzar hacia la negociación de un tratado", (disponible en https://www.icrc.org/es/document/armas-autonomas-el-cicr-insta-los-estados-avanzar-hacia-la-negociacion-de-un-tratado, último acceso de 28 de marzo 2024).

7 Cai: "Revised Zero Draft [Framework] Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law" (disponible en https://rm.coe.int/cai-2023-01-revised-zero-draft-framework-convention-public/1680aa193f, último acceso de 28 de marzo 2024).

8 Su vocación universal es clara: el Comité busca "desarrollar un instrumento que resulte atractivo, no sólo para los Estados de Europa, sino para el mayor número posible de Estados de todas las regiones del mundo. Cuanto más global sea el instrumento, más impacto tendrá en la vida de las personas de todo el planeta". El presidente del Comité hizo un llamado "a todos los Estados del mundo que defienden los valores de los derechos humanos, la democracia y el Estado de Derecho para que se unan a nuestros esfuerzos por desarrollar un conjunto de principios básicos compartidos aplicables al diseño, desarrollo y aplicación de la IA". Cai: "CAI – Committee on Artificial Intelligence" (disponible en https://www.coe.int/en/web/artificial-intelligence/cai, último acceso de 28 de marzo 2024).

9 Consejo de Europa: "Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos Personales (Convenio núm. 108)", Estrasburgo, Francia. 28 de enero de 1981, entró en vigor el 1 de octubre de 1985 y Consejo de Europa: "Protocolo del Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos Personales, relativo a la modernización del Convenio 108 (Convenio 108+)", Estrasburgo, Francia. Firmado el 10 de octubre de 2018. Véase Greenleaf, G.: "The influence of European data privacy standards outside Europe: Implications for globalization of Convention 108", *International Data Privacy Law*, vol. 2, núm. 2, 2012, pp. 68-92; Terwangne, C.: "Council of Europe convention 108+: A modernised international treaty for the protection of personal data", *Computer Law & Security Review*, vol. 40, 2021.; Bertoni, E.: "Convention 108 and the GDPR: Trends and perspectives in Latin America", *Computer Law & Security Review*, vol. 40, 2021.

nivel de tratados, el Consejo de Europa está replicando la estrategia de protección de datos personales y siguiendo el carril de la Unión Europea: de un reglamento general –por parte de la Unión Europea– a un tratado marco ratificable por cualquier Estado –por parte del Consejo de Europa–.

En Latinoamérica, no existen intentos similares al europeo a nivel de tratados. En primer término, no es posible advertir un esfuerzo por redactar o confeccionar un tratado general o marco en materia de IA. En segundo término, no existe un marco regulatorio en materia de protección de datos personales ni ciberseguridad, salvo por los desarrollos de soft law que se explican en la siguiente sección. En tercer término, la aplicación de tratados internacionales en materia de derechos humanos es limitada en la materia. En efecto, el principal tratado regional de derechos humanos –la Convención Americana sobre los Derechos Humanos[10]– sólo marginalmente se ha ocupado de los desafíos tecnológicos de los derechos. Pero, por ejemplo, no es posible identificar un caso en que la Corte Interamericana de Derechos Humanos haya reconocido el derecho a la protección de datos personales bajo el artículo 11 de la Convención (protección de la honra y dignidad, aunque en inglés es right to privacy)[11]. La Corte parece avanzar en la dirección de ampliar el radio de protección del derecho a la privacidad[12], especialmente tras la pandemia del Covid-19 y las medidas que los Estados partes implementaron para su control[13]. Sin embargo, la agenda de derechos humanos y tecnología pareciera todavía estar pendiente de precedentes por parte de la Corte Interamericana[14].

10 Organización de los Estados Americanos: *Convención Americana sobre Derechos Humanos*. Firmada el 22 de noviembre de 1969, entró en vigor el 18 de julio de 1978.

11 Affonso Souza, C. *et al.*: "From privacy to data protection: the road ahead for the Inter-American System of human rights", *The International Journal of Human Rights*, vol. 25, núm. 1, 2020 (argumentando que la relación entre tecnología y protección de datos será uno de los desafíos del Sistema Interamericano de derechos Humanos en los próximos años); Zingales, N.: "A Stronger Right to Data Protection During Pandemics? Leveraging The American Convention of Human Rights Against Governmental Inaction: A Brazilian Case-Study", *Revista Brasileira De Direitos Fundamentais & Justiça*, vol. 14, núm. 43, 2021, p. 450 (afirmando que la CADH "no incluye el derecho a la protección de datos personales" pero que se puede "argumentar que el alcance de la protección otorgada en virtud del artículo 11 es lo suficientemente amplio como para abarcar este derecho de alguna forma").

12 Corte Interamericana de Derechos Humanos. (2012). Caso Artavia Murillo y otros ("Fecundación in Vitro") vs. Costa Rica. Sentencia de 28 de noviembre de 2012. Véase la evolución jurisprudencial de la Corte, en esta materia, en Aguilar Cavallo, G. & Sandoval, M.I.: "La protección de datos personales en un contexto digital desde los estándares de la Corte Interamericana de Derechos Humanos", en AA.VV.: *Derecho digital y privacidad en América y Europa. Perspectiva chilena y comparada* (ed. C. Droguett González & N. Walker Silva), Tirant lo Blanch, Valencia, 2023, pp. 195-204.

13 En una declaración con motivo de la pandemia, la Corte comunicó que "[d]eben disponerse las medidas adecuadas para que el uso de la tecnología de vigilancia para monitorear y rastrear la propagación del coronavirus COVID-19, sea limitado y proporcional a las necesidades sanitarias y no implique una injerencia desmedida y lesiva para la privacidad, *la* protección de datos personales, y a la observancia general del principio de no discriminación." Corte Interamericana de Derechos Humanos: "Declaración de la Corte Interamericana de Derechos Humanos 1/20. Covid-19 y derechos humanos: los problemas y desafíos deben ser abordados con perspectiva de derechos humanos y respetando las obligaciones internacionales" (disponible en https://www.corteidh.or.cr/tablas/alerta/comunicado/declaracion_1_20_ESP.pdf, último acceso de 28 de marzo 2024).

14 A nivel de la Comisión, existen pronunciamientos sobre la materia. Véase Comisión Interamericana de Derechos Humanos: "Pandemia y derechos humanos en las Américas" (disponible en https://www.oas.org/es/cidh/informes/pdfs/2023/PandemiaDDHH_ES.pdf, último acceso de 28 de marzo 2024), pp. 89 y ss.; Comisión Interamericana de Derechos Humanos: "La CIDH y su RELE llaman a los Estados a adoptar

Desde el punto de vista de las estrategias individuales de los Estados de la región, es posible advertir la convergencia a los tratados internacionales en materia de protección de datos y ciberseguridad. En la primera materia, podemos anotar las ratificaciones de Uruguay y Argentina al Convenio 108+ del Consejo de Europa[15]. Sin embargo, países con autoridades garantes de protección de datos, como México, aún no han ratificar este tratado[16].

Una peculiaridad en el panorama latinoamericano del hard law internacional es el caso del DEPA, un tratado internacional ratificado por Chile, Singapur y Nueva Zelanda[17]. El tratado es un marco para fomentar la exportación de productos y servicios digitales, regulando los flujos de datos, la no discriminación a productos digitales, la identidad digital y privacidad, y la IA, entre otras materias. Como se ha señalado, el tratado "proporciona el modelo más completo hasta la fecha para un acuerdo comercial regional adaptado a la economía en transformación digital"[18]. El tratado se encuentra abierto para la firma de otros Estados partes y busca implementar mecanismos que permitan construir confianza en el flujo de datos[19]. En esa dimensión –en la regulación de datos para una economía que emplea la IA[20]– el tratado avanza en un modelo híbrido de regulación de este tipo de tecnologías. El artículo 8.2 del tratado versa sobre IA y reconoce la importancia que tiene en la economía digital. Su inciso segundo promueve la "elaboración de marcos éticos y de gobernanza para el uso fiable, seguro y responsable de las tecnologías de la inteligencia artificial" y busca que "esos marcos estén armonizados internacionalmente". Dichos marcos deberán tener en cuenta "los principios o directrices reconocidos internacionalmente, en particular la explicabilidad, la

medidas para reducir las brechas digitales de las personas mayores", (disponible en https://www.oas.org/es/cidh/jsForm/?File=/es/cidh/prensa/comunicados/2021/259.asp, último acceso de 28 de marzo 2024).

15 Véase el detalle de las ratificaciones [en línea]: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=223 (última visita efectuada 26.03.24).

16 México ratificó el Convenio 108 pero no ha podido dar el salto para ratificar el Convenio 108+. Una de las principales dificultades estriba en la diferencia de estándares normativos entre la Ley Federal de Protección de Datos Personales en Posesión de los Particulares –que regula al sector privado– y la Ley General de Protección de Datos en Posesión de Sujetos Obligados –que regula al sector público–. Al respecto, véase Mendoza Enríquez, O.: "Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento", *IUS. Revista del Instituto de Ciencias Jurídicas de Puebla*, vol. 12, núm. 4, 2018, pp. 279 y ss.

17 En el caso de Chile, véase Decreto No. 110, del Ministerio Relaciones Exteriores: Promulga el Acuerdo de Asociación de Economía Digital entre la República de Chile, Nueva Zelanda y la República de Singapur (Diario Oficial, 30.11.21). Disponible [en línea]: https://www.bcn.cl/leychile/navegar?idNorma=1168805&tipoVersion=0 (última visita efectuada 26.12.23).

18 Ciuriak, D. & Fray, R.: "The Digital Economy Partnership Agreement. Should Canada Join?", *Centre for International Governance Innovation Policy* Brief, núm 171, 2022 (disponible en https://www.cigionline.org/static/documents/PB_no.171.pdf, último acceso de 28 de marzo 2024).

19 Schaffer, G.: "Trade Law in a Data-Driven Economy. The Need for Modesty and Resilience", en AA.VV.: *Artificial Intelligence and International Economic Law. Disruption, Regulation, and Reconfiguration* (ed. por S. Peng *et al.*), Cambridge University Press, Cambridge, 2021, p. 44.

20 Streinz, T.: "International Economic Law's Regulation of Data as a Resource for the Artificial Intelligence Economy", en AA.VV.: *Artificial Intelligence and International Economic Law. Disruption, Regulation, and Reconfiguration* (ed. por S. Peng *et al.*), Cambridge University Press, Cambridge, 2021, p. 176; Lee, J.: "Artificial Intelligence", cit., p. 229.

transparencia, la equidad y los valores centrados en el ser humano". Se trata de un modelo híbrido por el tipo de norma: tal como ha señalado Soprana, "el artículo 8.2 está redactado en un lenguaje más bien blando, de máximo empeño, no puede considerarse un compromiso vinculante para desarrollar marcos de gobernanza de la IA, sino más bien una herramienta de señalización"[21]. El marco obligatorio estaría dado por el tratado en sus reglas pero con compromiso que *insta* a los Estados partes en avanzar en los marcos éticos nacionales sobre IA. La norma no deja de ser curiosa: es una bisagra particular entre hard law y soft law[22]. Inserta en un tratado que es, evidentemente obligatorio, exhorta a las partes a avanzar en marcos éticos de gobernanza de la IA, con apertura a los desarrollos regionales e internacionales en la materia.

2. Soft law.

Recientemente, la Asamblea General de Naciones Unidas aprobó una resolución general con lineamientos y directrices relevantes para la gobernanza de la IA, lo que constituye un primer instrumento soft law de carácter general en la materia[23]. Su contenido fue promovido por Estados latinoamericanos como Argentina, Brasil, Chile, Colombia, Costa Rica, Ecuador, Guatemala, Paraguay, República Dominicana y Perú. Se trata de una resolución que busca que los Estados se "abstengan o dejen de usar sistemas de [IA] que sean imposibles de operar en consonancia con el derecho internacional o que supongan riesgos indebidos para el disfrute de los derechos humanos [...]"[24].

Fuera del nivel de las obligaciones internacionales propias de los tratados, y a nivel regional, los instrumentos de soft law relativos a la IA no abundan en la región. Siguiendo la examinación de fuentes directas y circundantes sobre IA, es posible advertir sólo algunos limitados instrumentos en materia de protección de datos personales y, curiosamente, sobre neuroderechos.

Por ejemplo, a nivel de la Organización de Estados Americanos (OEA), se adoptaron los "Principios de Actualizados sobre la Privacidad y la Protección de Datos Personales"[25]. El documento, preparado por el Comité Jurídico

21 Soprana, M.: "The Digital Economy Partnership Agreement (DEPA): Assessing the Significance of the New Trade Agreement on the Block", *Trade, Law and Development*, vol. XIII, núm. 1, 2021, p. 161.

22 Contreras, P. & Trigo, P., "La gobernanza", cit.

23 Naciones Unidas: "Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development", Res. A/78/L.49.ES. (disponible en https://digitallibrary.un.org/record/4040897?v=pdf, último acceso de 28 de marzo 2024).

24 Naciones Unidas: "Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development", Res. A/78/L.49.ES. (disponible en https://digitallibrary.un.org/record/4040897?v=pdf, último acceso de 28 de marzo 2024), §5.

25 Comité Jurídico Interamericano: "Principios actualizados sobre la privacidad y la protección de datos personales", (disponible en https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf, último acceso de 28 de marzo 2024).

Interamericano (CJI) de la OEA, contiene estándares básicos y bastante comunes en materia de protección de datos personales, fácilmente reconocibles en las normas domésticas de los Estados Partes de la organización. [Completar]. Adicionalmente, la OEA ha adoptado su "Declaración de Principios interamericanos en materia de Neurociencias, Neurotecnologías y Derechos Humanos"[26]. Al igual que los principios de protección de datos, se trata de un documento preparado por el CJI y enuncia 10 principios sobre la materia con el objeto de fijar una

"directriz importante para que las personas pueden aprovechar con plenitud las ventajas y beneficios de los avances científicos y sus aplicaciones en el campo de la neurociencia y desarrollo de las neurotecnologías en la seguridad de que no habrá menoscabo de sus derechos humanos, estableciendo de esta manera estándares internacionales que contribuyan a orientar y armonizar las regulaciones nacionales necesarias en esta materia".[27]

A nivel de Apec, no hay un esquema de soft law que provea una directriz común para sus Estados miembros en materia de IA. Se suele destacar la integración generada a partir del DEPA en el caso de Chile, Nueva Zelanda y Singapur[28], así como del "Digital Economy Agreement" entre Australia y Singapur[29], además de relevar las estrategias nacionales que algunos países contemplan[30]. Desde el punto de vista de regulaciones conexas, Apec provee un esquema de protección de datos personales en el tráfico transfronterizo de datos, conocido como "cross-border privacy rules" (CBPR, por sus siglas en inglés). Se trata, básicamente, de un esquema voluntario que se adopta a nivel de países, y que provee una certificación por quienes se enmarcan bajo dicho sistema[31]. Sin embargo, tal como ha afirmado Greenleaf, es un sistema con escaso impacto en elevar los estándares de protección

26 Comité Jurídico Interamericano: "Declaración de Principios interamericanos en materia de Neurociencias, Neurotecnologías y Derechos Humanos", OEA/Ser. Q. CJI/RES. 281 (CII-O/23) corr. 1. (disponible en https://www.oas.org/es/sla/cji/docs/CJI-RES_281_CII-O-23_corr1_ESP.pdf, último acceso de 28 de marzo 2024).

27 Comité Jurídico Interamericano: "Declaración de Principios", cit., §1.

28 Apec Business Advisory Council: "Trust: Providing a framework for ethical AI" (disponible en https://aiinapec.info/trust-providing-a-framework-for-ethical-ai-2/ último acceso de 28 de marzo 2024). Véase también Wirjo, A. *et al.*: "Artificial Intelligence in Economic Policymaking", *APEC Policy Brief*, núm. 52, 2022 (disponible en https://www.apec.org/docs/default-source/publications/2022/11/artificial-intelligence-in-economic-policymaking/222_psu_artificial-intelligence-in-economic-policymaking.pdf?sfvrsn=341777ad_2, último acceso de 28 de marzo 2024).

29 Ministerio de Comercio e Industria de Singapur "The Singapore-Australia Digital Economy Agreement (SADEA)" (disponible en https://www.dfat.gov.au/sites/default/files/australia-singapore-digital-economy-agreement.pdf, último acceso de 28 de marzo 2024).

30 Apec Business Advisory Council: "Snapshot of Domestic AI Strategies, Agencies, and Initiatives" (disponible en https://aiinapec.info/snapshot-of-domestic-ai-strategies-agencies-and-initiatives/ último acceso de 28 de marzo 2024).

31 Apec: "What is the Cross-Border Privacy Rules System" (disponible enhttps://www.apec.org/about-us/about-apec/fact-sheets/what-is-the-cross-border-privacy-rules-system último acceso de 28 de marzo 2024).

de datos personales y en los numerosos intentos de reforma legislativa a dichos marcos jurídicos[32].

A nivel de otras instancias transnacionales, destaca el caso de la Red Iberoamericana de Protección de Datos (RIPD)[33]. La RIPD es una instancia de cooperación y diálogo de aquellas entidades públicas con competencias para "promover, impulsar y tomar decisiones en materia de protección de datos personales en sus respectivos países", junto a observadores e invitados[34]. Como tal, es una de las entidades internacionales que, sin ser un organismo internacional, permite la convergencia entre estándares europeos y latinoamericanos de protección de datos personales. Dentro de sus funciones se encuentra brindar asistencia técnica y transferencia de conocimientos tecnológicos a sus integrantes (RIPD, art. 1, letra c), lo que funda la generación de estándares y directrices. En materia de IA, la RIPD ha publicado dos documentos relevantes: las "Recomendaciones generales para el tratamiento de datos en inteligencia artificial"[35] y la "Declaración sobre neurodatos de la RIPD"[36]. El primer documento es uno de los pocos instrumentos de soft law que es específico sobre IA, aunque aplicado al tratamiento de datos personales. Si bien son unas meras recomendaciones, su contenido dialoga con el marco europeo del RGPD y los lineamientos del Grupo de Trabajo del Artículo 29, en materia de decisiones automatizadas[37], entre otros instrumentos europeos. Un paso más allá es la Declaración sobre neurodatos que, en línea con el CIJ de la OEA, fijando directrices genéricas sobre la protección de la autodeterminación informativa y de la privacidad en materia de neurotecnologías.

Por último, ministros de Estado de países de América Latina y el Caribe, recientemente, han emitido la "Declaración de Santiago para promover una inteligencia artificial en América Latina y el Caribe"[38]. El documento ha sido

32 Greenleaf, G.: "Five years of the APEC Privacy Framework: Failure or promise?", *Computer Law & Security Review*, vol. 25, núm. 1, 2009, pp. 28-43. Véase también, en clave comparativa con el RGPD, Sullivan, C.: "EU GDPR or APEC CBPR? A comparative analysis of the approach of the EU and APEC to cross border data transfers and protection of personal data in the IoT era", *Computer Law & Security Review*, vol. 35, núm.4, 2019, pp. 380-397.

33 Véase, Red Iberoamericana de Protección de Datos: "Historia". (disponible en https://www.redipd.org/es/la-red/historia-de-la-red-iberoamericana-de-proteccion-de-datos-ripd, último acceso de 28 de marzo 2024).

34 Red Iberoamericana de Protección de Datos: "Reglamento de la Red Iberoamericana de Protección de Datos (RIPD)", Artículos 2-5 (disponible en https://www.redipd.org/sites/default/files/2019-11/reglamento-ripd.pdf, último acceso de 28 de marzo 2024).

35 Red Iberoamericana de Protección de Datos: "Recomendaciones generales para el tratamiento de datos en la Inteligencia Artificial" (disponible en https://www.redipd.org/sites/default/files/2020-02/guia-recomendaciones-generales-tratamiento-datos-ia.pdf, último acceso de 28 de marzo 2024).

36 Red Iberoamericana de Protección de Datos: "Declaración sobre neurodatos de la RIPD" (disponible en https://www.redipd.org/sites/default/files/2023-10/declaracion-neurodatos-ripd.pdf, último acceso de 28 de marzo 2024).

37 Red Iberoamericana de Protección de Datos: "Recomendaciones generales", cit.

38 Cumbre Ministerial de Altas Autoridades de América Latina y el Caribe: "Declaración de Santiago. 'Para promover una inteligencia artificial ética en América Latina y el Caribe'" (disponible en https://minciencia.gob.cl/uploads/filer_public/40/2a/402a35a0-1222-4dab-b090-5c81bbf34237/declaracion_de_santiago.pdf, último acceso de 28 de marzo 2024).

promovido a instancias de UNESCO y de la CAF y constituyó un Grupo de Trabajo para generar un "Consejo intergubernamental de Inteligencia Artificial para América Latina y el Caribe, en el marco de la Recomendación sobre la Ética de la IA de la UNESCO, con el propósito de fortalecer las capacidades regionales en la materia"[39]. Como instrumento es meramente declarativo, sin pretensiones mayores de normatividad, pero busca alinear objetivos para una acción estatal conjunta en materia de ética e IA.

3. Estrategias nacionales y normativas domésticas.

En un tercer nivel, encontramos las estrategias o políticas nacionales en materia IA. A partir de una reconstrucción de la información recabada en fuentes primarias de los Estados y con base al Índice Latinoamericano de Inteligencia Artificial 2023[40], un instrumento único en su clase. El índice contiene una revisión de doce países de la región y detalla los hallazgos en distintas dimensiones: factores habilitantes como entorno para la IA, de investigación, desarrollo y adopción de IA y de gobernanza, además de medir la percepción pública sobre la IA[41]. Para efectos de este trabajo, hemos restringido el análisis a una muestra de los países latinoamericanos que forman parte de la OCDE, esto es, Brasil, Chile, Colombia, Costa Rica, México, más los países invitados de la región, como Argentina y Perú[42]. Conforme a los cuatro criterios del indicador de gobernanza de IA, de acuerdo con CENIA, es posible resumir la información de la siguiente forma.

A) Argentina.

Es un país invitado de la OCDE. En la dimensión de "Estrategia Nacional", Argentina cuenta con un documento marco con participación ciudadana. De acuerdo con CENIA, el país además cuenta con instituciones "dedicadas a este propósito y se reconocen las competencias y capacidades de los organismos encargados de impulsar iniciativas relacionadas con la IA en el país"[43]. El país carece de una regulación general de la IA, pese a que existen proyectos en curso, como se explica en infra. Finalmente, Argentina no registra experiencias de experimentación regulatoria.

B) Brasil.

Es uno d ellos países con mayor índice de gobernanza de la IA en la región, puesto que cuenta con una estrategia nacional, instituciones con competencias en

39 Cumbre Ministerial de Altas Autoridades de América Latina y el Caribe: "Declaración de Santiago", cit., p. 4.

40 Cenia: "Índice Latinoamericano de Inteligencia artificial 2023" (disponible en https://indicelatam.cl/wp-content/uploads/2023/09/ILIA-ESP_compressed.pdf, último acceso de 28 de marzo 2024).

41 Cenia: "Índice Latinoamericano", cit., pp. 7-15.

42 Para el listado de países miembros e invitados, véase OCDE, Disponible en: https://www.oecd.org/acerca/, visitado el día 8 de abril de 2024.

43 Cenia: "Índice Latinoamericano", cit., p. 189.

materia de IA y alternativas de experimentación regulatoria[44]. Si bien no cuenta con una regulación general de la IA, sí participa activamente en la regulación internacional en comité internacionales y además cuenta con legislaciones sectoriales o específicas, como su marco regulatoria en protección de datos personales, como se explica más abajo.

C) Chile.

Chile cuenta con un desempeño destacado en gobernanza de la IA en la región, al tener una estrategia nacional desarrollada con mecanismos de participación y con institucionalidad a cargo de la coordinación en la materia[45]. No tiene una legislación general sobre la IA –pese a tener leyes específicas e importantes reformas en curso– y carece de mecanismos de experimentación regulatoria o sandboxes.

D) Colombia.

Colombia carece de una estrategia nacional vigente y no cuenta con instituciones con competencias definidas para hacerse cargo de la IA. En materia regulatoria, no tiene una legislación general de la IA pero sí cuenta con leyes especiales en protección de datos y ciberseguridad y, además, de mecanismos de experimentación regulatoria[46].

E) Costa Rica.

Costa Rica también carece de una estrategia nacional, aunque recientemente ha impulsado un proceso de consulta para un documento marco al respecto[47]. Si bien no cuenta con instituciones competentes a cargo conforme al índice, la consulta pública de la estrategia es llevada por el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones. El país carece de una regulación general de la IA pero cuenta con normativas específicas en materia de protección de datos y ciberseguridad y existen iniciativas de experimentación regulatoria[48].

44 Cenia: "Índice Latinoamericano", cit., p. 199.

45 Cenia: "Índice Latinoamericano", cit., p. 204.

46 Cenia: "Índice Latinoamericano", cit., p. 209.

47 Véase Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones de Costa Rica: "Estrategia Nacional de Inteligencia Artificial 2024-2027" (disponible en https://www.micitt.go.cr/sites/default/files/transparencia/consulta-publica/Estrategia%20Nacional%20de%20Inteligencia%20Artificial%20%28Version%2021.03.24%29%20Para%20consulta%20pública.pdf, último acceso de 28 de marzo 2024).

48 Cenia: "Índice Latinoamericano", cit., p. 214.

F) México.

México carece de una estrategia nacional de IA vigente, pese a los esfuerzos multisectoriales que se han llevado a cabo[49]. También carece de instituciones con competencia en la materia y con una regulación general, pese a que cuenta con normativas específicas en protección de datos personales[50]. Además presenta un caso de experimentación regulatoria, junto al Banco Interamericano de Desarrollo, en materia de transparencia y explicabilidad de la IA[51].

G) Perú.

Perú cuenta con una estrategia nacional vigente e instituciones competentes a cargo de la materia. Si bien carece de una regulación general, su marco regulatorio contempla normativas en protección de datos personales y ciberseguridad[52]. Perú carece de experiencias de experimentación regulatoria.

H) Balance.

A nivel de los países seleccionados, la mayoría de los Estados cuentan con una estrategia o política nacional de IA. Como tal, dichos documentos no fijan más que un posible horizonte regulatorio pero en caso alguno pueden ser considerados fuentes formales de derecho. Al contrario, son un instrumento de política a efectos de generar el alineamiento entre los objetivos declarados de cada Estado, con relación a la IA, una detección preliminar de brechas que deben ser resueltas por la acción estatal y la priorización de líneas de acción. Sin embargo, las estrategias o políticas nacionales también conectan valores generales o principios sobre los que debe orientarse la acción estatal, lo que puede permitir, eventualmente, una directriz ética o normativa en el desarrollo y evaluación de sistemas de IA[53].

Desde el punto de vista de la regulación de la IA, ningún Estado cuenta con una ley o normativa general sobre el uso de sistemas de IA. Sin embargo, actualmente existen diversos proyectos en curso, como en México, Argentina, Brasil o Chile[54]. Esto no es más que una manifestación de una tendencia mundial. Un análisis de

49 Véase IA2030Mx: "Agenda Nacional Mexicana de Inteligencia Artificial" (disponible en https://www.ia2030.mx/agenda2020, último acceso de 28 de marzo 2024).

50 Cenia: "Índice Latinoamericano", cit., p. 224.

51 Cenia: "Índice Latinoamericano", cit., p. 224.

52 CENIA: "Índice Latinoamericano", cit., p. 239.

53 En el caso de Chile, la Política Nacional de Inteligencia Artificial comprende un eje sobre "Ética, Aspectos Legales y Regulatorios e Impactos Socioeconómicos". Ministerio de Ciencia, Tecnología, Conocimiento e Innovación de Chile: "Política Nacional de Inteligencia Artificial" (disponible en https://www.minciencia.gob.cl/areas/inteligencia-artificial/politica-nacional-de-inteligencia-artificial/, último acceso de 28 de marzo 2024), pp. 49 y ss.

54 Para un mapeo de los intentos regulatorios de la región, actualizado al 23 de febrero de 2024, véase Gutiérrez, J.D.: "Regulación sobre IA" (disponible en https://forogpp.com/inteligencia-artificial/regulacion-sobre-ia/, último acceso de 28 de marzo 2024).

los registros parlamentarios sobre IA en 81 países muestra igualmente que las menciones a la IA en los procedimientos legislativos mundiales han aumentado casi 6,5 veces desde 2016[55]. Los proyectos de ley, en los países seleccionados de América Latina, corresponden a iniciativas legislativas de congresistas y no de los Ejecutivos. Por lo tanto, son iniciativas fragmentarias y que no necesariamente se encuentran alineadas a la estrategia o política nacional de cada país. El enfoque de los proyectos es distinto. Mientras los casos de Brasil y Chile buscan adoptar un enfoque de riesgos importado del borrador del Reglamento Europeo de IA (AIA por sus siglas en inglés)[56], en Argentina, el proyecto de ley contempla reglas generales de definición de la IA, algunos principios y la regulación de materias específicas, como el uso de la IA en educación[57].

A nivel de la regulación sectorial o específica, el principal fenómeno responde a las reformas de las leyes de protección de datos personales en la región, orientadas a los estándares definidos por el RGPD. En esto, el "efecto Bruselas" es particularmente claro[58] y cómo el RGPD se está convirtiendo en el "golden standard" en materia de protección de datos personales[59]. Dicho efecto se entiende como el poder unilateral que tiene la Unión Europea para regular mercados globales[60]. En materia digital, su impacto e influencia afecta países de todos los continentes y con distintos sistemas jurídicos[61].

En Latinoamérica, el caso más relevante es la Ley No. 13.709/2018, General de Protección de Datos Personales de Brasil[62]. Brasil, actualmente, se encuentra en proceso para ser reconocido como país adecuado bajo el RGPD de la UE[63]. En el caso chileno, la reforma a la ley de protección de datos personales sigue el

55 Stanford University Human-Centered Artificial Intelligence: "Artificial Intelligence Index Report 2023" (disponible en https://aiindex.stanford.edu/wp-content/uploads/2023/04/HAI_AI-Index-Report_2023.pdf, último acceso de 28 de marzo 2024).

56 Parlamento Europeo: "Resolución legislativa del Parlamento Europeo, de 13 de marzo de 2024, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD))" (disponible en https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_ES.html, último acceso de 28 de marzo 2024).

57 En el caso de Brasil, véase el Projeto de Lei nº 2338/2003, que que dispõe sobre o uso da Inteligência Artificial y en el caso de Chile, véase el proyecto de ley Boletín No. 15.869-19, que regula los sistemas de inteligencia artificial, la robótica y las tecnologías conexas en sus distintos ámbitos de aplicación.

58 Bradford, A.: *Brussels Effect: How the European Union Rules the World*, Oxford University Press, Oxford, 2020.

59 Buttarelli, G. "The EU GDPR as a clarion call for a new global digital gold standard", *International Data Privacy Law*, vol. 6, núm 2, 2016, pp. 77-78.

60 Bradford, A.: "Brussels Effect", cit., p. 14.

61 Fahey, E.: *The EU as a Global Digital Actor. Institutionalising Global Data Protection, Trade, and Cibersecurity*, Hart Publishing, Oxford, 2022.

62 Lamounier Heringer, H.M.: "La Autoridad Nacional de Protección de Datos bajo la perspectiva del análisis costo-beneficio", *Revista de Derecho Público*, núm. 98, 2023, pp. 66 y ss.

63 Bordachar, M.: "Comentarios al proyecto de ley chileno sobre protección de datos personales: deficiencias e inconsistencias en los derechos ARCO", *Revista chilena de derecho y tecnología*, 11(1), pp. 395–412.

mismo rumbo[64], con la presencia de agentes de la UE durante la tramitación ante el Congreso Nacional[65]. La influencia de este tipo de normativas tiene impacto en la regulación de la IA. El caso más relevante es el trasplante del art. 22 RGPD, sobre derechos de los titulares de datos frente a sistemas de toma de decisiones automatizadas[66]. En el caso de Brasil, corresponde al art. 20[67] y en el caso de Chile, se encontraría en el art. 8bis del proyecto de ley[68].

Pero, además, y como peculiaridad regional, los Estados están avanzando al reconocimiento doméstico de los denominados "neuroderechos". El primer caso sería el de Chile, con la constitucionalización de una regla especial relativa a la investigación científica y a la protección de la actividad cerebral[69]. Es discutible que la disposición consagre un "neuroderecho"[70] y el único caso en que se ha citado la disputa se resolvió sobre la base de los deberes estatales frente a la importación de ciertos dispositivos considerados como "médicos" por la Corte Suprema[71]. Lo interesante de este caso no es su novedad –destacada por la literatura– sino el tipo de exportación que está generando en países como Brasil y México, cuyos legisladores buscan reformar sus constituciones y consagrar una variante de la norma constitucional chilena[72].

64 Boletín 11.144-07 y su tramitación (disponible en: https://www.camara.cl/pley/pley_detalle.aspx?prmID=11661&prmBoletin=11144-07, último acceso de 28 de marzo 2024).

65 Por ejemplo, con la asistencia de Bruno Gencarelli, Head of the International Data Flows and Protection Unit. European Commission, a lo largo de la tramitación. Véase, respecto del Senado, en https://www.senado.cl/appsenado/index.php?mo=comisiones&ac=sesiones_celebradas&idcomision=186&tipo=3&legi=485&ano=2018&desde=0&hasta=0&idsesion=12513&idpunto=15909&listado=2 y en el caso de la Cámara de Diputados https://www.camara.cl/legislacion/comisiones/resultados_semana.aspx?prmSemana=2022-39.

66 Véase https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm.

67 Boletín 11.144-07 y su tramitación (disponible en: https://www.camara.cl/pley/pley_detalle.aspx?prmID=11661&prmBoletin=11144-07, último acceso de 28 de marzo 2024).

68 Viollier, P. & Fischer, E.: "La intervención humana como resguardo ante la toma automatizada de decisiones: implicancias éticas y jurídicas", en AA.VV.: *Introducción a la Ética y el Derecho de la Inteligencia Artificial* (ed. por M. Azuaje), Wolters Kluwer – La Ley, Madrid, 2023, pp. 151-169.

69 Dicha cláusula se encuentra recogida en el artículo 19 No. 1, inc. final de la Constitución chilena y fue introducida mediante reforma constitucional (Ley No. 21.383, de 25 de octubre de 2021). El precepto constitucional dispone: "El desarrollo científico y tecnológico estará al servicio de las personas y se llevará a cabo con respeto a la vida y a la integridad física y psíquica. La ley regulará los requisitos, condiciones y restricciones para su utilización en las personas, debiendo resguardar especialmente la actividad cerebral, así como la información proveniente de ella […]".

70 Paredes, F. & Quiroz, C.: "Neuroderechos en Chile: Estado del arte y desafíos", en AA.VV.: *Neurodireito, neurotecnologia e direitos humanos* (org. por A. D'Ávila Lopes *et al.* (org.)) Livraria do Advogado, Porto Alegre, 2022; Contreras, P. "¿Qué decidió la Corte Suprema en el denominado caso de los 'neuroderechos' (*Girardi vs. Emotiv*)?", en AA.VV.: *En defensa de los neuroderechos* (ed. por M. Sánchez *et al.*), Kamanau, Santiago (disponible en https://defensaneuroderechos.org/, último acceso de 28 de marzo 2024).

71 Sentencia de la Corte Suprema de Chile, Rol 10.5065-2023, *Girardi vs. Emotiv*, 09 de agosto de 2023 (en adelante, "SCS, R. 10.5065-2023").

72 Para una panorámica al respecto, véase Do, B. *et al.*: "Privacy and the future of 'neurorights' in Latin America", (disponible en https://fpf.org/blog/privacy-and-the-rise-of-neurorights-in-latin-america/, último acceso de 28 de marzo 2024); Cámara de Diputados de México: "México se une a la tendencia internacional por una legislación a favor de los neuroderechos: María Eugenia Hernández" (disponible en https://comunicacionsocial.diputados.gob.mx/index.php/notilegis/mexico-se-une-a-la-tendencia-internacional-por-una-legislacion-a-favor-de-los-neuroderechos-maria-eugenia-hernandez, último acceso de 28 de marzo 2024); Cámara de Diputados de Brasil: "Proyecto de ley No. 522/2022. Modifica a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), a fim de conceituar dado neural e regulamentar a sua

III. ¿CONVERGENCIA O CAMINO PROPIO?

El panorama latinoamericano ofrece distintos vectores para la gobernanza de la IA. Observando algunas de las trayectorias, parece existir una tendencia a la convergencia con estándares internacional, especialmente respecto de Europa. Si bien no existen tratados internacionales aplicables o instrumentos de soft law directamente relacionados con la regulación de la IA, los incipientes pasos de la región se mueven a la apertura respecto de los órganos internacionales y de la actividad normativa de la Unión Europea.

En términos de convergencia regulatoria, es posible considerar los siguientes factores que se sintetizan a continuación. En primer término, a nivel universal, la región se inserta en el trabajo de organismos como Naciones Unidas y UNESCO. Respecto del primero, la reciente resolución de la Asamblea General fue ampliamente apoyada por Estados latinoamericanos[73] y fija un horizonte de soft law coherente con las estrategias regulatorias domésticas de estos países. Otro tanto ocurre con las colaboraciones junto a UNESCO. La Declaración de Santiago es un tímido paso multilateral que busca alinear un trabajo conjunto a nivel de desarrollo de directrices éticas y marcos para la formulación de políticas públicas.

Desde el punto de vista del efecto "Bruselas", los esfuerzos todavía son fragmentarios y se ubican principalmente en regulaciones anexas a la IA, como la protección de datos personales. Quizás los ejemplos más notables se observan en cómo se expande la influencia del RGPD y su impacto en estas normativas en la región. Los casos de Brasil –con la Ley No. 13.709/2018– y de Chile –con el proyecto de ley Boletín 11144-07– son los más significativos, pero con otras iniciativas en curso en el mismo sentido[74]. El soft law regional en protección de datos se observa principalmente a raíz de lo impulsado por la OEA y la RIPD.

Ahora bien, con la aprobación del Parlamento Europeo del Reglamento Europeo de Inteligencia Artificial[75] ("AIA", por sus siglas en inglés), los proyectos

proteção" (disponible enhttps://www.camara.leg.br/propostas-legislativas/2317524, último acceso de 28 de marzo 2024). En términos de procesos de integración regional, el Parlamento Latinoamericano y Caribeño ha adoptado una "Ley Modelo de Neuroderechos para América Latina y el Caribe". Véase Parlatino: "Ley Modelo de Neuroderechos para América Latina y el Caribe" (disponible en https://parlatino.org/wp-content/uploads/2017/09/leym-neuroderechos-7-3-2023.pdf, último acceso de 28 de marzo 2024). En clave crítica, véase Borbón, D. *et al.*: "El preocupante clausulado de la Ley Modelo de Neuroderechos del Parlatino", *IUS ET SCIENTIA*, vol. 9, núm. 2, 2023, pp. 228–260.

73 Para el detalle de los promotores y patrocinadores, véase Naciones Unidas: "Seizing the opportunities", cit.

74 Por ejemplo, en el caso de Argentina, con el Mensaje 87/2023 como Proyecto de Ley de Protección de Datos Personales, cuyo informe de elaboración del anteproyecto declara la influencia del RGPD. Véase Acceso a la Información Pública de Argentina: "Informe sobre el proceso de elaboración participativa de normas en relación al anteproyecto de Ley de Protección de Datos Personales" (disponible en https://www.argentina.gob.ar/sites/default/files/informe_consulta_publica_aaip.pdf, último acceso de 28 de marzo 2024), pp. 2-8 (declarando el "especial interés a la preservación de la categoría de país adecuado de la República Argentina por parte de la Unión Europea").

75 Parlamento Europeo: "Resolución legislativa", cit.

de ley en curso en Chile podría tener la influencia del nuevo marco europeo. Algunos de ellos –nuevamente el de Brasil y Chile– ya tienen una inspiración basada en el enfoque de riesgos regulatorios, pero es posible conjeturar que, tras la cristalización del texto final de AIA la tramitación legislativa tenga cambios para converger con su contenido.

A nivel de caminos propios, existen estrategias unilaterales que dependen de las relaciones internacionales de cada país. Por ejemplo, el DEPA es un ejemplo de la apertura de Chile hacia el Asia-Pacífico y el tipo de regulación de la IA es de una naturaleza *sui generis* que no se observa en el resto del panorama comparado. Otro tanto son los esfuerzos de Brasil en el marco de BRICS[76], con el anuncio de un grupo de estudio sobre IA[77].

Una de las peculiaridades de la región estriba en la activa promoción de los denominados "neuroderechos". Tanto a nivel de soft law regional como en las normativas domésticas, existe un impulso inicial en regular neuro tecnologías que podrían afectar derechos fundamentales. El germen de esta actividad regulatoria se encuentra en la reforma constitucional chilena ya referida y su posterior exportación a proyectos legislativos en México y Brasil[78]. Además, tanto la OEA como la RIPD han adoptado instrumentos de recomendaciones aplicables a las neuro tecnologías.

IV. CONCLUSIONES.

La regulación e la IA, en América Latina, sigue siendo una asignatura incipiente. Las condiciones de cooperación regional no generan incentivos correctos para integración regulatoria y sólo se observan tímidos esfuerzos conjuntos, entre los Estados, que permitan superar los dilema de acción colectiva y los costos de transacción asociados a la gobernanza y regulación de este tipo de tecnologías.

En el panorama bosquejado en este trabajo, se examinaron tres niveles de regulación sobre IA en países latinoamericanos. En primer término, a nivel de tratados internacionales, no existen instrumentos o iniciativas que regulen la IA o cuyo desarrollo puede ser normado. Con relación al soft law, es posible

76 Véase en general, Cyman, D. *et al.*: "Regulation of Artificial Intelligence in BRICS and the European Union", *BRICS Law Journal*, vol. 8, núm. 1, 2021, pp. 86-115; Belli, L.: "New Data Architectures in Brazil, China, and India: From Copycats to Innovators, Towards a post-Western Model of Data Governance", *The Indian Journal of Law and Technology*, vol. 18, 2022, pp. 1-58.

77 Embassy of China in India "Seeking development through solidarity and cooperation and shouldering our responsibility for peace" (disponible en http://in.china-embassy.gov.cn/eng/zgxw/202308/t20230823_11130928.htm#:~:text=BRICS%20countries%20have%20agreed%20to,information%20exchange%20and%20technological%20cooperation., último acceso de 28 de marzo 2024); Digwatch: "BRICS announces formation of AI study group", (disponible en https://dig.watch/updates/brics-members-announce-formation-of-ai-study-group, último acceso de 28 de marzo 2024).

78 Do, B. *et al.*: "Privacy and the future", cit.

identificar algunos instrumentos relativos a la protección de datos personales y los "neuroderechos", ambas temáticas que se intersectan con la IA. Finalmente, en el plano de las estrategias nacionales y normativas domésticas, en los países seleccionados es posible identificar un surgimiento de políticas estrategias nacionales y, además, normativas específicas en protección de datos y ciberseguridad. En esto, además, se puede constatar un acotado efecto "Bruselas" en la última generación de normas sobre protección de datos personales.

Los proyectos de ley que buscan regular, de forma general, a la IA pueden tener un giro con la aprobación de la AIA. Esto abre un espacio para investigaciones futuras. Sin embargo, sin cambios estructurales en la cooperación, la opción por convergencia internacional o por los caminos propios seguirá el derrotero de la iniciativa de cada Estado, privilegiando sus normativas domésticas en la regulación de estas tecnologías.

BIBLIOGRAFÍA

Acceso a la Información Pública de Argentina: "Informe sobre el proceso de elaboración participativa de normas en relación al anteproyecto de Ley de Protección de Datos Personales" (disponible en https://www.argentina.gob.ar/sites/default/files/informe_consulta_publica_aaip.pdf, último acceso de 28 de marzo 2024).

Affonso Souza, C. *et al*.: "From privacy to data protection: the road ahead for the Inter-American System of human rights", *The International Journal of Human Rights*, vol. 25, núm. 1, 2020.

Aguilar Cavallo, G. & Sandoval, M.I.: "La protección de datos personales en un contexto digital desde los estándares de la Corte Interamericana de Derechos Humanos", en A.A.VV.: *Derecho digital y privacidad en América y Europa. Perspectiva chilena y comparada* (ed. C. Droguett González & N. Walker Silva), Tirant lo Blanch, Valencia, 2023.

Apec: "What is the Cross-Border Privacy Rules System" (disponible en https://www.apec.org/about-us/about-apec/fact-sheets/what-is-the-cross-border-privacy-rules-system último acceso de 28 de marzo 2024).

Apec Business Advisory Council: "Trust: Providing a framework for ethical AI" (disponible en https://aiinapec.info/trust-providing-a-framework-for-ethical-ai-2/ último acceso de 28 de marzo 2024).

Apec Business Advisory Council: "Snapshot of Domestic AI Strategies, Agencies, and Initiatives" (disponible en https://aiinapec.info/snapshot-of-domestic-ai-strategies-agencies-and-initiatives/ último acceso de 28 de marzo 2024).

Arun, C.: "AI and the Gobal South: Designing for other Worlds", en AA.VV.: *The Oxford Handbook of Ethics of AI* (ed. por M. Dubber *et al*), Oxford University Press, Oxford, 2020.

Arvidsson, M. & Noll, G.: "Artificial Intelligence, Decision Making and International Law", *Nordic Journal of International Law*, vol. 92, 2023, pp. 1-8.

Belli, L.: "New Data Architectures in Brazil, China, and India: From Copycats to Innovators, Towards a post-Western Model of Data Governance", *The Indian Journal of Law and Technology*, vol. 18, 2022, pp. 1-58.

Bertoni, E.: "Convention 108 and the GDPR: Trends and perspectives in Latin America", *Computer Law & Security Review*, vol. 40, 2021.

Borbón, D. *et al.*: "El preocupante clausulado de la Ley Modelo de Neuroderechos del Parlatino", *IUS ET SCIENTIA*, vol. 9, núm. 2, 2023, pp. 228–260.

Bordachar, M.: "Comentarios al proyecto de ley chileno sobre protección de datos personales: deficiencias e inconsistencias en los derechos ARCO", *Revista chilena de derecho y tecnología*, 11(1), pp. 395–412.

Bradford, A.: *Brussels Effect: How the European Union Rules the World*, Oxford University Press, Oxford, 2020.

Buttarelli, G. "The EU GDPR as a clarion call for a new global digital gold standard", *International Data Privacy Law*, vol. 6, núm 2, 2016.

Cai: "Revised Zero Draft [Framework] Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law" (disponible en https://rm.coe.int/cai-2023-01-revised-zero-draft-framework-convention-public/1680aa193f, último acceso de 28 de marzo 2024).

Cai: "CAI – Committee on Artificial Intelligence" (disponible en https://www.coe.int/en/web/artificial-intelligence/cai, último acceso de 28 de marzo 2024).

Cámara de Diputados de Brasil: "Proyecto de ley No. 522/2022. Modifica a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), a fim de conceituar dado neural e regulamentar a sua proteção" (disponible en https://www.camara.leg.br/propostas-legislativas/2317524, último acceso de 28 de marzo 2024).

Cámara de Diputados de México: "México se une a la tendencia internacional por una legislación a favor de los neuroderechos: María Eugenia Hernández" (disponible en https://comunicacionsocial.diputados.gob.mx/index.php/notilegis/mexico-se-une-a-la-tendencia-internacional-por-una-legislacion-a-favor-de-los-neuroderechos-maria-eugenia-hernandez, último acceso de 28 de marzo 2024).

Cenia: "Índice Latinoamericano de Inteligencia artificial 2023" (disponible en https://indicelatam.cl/wp-content/uploads/2023/09/ILIA-ESP_compressed.pdf, último acceso de 28 de marzo 2024).

Cicr: "Armas autónomas: el CICR insta a los Estados a avanzar hacia la negociación de un tratado", (disponible en https://www.icrc.org/es/document/armas-autonomas-el-cicr-insta-los-estados-avanzar-hacia-la-negociacion-de-un-tratado, último acceso de 28 de marzo 2024).

Ciuriak, D. & Fray, R.: "The Digital Economy Partnership Agreement. Should Canada Join?", *Centre for International Governance Innovation Policy* Brief, núm 171,

2022 (disponible en https://www.cigionline.org/static/documents/PB_no.171.pdf, último acceso de 28 de marzo 2024).

Clarke, R.: "Regulatory alternatives for AI", *Computer Law & Security Review*, vol. 35, núm 4, 2019, pp. 398-409.

Comisión Interamericana de Derechos Humanos: "La CIDH y su RELE llaman a los Estados a adoptar medidas para reducir las brechas digitales de las personas mayores", (disponible en https://www.oas.org/es/cidh/jsForm/?File=/es/cidh/prensa/comunicados/2021/259.asp, último acceso de 28 de marzo 2024).

Comisión Interamericana de Derechos Humanos: "Pandemia y derechos humanos en las Américas" (disponible en https://www.oas.org/es/cidh/informes/pdfs/2023/PandemiaDDHH_ES.pdf, último acceso de 28 de marzo 2024).

"Principios actualizados sobre la privacidad y la protección de datos personales", (disponible en https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf, último acceso de 28 de marzo 2024).

Comité Jurídico Interamericano: "Declaración de Principios interamericanos en materia de Neurociencias, Neurotecnologías y Derechos Humanos", OEA/Ser. Q. CJI/RES. 281 (CII-O/23) corr. 1. (disponible en https://www.oas.org/es/sla/cji/docs/CJI-RES_281_CII-O-23_corr1_ESP.pdf, último acceso de 28 de marzo 2024).

Consejo de Europa: "Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos Personales (Convenio núm. 108)", Estrasburgo, Francia. 28 de enero de 1981, entró en vigor el 1 de octubre de 1985.

Consejo de Europa: "Protocolo del Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos Personales, relativo a la modernización del Convenio 108 (Convenio 108+)", Estrasburgo, Francia. Firmado el 10 de octubre de 2018.

Contreras, P. "¿Qué decidió la Corte Suprema en el denominado caso de los 'neuroderechos' (*Girardi vs. Emotiv*)?", en AA.VV.: *En defensa de los neuroderechos* (ed. por M. Sánchez *et al.*), Kamanau, Santiago (disponible en https://defensaneuroderechos.org/, último acceso de 28 de marzo 2024).

Contreras, P. & Trigo, P.: "La gobernanza de la inteligencia artificial. Esbozo de un mapa entre *hard law* y *soft law* internacional", en AA.VV.: *Inteligencia artificial y derecho* (ed. por M. Azuaje & P. Contreras), Tirant lo Blanch, Valencia, 2021, pp. 457-477.

Corte Interamericana de Derechos Humanos: "Declaración de la Corte Interamericana de Derechos Humanos 1/20. Covid-19 y derechos humanos: los problemas y desafíos deben ser abordados con perspectiva de derechos humanos y respetando las obligaciones internacionales" (disponible en https://www.corteidh.or.cr/tablas/alerta/comunicado/declaracion_1_20_ESP.pdf, último acceso de 28 de marzo 2024).

Cumbre Ministerial de Altas Autoridades de América Latina y el Caribe: "Declaración de Santiago. 'Para promover una inteligencia artificial ética en América Latina y el Caribe'" (disponible en https://minciencia.gob.cl/uploads/filer_public/40/2a/402a35a0-1222-4dab-b090-5c81bbf34237/declaracion_de_santiago.pdf, último acceso de 28 de marzo 2024).

Cyman, D. *et al.*: "Regulation of Artificial Intelligence in BRICS and the European Union", *BRICS Law Journal*, vol. 8, núm. 1, 2021, pp. 86-115.

Digwatch: "BRICS announces formation of AI study group", (disponible en https://dig.watch/updates/brics-members-announce-formation-of-ai-study-group, último acceso de 28 de marzo 2024).

Do, B. *et al.*: "Privacy and the future of 'neurorights' in Latin America", (disponible en https://fpf.org/blog/privacy-and-the-rise-of-neurorights-in-latin-america/, último acceso de 28 de marzo 2024).

Embassy of China in India "Seeking development through solidarity and cooperation and shouldering our responsibility for peace" (disponible en http://in.china-embassy.gov.cn/eng/zgxw/202308/t20230823_11130928.htm#:~:text=BRICS%20countries%20have%20agreed%20to,information%20exchange%20and%20technological%20cooperation., último acceso de 28 de marzo 2024).

Fahey, E.: *The EU as a Global Digital Actor. Institutionalising Global Data Protection, Trade, and Cibersecurity*, Hart Publishing, Oxford, 2022.

Greenleaf, G.: "Five years of the APEC Privacy Framework: Failure or promise?", *Computer Law & Security Review*, vol. 25, núm. 1, 2009, pp. 28-43.

Greenleaf, G.: "The influence of European data privacy standards outside Europe: Implications for globalization of Convention 108", *International Data Privacy Law*, vol. 2, núm. 2, 2012, pp. 68-92.

Gutiérrez, J.D.: "Regulación sobre IA" (disponible en https://forogpp.com/inteligencia-artificial/regulacion-sobre-ia/, último acceso de 28 de marzo 2024).

IA2030Mx: "Agenda Nacional Mexicana de Inteligencia Artificial" (disponible en https://www.ia2030.mx/agenda2020, último acceso de 28 de marzo 2024).

Lamounier Heringer, H.M.: "La Autoridad Nacional de Protección de Datos bajo la perspectiva del análisis costo-beneficio", *Revista de Derecho Público*, núm. 98, 2023, pp. 61-77.

Lee, J.: *Artificial Intelligence and International* Law, Springer, Dordrecht, 2022.

Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones de Costa Rica: "Estrategia Nacional de Inteligencia Artificial 2024-2027" (disponible en https://www.micitt.go.cr/sites/default/files/transparencia/consulta-publica/Estrategia%20Nacional%20de%20Inteligencia%20Artificial%20%28Version%2021.03.24%29%20Para%20consulta%20pública.pdf, último acceso de 28 de marzo 2024).

Ministerio de Ciencia, Tecnología, Conocimiento e Innovación de Chile: "Política Nacional de Inteligencia Artificial" (disponible en https://www.minciencia.gob.cl/areas/inteligencia-artificial/politica-nacional-de-inteligencia-artificial/, último acceso de 28 de marzo 2024).

Ministerio de Comercio e Industria de Singapur "The Singapore-Australia Digital Economy Agreement (SADEA)" (disponible en https://www.dfat.gov.au/sites/default/files/australia-singapore-digital-economy-agreement.pdf, último acceso de 28 de marzo 2024).

Mendoza Enríquez, O.: "Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento", *IUS. Revista del Instituto de Ciencias Jurídicas de Puebla*, vol. 12, núm. 4, 2018, pp. 267-291.

Naciones Unidas: "Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development", Res. A/78/L.49.ES. (disponible en https://digitallibrary.un.org/record/4040897?v=pdf, último acceso de 28 de marzo 2024).

Organización de los Estados Americanos: *Convención Americana sobre Derechos Humanos*. Firmada el 22 de noviembre de 1969, entró en vigor el 18 de julio de 1978.

Paredes, F. & Quiroz, C.: "Neuroderechos en Chile: Estado del arte y desafíos", en AA.VV.: *Neurodireito, neurotecnologia e direitos humanos* (org. por A. D'Ávila Lopes *et al.* (org.)) Livraria do Advogado, Porto Alegre, 2022.

Parlamento Europeo: "Resolución legislativa del Parlamento Europeo, de 13 de marzo de 2024, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD))" (disponible en https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_ES.html, último acceso de 28 de marzo 2024).

Parlatino: "Ley Modelo de Neuroderechos para América Latina y el Caribe" (disponible en https://parlatino.org/wp-content/uploads/2017/09/leym-neuroderechos-7-3-2023.pdf, último acceso de 28 de marzo 2024).

Red Iberoamericana de Protección de Datos: "Historia". (disponible en https://www.redipd.org/es/la-red/historia-de-la-red-iberoamericana-de-proteccion-de-datos-ripd, último acceso de 28 de marzo 2024).

Red Iberoamericana de Protección de Datos: "Reglamento de la Red Iberoamericana de Protección de Datos (RIPD)", Artículos 2-5 (disponible en https://www.redipd.org/sites/default/files/2019-11/reglamento-ripd.pdf, último acceso de 28 de marzo 2024).

Red Iberoamericana de Protección de Datos: "Recomendaciones generales para el tratamiento de datos en la Inteligencia Artificial" (disponible en https://www.redipd.org/sites/default/files/2020-02/guia-recomendaciones-generales-tratamiento-datos-ia.pdf, último acceso de 28 de marzo 2024).

Red Iberoamericana de Protección de Datos: "Declaración sobre neurodatos de la RIPD" (disponible en https://www.redipd.org/sites/default/files/2023-10/declaracion-neurodatos-ripd.pdf, último acceso de 28 de marzo 2024).

Schaffer, G.: "Trade Law in a Data-Driven Economy. The Need for Modesty and Resilience", en AA.VV.: *Artificial Intelligence and International Economic Law. Disruption, Regulation, and Reconfiguration* (ed. por S. Peng *et al.*), Cambridge University Press, Cambridge, 2021.

Soprana, M.: "The Digital Economy Partnership Agreement (DEPA): Assessing the Significance of the New Trade Agreement on the Block", *Trade, Law and Development*, vol. XIII, núm. 1, 2021.

Terwangne, C.: "Council of Europe convention 108+: A modernised international treaty for the protection of personal data", *Computer Law & Security Review*, vol. 40, 2021.

STREINZ, T.: "International Economic Law's Regulation of Data as a Resource for the Artificial Intelligence Economy", en AA.VV.: *Artificial Intelligence and International Economic Law. Disruption, Regulation, and Reconfiguration* (ed. por S. PENG *et al.*), Cambridge University Press, Cambridge, 2021.

STANFORD UNIVERSITY HUMAN-CENTERED ARTIFICIAL INTELLIGENCE: "Artificial Intelligence Index Report 2023" (disponible en https://aiindex.stanford.edu/wp-content/uploads/2023/04/HAI_AI-Index-Report_2023.pdf, último acceso de 28 de marzo 2024).

SULLIVAN, C.: "EU GDPR or APEC CBPR? A comparative analysis of the approach of the EU and APEC to cross border data transfers and protection of personal data in the IoT era", *Computer Law & Security Review*, vol. 35, núm.4, 2019, pp. 380-397.

VIOLLIER, P. & FISCHER, E.: "La intervención humana como resguardo ante la toma automatizada de decisiones: implicancias éticas y jurídicas", en AA.VV.: *Introducción a la Ética y el Derecho de la Inteligencia Artificial* (ed. por M. AZUAJE), Wolters Kluwer – La Ley, Madrid, 2023, pp. 151-169.

WIRJO, A. *et al.*: "Artificial Intelligence in Economic Policymaking", *APEC Policy Brief*, núm. 52, 2022 (disponible en https://www.apec.org/docs/default-source/publications/2022/11/artificial-intelligence-in-economic-policymaking/222_psu_artificial-intelligence-in-economic-policymaking.pdf?sfvrsn=341777ad_2, último acceso de 28 de marzo 2024).

ZINGALES, N.: "A Stronger Right to Data Protection During Pandemics? Leveraging The American Convention of Human Rights Against Governmental Inaction: A Brazilian Case-Study", *Revista Brasileira De Direitos Fundamentais & Justiça*, vol. 14, núm. 43, 2021, pp. 427–462.

EL USO JURISDICCIONAL DE LA INTELIGENCIA ARTIFICIAL: HABILITACIÓN LEGAL, GARANTÍAS NECESARIAS Y LA SUPERVISIÓN POR EL CGPJ*

JURISDICTIONAL USE OF ARTIFICIAL INTELLIGENCE: LEGAL BASES AND NECESSARY GUARANTEES AND SUPERVISION BY THE CGPJ

Actualidad Jurídica Iberoamericana Nº 21, agosto 2024, ISSN: 2386-4567, pp. 494-527

* El presente estudio es resultado de investigación de los siguientes proyectos: MICINN Proyecto "Derechos y garantías públicas frente a las decisiones automatizadas y el sesgo y discriminación algorítmicas" 2023-2025 (PID2022-136439OB-I00) financiado por MCIN/AEI/10.13039/501100011033/; Proyecto "Algoritmic law" (Prometeo/2021/009, 2021-24 Generalitat Valenciana); "Algorithmic Decisions and the Law: Opening the Black Box" (TED2021-131472A-I00) y "Transición digital de las Administraciones públicas e inteligencia artificial" (TED2021-132191B-I00) del Plan de Recuperación, Transformación y Resiliencia. Estancia Generalitat Valenciana CIAEST/2022/1, Convenio de Derechos Digitales-SEDIA Ámbito 5 (2023/C046/00228673) y Ámbito 6. (2023/C046/00229475).

Lorenzo
COTINO
HUESO

ARTÍCULO RECIBIDO: 29 de mayo de 2023
ARTÍCULO APROBADO: 1 de julio de 2024

RESUMEN: El estudio apuesta por el potencial del uso jurisdiccional de la inteligencia artificial (IA), pero con suficientes garantías legales. El análisis se centra en la cobertura legal necesaria y variable en razón de los diferentes derechos concurrentes. Se subraya que el Reglamento de IA (RIA) de la UE no sirve como una habilitación legal. A partir de las exigencias constitucionales, se analiza la novedosa regulación de sistemas automatizados y de IA en el Real Decreto-ley 6/2023, que se considera insuficiente. Asimismo, también se analiza y valora la obligación de regular legalmente garantías, señalando la dificultad de regular garantías añadidas a las del RIA. Además, se propone una regulación de garantías basada en estándares comparados. Finalmente, se recuerdan las funciones de supervisión que tienen las autoridades de vigilancia según el RIA y se argumenta que solo el Consejo General del Poder Judicial (CGPJ) puede ser la autoridad de supervisión de los sistemas de IA jurisdiccionales de alto riesgo en España, debido tanto a su independencia como a la separación de poderes. Ni la Autoridad Española de Supervisión de la Inteligencia Artificial (AESIA) ni la Agencia Española de Protección de Datos (AEPD) cumplen con los requisitos necesarios para esta función en el ámbito jurisdiccional.

PALABRAS CLAVE: Inteligencia artificial; sistemas automatizados; protección de datos; uso justicia; Consejo General del Poder Judicial; legalidad.

ABSTRACT: *The study supports the potential for the jurisdictional use of artificial intelligence (AI), but with sufficient legal guarantees. The analysis focuses on the necessary and varying legal coverage due to different concurrent rights. It is stressed that the EU's AI Regulation does not serve as a legal enabling act. Based on the constitutional requirements, the new regulation of automated systems and AI in Royal Decree-Law 6/2023 is analysed, which is considered insufficient. It is also studied the obligation to regulate guarantees by law, pointing out the difficulty of regulating guarantees in addition to those of the RIA. Furthermore, a regulation of guarantees based on comparative standards is proposed. Finally, the supervisory functions of the authorities under the RIA are described and it is explained that only the General Council of the Judiciary (Consejo General del Poder Judicial) can be the supervisory authority for high-risk jurisdictional IA systems in Spain, due to its independence and the separation of powers. Neither the Spanish Artificial Intelligence Supervisory Authority (AESIA) nor the Spanish Data Protection Agency (AEPD) fulfil the necessary requirements for this role in the jurisdictional sphere.*

KEY WORDS: *Artificial intelligence; automated systems; data protection; justice; Consejo General del Poder Judicial; legality.*

SUMARIO.- I. HAY QUE ALLANAR EL TERRENO PARA LOS USOS JURISDICCIONALES DE LA INTELIGENCIA ARTIFICIAL, PERO CON GARANTÍAS.- II. LA NECESARIA REGULACIÓN POR LEY DEL USO JURISDICCIONAL DE SISTEMAS AUTOMATIZADOS Y DE INTELIGENCIA ARTIFICIAL.- 1. La variable cobertura legal para las actuaciones jurisdiccionales con sistemas automatizados.- 2. Una mayor cobertura legal si se utiliza inteligencia artificial.- 3. El reglamento IA no sirve como habilitación legal.- III. LA (INSUFICIENTE) HABILITACIÓN EN EL REAL DECRETO-LEY 6/2023: ORIENTACIÓN AL DATO Y ACTUACIONES AUTOMATIZADAS, PROACTIVAS Y ASISTIDAS PARA USO JURISDICCIONAL.- 1. La regulación en España de las actuaciones judiciales automatizadas, ahora con inteligencia artificial.- 2. La habilitación general casi en blanco del artículo 35 de "orientación al dato".- 3. Inteligencia artificial y actuaciones automatizadas, proactivas y asistidas.- IV. ADEMÁS, LA LEY DEBE REGULAR GARANTÍAS EN EL MARCO DEL RIA. UNA PROPUESTA.- 1. La regulación de garantías en el Real Decreto-Ley 6/2023 y su difícil conjunción con las del RIA.- 2. Una propuesta de regulación de garantías.- V. PARA TERMINAR: SÓLO EL CGPJ PUEDE SER LA AUTORIDAD DE SUPERVISIÓN DE LOS SISTEMAS DE IA JURISDICCIONALES DE ALTO RIESGO.- 1. Las autoridades de vigilancia del reglamento de IA y sus facultades.- 2. La AESIA no podría ser la autoridad de vigilancia para el ámbito judicial por falta de independencia.- 3. La AEPD tampoco puede ser la autoridad para la inteligencia artificial de uso jurisdiccional, sólo el CGPJ.

I. HAY QUE ALLANAR EL TERRENO PARA LOS USOS JURISDICCIONALES DE LA INTELIGENCIA ARTIFICIAL, PERO CON GARANTÍAS.

Las posibilidades de uso de sistemas automatizados, especialmente en el ámbito jurisdiccional, son enormes. Contamos con más de cien experiencias en Europa, aunque son esencialmente instrumentales y de gestión en justicia. [1] No obstante, se vislumbra un mayor potencial en Iberoamérica, especialmente de la mano del IALAB, [2] con experiencias como "Prometea" [3] y el JUSLAB en Argentina.

1 Cernada Badía, R.: "De la digitalización a la inteligencia artificial: el porvenir de la justicia en la Unión Europea", en AA.VV.: *Algoritmos abiertos y que no discriminen en el sector público* (coord. por L. Cotino Hueso y P. Simó Castellanos), Tirant lo Blanch, Valencia, 2023, pp. 239-264. Al respecto de casos de uso en justicia en la UE, Comisión Europea: *Study on the use of innovative technologies in the justice field – Final report*, Dirección General de Justicia y Consumidores Publications Office, Bruselas, septiembre de 2020, https://data.europa.eu/doi/10.2838/58510 Ver también, Comisión Europea: *Comunicación de la Comisión al Parlamento europeo, al Consejo, al Comité Económico y Social europeo y al Comité de las Regiones: La digitalización de la justicia en la UE: Un abanico de oportunidades* {SWD(2020) 540 final}, de 2 de diciembre de 2020.

2 Desde IALAB: *Directrices de uso de la IA generativa de texto y ChatGPT en la Justicia* (dir. por J.G. Corvalán y M. Sánchez Caparrós), Thomson Reuters-La Ley- IALAB, 2023, https://ialab.com.ar/wp-content/uploads/2023/11/Guia-de-directrices-usos-de-ChatGPT-e-IA-generativa-en-la-justicia.pdf.
También, Le Fevre Cervini: *Uso estratégico de datos e inteligencia artificial en la justicia. Informe 6*. Caracas: CAF. 2022, https://scioteca.caf.com/handle/123456789/1932.

3 https://es.wikipedia.org/wiki/Prometea Corvalán, J. G.: "Inteligencia artificial: retos, desafíos y oportunidades-Prometea: la primera inteligencia artificial de Latinoamérica al servicio de la Justicia". *Revista de Investigações Constitucionais*, 2018, vol. 5, pp. 295-316.
Estevez, E. y otros: *PROMETEA: Transformando la Administración de Justicia con herramientas de inteligencia artificial*, BID, Washington, 2020.

• Lorenzo Cotino Hueso
Catedrático de Derecho Constitucional, Universidad de Valencia. ValgrAI. Correo electrónico: **cotino@uv.es**. OdiseIA.

[4]Y ello sin mencionar los usos casi de ciencia ficción en China (como el sistema Xiao Zhi 3.0 de Alibaba en el Tribunal de Hangzhou),[5] donde el uso judicial de IA seré obligatorio en 2025.[6]

No pretendo en este estudio adentrarme en el interesante debate sobre si excluir la IA de las decisiones jurisdiccionales, permitirla como apoyo a los humanos o incluso alcanzar la robotización judicial, sustituyendo al juez humano.[7] Existen ya numerosas obras de referencia sobre la llamada algoritmización de la justicia,[8] a las que me remito.[9]

Como no podía ser de otra forma, hasta ahora, la Constitución y las leyes parten de la premisa de que son humanos quienes realizan tales funciones jurisdiccionales, por lo que no ha habido necesidad de efectuar una particular precisión al respecto. En esta dirección, el CGPJ afirma que la potestad jurisdiccional

4 Laboratorio de Innovación Judicial https://juslab.com.ar/ ver, Ministerio de Modernización de la Nación: "Kit de Innovación", https://acortar.link/WRqYxg.

5 Stern R.E. y otros: "Automating Fairness? Artificial Intelligence in the Chinese Court"s., *Columbia Journal of Transnational Law,* 2021, núm. 59, pp. 515-553, https://scholarship.law.columbia.edu/faculty_scholarship/2940.

6 https://english.court.gov.cn/2022-12/12/c_838810.htm Ver, [s.a]: *Opinions on Regulating and Strengthening the Application of Artificial Intelligence in Judicial Fields*, diciembre de 2022, https://www-old.ciftis.org/article/14978341100187648.html.

7 Sobre el tema, destaca en España inicialmente Nieva Fenoll, J.: *Inteligencia artificial y proceso judicial*, Marcial Pons, 2018. Más recientemente, "Perder el control digital: ¿hacia una distopía judicial?", en AA.VV.: *El proceso judicial en un marco cultural y digital* (dir. por S. Calaza López), Colex, 2023. También, Roberto Granero, H.: "Derechos y garantías concretas frente al uso de inteligencia artificial y decisiones automatizadas, especialmente en el ámbito judicial y de aplicación de la ley", pp. 107-137 y Amoni Reverón, G. A.: "Libertad, presunción de inocencia y defensa ante la irrupción de la inteligencia artificial en el ámbito policial y judicial penal", pp. 193-236. Ambos en AA.VV.: *Derechos y garantías ante la inteligencia artificial y las decisiones automatizadas* (ed. por L. Cotino Hueso), Thomson-Reuters Aranzadi, Cizur, 2022. Son diversos los estudios de Simón Castellano, P. entre otros, con Pérez Domínguez, S.: "Attitudes and perceptions regarding algorithmic judicial judgement: barriers to innovation in the judicial system?, *IDP: revista de Internet, derecho y política*, 2023, núm. 39 ("Digitalitzación y algoritmitzación de la justicia").

8 Expresión seguida en diversos estudios de Barona Vilar, S.: *Algoritmización del Derecho y de la Justicia. De la Inteligencia Artificial a la Smart Justice*, Tirant lo Blanch, Valencia, 2021. Entre otros, "Una justicia 'digital' y 'algorítmica' para una sociedad en estado de mudanza", en AA.VV.: *Justicia algorítmica y neuroderecho. Una mirada multidisciplinar* (ed. por S. Barona Vilar), Tirant lo Blanch, Valencia, 2021; "La seductora algoritmización de la justicia. Hacia una justicia poshumanista (Justicia+) ¿utópica o distópica?", en AA.VV.: *Justicia poliédrica en periodo de mudanza: Nuevos conceptos, nuevos sujetos, nuevos instrumentos y nueva intensidad* (ed. por S. Barona Vilar), Tirant lo Blanch, Valencia, 2022, pp. 36-47.

9 En general cabe remitir a diversos trabajos de autores de referencia en *El Cronista del Estado Social y Democrático de Derecho*, 2022, núm. 100 (Inteligencia artificial y derecho, ed. por A. Boix Palop):
Barona Vilar, S.: "La seductora algoritmización de la justicia. Hacia una justicia poshumanista (Justicia+) ¿utópica o distópica?", 36-47; Martínez Garay, L. y García Ortiz A. M.: "Paradojas de los algoritmos predictivos utilizados en el sistema de justicia penal", pp. 160-173; Miró Llinares, F.: "Inteligencia artificial, delito y control penal: nuevas reflexiones y algunas predicciones sobre su impacto en el derecho y la justicia penal", pp. 174-183.
También, los estudios de Bueno y Bujosa en *El impacto de las tecnologías disruptivas en el derecho procesal* (dir. por F. Bueno de Mata), Aranzadi Thomson Reuters, 2022.
Asimismo, Montesinos García, A.: "Empleo de la inteligencia artificial en algunas fases del proceso judicial civil: prueba, medidas cautelares y sentencia", *Actualidad civil*, 2022, núm. 11; "Afectación de los derechos y garantías procesales por el empleo de algoritmos predictivos", en AA.VV.: *El proceso como garantía* (dir. por J. M. Asencio Mellado y O. Fuentes Soriano), Atelier, Madrid, 2023, pp. 703-714.

es una función "consustancial y ontológicamente anudada a la naturaleza humana, con independencia, imparcialidad, exclusividad y con exclusivo sometimiento al imperio de la ley", lo que implica "debidos controles, evaluaciones y las garantías adecuadas" (nº 51) [10]. El CGPJ viene a afirmar lo que se ha dado en llamar una "reserva de humanidad"[11], esto es, delimitar ciertos espacios vedados a la actuación o decisiones de la IA, para asegurar que se aplican las cualidades, discrecionalidad, criterio y sensibilidad propias de los humanos. Así, para la potestad jurisdiccional afirma que corresponde a los humanos "verificar la realidad de los hechos que configuran el objeto del proceso, así como subsumir los hechos en las normas, seleccionando e interpretando el Derecho de aplicación al caso, y emitir los oportunos pronunciamientos resolviendo, conforme a la ley, la controversia existente entre las partes, cuidándose, en su caso, de la ejecución del fallo" (nº 163). [12] Se afirma en este sentido para los ciudadanos "el derecho a una resolución fundada en Derecho dictada por un Juez o Tribunal, esto es, el derecho a que su caso sea resuelto por un Juez-persona" (nº 164, Conclusión 68). [13] El alcance de este presunto derecho y la delimitación de hasta dónde puede llegar la IA en el ámbito de la justicia es una cuestión que irá resolviendo el legislador y la jurisprudencia (constitucional en su caso), acompañando un imparable proceso de avance tecnológico.

Sería deseable una actualización constitucional al respecto, pero cuanto menos, como se expondrá, es necesaria la habilitación legal del uso de sistemas automatizados, algoritmos y, en particular, de IA para algunas concretas funciones de naturaleza jurisdiccional. Y que dicha regulación legal incluya suficientes garantías. En esta línea, este estudio pretende ser operativo y concretar las exigencias básicas de habilitación legal y de regulación con garantías suficientes del uso de sistemas automatizados e incluso de IA en las funciones jurisdiccionales. Una vez concretadas tales exigencias, se analiza el actual -y mejorable- régimen

10 CGPJ: *Informe al Anteproyecto de ley de eficiencia digital del Servicio público de justicia, Acuerdo adoptado por el Pleno*, de 24 de febrero de 2022, https://www.poderjudicial.es/stfls/CGPJ/COMISI%C3%93N%20DE%20ESTUDIOS%20E%20INFORMES/INFORMES%20DE%20LEY/FICHERO/20220224%20Informe%20al%20anteproyecto%20de%20Ley%20de%20Eficiencia%20Digital%20del%20Servicio%20P%C3%BAblico%20de%20Justicia.pdf . Se trata de un informe de 211 páginas. En concreto, "las exigencias derivadas de los principios consagrados en el artículo 117 CE, y del artículo 24.1 CE, imponen la necesidad de los debidos controles, evaluaciones y las garantías adecuadas en la configuración, en la utilización y en el resultado de los mecanismos de inteligencia artificial aplicados a la función jurisdiccional, no solo en cuanto a los algoritmos empleados sino también, y específicamente, en orden a salvaguardar el ejercicio de la función jurisdiccional, consustancial y ontológicamente anudada a la naturaleza humana, con independencia, imparcialidad, exclusividad y con exclusivo sometimiento al imperio de la ley."

11 Expresión que ha tenido su éxito de la mano de Ponce Solé, J.: "Inteligencia artificial, Derecho administrativo y reserva de humanidad: algoritmos y procedimiento administrativo debido tecnológico", en Monográfico sobre IA (coord. por A. Boix y L. Cotino), *Revista General de Derecho Administrativo*, 2019, núm. 50.

12 CGPJ: *Informe,* cit.

13 CGPJ: *Informe,* cit.

legal en España, actualmente el Real Decreto-ley 6/2023, de 19 de diciembre,[14] y del Reglamento de inteligencia artificial de la UE (RIA) de 2024.[15]

Debo confesar que este esfuerzo lo realizo con la intención de facilitar y allanar el camino para el uso jurisdiccional de estas tecnologías. Así lo pretendo bajo la convicción de un derecho a la IA, más bien, una obligación o deber de IA para una mayor efectividad de los derechos fundamentales, [16] en este caso, en el ámbito de la justicia. Sin duda alguna, hay que exigir no pocas garantías en el terreno jurisdiccional. Sin embargo, hay que huir de las reacciones que me atrevo a señalar de "bicho bola", que lamentablemente creo que son las generalizadas entre juristas y, más si cabe, respecto del uso de IA en justicia y aplicación de la ley. En cuestiones de mirar al futuro es más que fácil equivocarse, pero creo que la mayoría de los discursos actuales de cerrazón al uso jurisdiccional de la IA los veremos como cándidos y con cierta nostalgia dentro de no muchos años.

La función jurisdiccional en esencia implica la facultad de juzgar y hacer ejecutar lo juzgado, la resolución de conflictos aplicando la ley y, en su caso, con valoración de las pruebas, la instrucción e investigación, la protección específica de derechos, la ejecución de sentencias y resoluciones, así como la adopción de medidas cautelares. Y para todo ello pueden utilizarse, de un modo u otro, sistemas automatizados y, en especial, la IA. Así, resulta de especial interés intentar concretar algunas funciones jurisdiccionales que pueden ser realizadas a través de sistemas de IA. La IA puede ser utilizada para la adopción o, mayormente, asistencia en la redacción de sentencias y resoluciones basadas en la jurisprudencia y normativa aplicable. Asimismo, respecto de las fuentes de prueba y su valoración, la IA puede ser utilizada para:

- La generación o ejecución de informes y auditorías destinados al proceso con valor probatorio.

- La evaluación de evidencias científicas presentadas, verificación de datos y el análisis de la metodología empleada en estudios y peritajes.

- El análisis y predicción de riesgos, lo cual puede ser en el contexto del asesoramiento en resoluciones judiciales, para la toma de medidas cautelares o en la ejecución de sentencias, como las decisiones sobre peligrosidad del reo.

14 Real Decreto-ley 6/2023, de 19 de diciembre, por el que se aprueban medidas urgentes para la ejecución del Plan de Recuperación, Transformación y Resiliencia en materia de servicio público de justicia, función pública, régimen local y mecenazgo.

15 Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (mayo 2024).

16 Al respecto, mi estudio, "Cómo abordar jurídicamente el impacto de la inteligencia artificial en los derechos fundamentales", en *Derecho y Tecnologías*, Fundación Ramón Areces, Madrid, 2024.

Y lo cierto es que en buena medida el RIA ha recogido estas funciones jurisdiccionales que considera de "alto riesgo"[17]. Así, "se considerarán de alto riesgo los sistemas de IA contemplados en el anexo III" (art. 6.2 RIA). Cabe subrayar que este riesgo debe darse, "en particular", por "influir sustancialmente en el resultado de la toma de decisiones" (art. 6.3 RIA). Por las finalidades de uso de IA que ahora interesan, son de alto riesgo los sistemas IA para la "Garantía del cumplimiento del Derecho" (Anexo III. 6), en concreto para:

- "evaluar el riesgo de que una persona física sea víctima de delitos",
- "polígrafos o herramientas similares",
- "para evaluar la fiabilidad de las pruebas durante la investigación o el enjuiciamiento de delitos",
- "para evaluar el riesgo de que una persona física cometa un delito o reincida en la comisión de un delito […] o para evaluar rasgos y características de la personalidad o comportamientos delictivos pasados de personas físicas o colectivos" así como "para elaborar perfiles de personas físicas […] durante la detección, la investigación o el enjuiciamiento de delitos".

Son también de alto riesgo los sistemas del ámbito de la "Administración de justicia" (Anexo III. 8). En este ámbito se ha ido precisando el alcance desde la primera versión de 2021. [18] En la versión final, son de alto riesgo los sistemas IA "destinados a ser utilizados por una autoridad judicial" (8.a), para "ayudar" "en la investigación e interpretación de hechos y de la ley, así como en la aplicación de la ley a un conjunto concreto de hechos". También se incluyen los sistemas IA "utilizados de forma similar en una resolución alternativa de litigios" (8.a), a lo que se añade "cuando los resultados de los procedimientos de resolución alternativa de litigios surtan efectos jurídicos para las partes" (Consid. 61).

El RIA excluye como de alto riesgo "los sistemas de IA destinados a actividades administrativas meramente accesorias que no afectan a la administración de justicia propiamente dicha en casos concretos, como la anonimización o seudonimización de resoluciones judiciales, documentos o datos, la comunicación entre los miembros del personal o las tareas administrativas" (Consid. 61).

17 Sobre los sistemas de alto riesgo en el RIA me remito al *Tratado sobre el Reglamento de Inteligencia Artificial de la Unión Europea* (coord. por L. Cotino Hueso y P. Simó Castellanos), Aranzadi, 2024.

18 Así, la versión de 2021 de la Comisión hablaba de sistemas para "asistir a una autoridad judicial en la investigación e interpretación de los hechos y del Derecho y en la aplicación del Derecho a un conjunto concreto de hechos." A lo que se fue añadiendo que los sistemas puedan ser "utilizados por una autoridad judicial, o en su nombre· (desde Versión del Consejo de la UE).

Como se verá, el RIA es más claro y preciso que el Real Decreto-ley 6/2023 al regular las finalidades del uso jurisdiccional de IA. Sin embargo, y como también se dirá, el RIA no vale como norma legal habilitante.

II. LA NECESARIA REGULACIÓN POR LEY DEL USO JURISDICCIONAL DE SISTEMAS AUTOMATIZADOS Y DE INTELIGENCIA ARTIFICIAL.

1. La variable cobertura legal para las actuaciones jurisdiccionales con sistemas automatizados.

En diversos estudios y como punto de partida, he considerado adecuado partir de un concepto inclusivo que no se ciña estrictamente al concepto de "IA", sino que gire sobre el uso público de medios electrónicos, software, sistemas automatizados o algoritmos, es decir, sistemas informáticos que integren fórmulas más o menos complejas y las apliquen a los datos. Esto permite configurar un "suelo" básico, un "mínimo común" general que confiera un tratamiento jurídico homogéneo a los algoritmos públicos, en nuestro caso, en el ámbito de la Justicia.

Ahora bien, según cada supuesto específico de tecnología empleada y cada concreta finalidad de uso de los sistemas en el ámbito de la justicia, y especialmente para su uso jurisdiccional, se requerirá una regulación legal más densa o intensa. También serán variables los derechos afectados y el riesgo o impacto en los mismos, así como las exigencias legales para la habilitación legal y regulación de garantías o límites. En el terreno jurisdiccional, la exigencia de legalidad se concentra especialmente en el ámbito procesal penal, pero no sólo. El uso jurisdiccional de sistemas informáticos tendrá variable impacto en las garantías procesales en juego (art. 24 CE) o en los derechos y el principio de legalidad penal y sancionadora (art. 25 CE). Asimismo, cabe partir del principio de legalidad procesal en general respecto del "ejercicio de la potestad jurisdiccional en todo tipo de procesos" en razón del artículo 117.3º CE. Las referencias a la sujeción a la ley son reiteradas en la LOPJ, como en los artículos 2 y 9, [19] entre otros, o con claridad, el "Principio de legalidad procesal" expresado en el artículo 1 LEC. [20]

Por otra parte, ya respecto de sistemas automatizados en justicia que tratan datos personales, la exigencia de regulación legal es una exigencia constitucional reconocida por los tribunales, así como por la normativa de protección de datos. Así, tanto el TJUE como el TC han sido particularmente exigentes no sólo en la

19 Así, "El ejercicio de la potestad jurisdiccional, juzgando y haciendo ejecutar lo juzgado, corresponde exclusivamente a los Juzgados y Tribunales determinados en las leyes" y "no ejercerán más funciones que las señaladas en el párrafo anterior, y las demás que expresamente les sean atribuidas por ley en garantía de cualquier derecho." (art. 2 LOPJ). De igual modo, "Los Juzgados y Tribunales ejercerán su jurisdicción exclusivamente en aquellos casos en que les venga atribuida por esta u otra Ley." (art. 9 LOPJ).

20 Artículo 1. "Principio de legalidad procesal": En los procesos civiles, los tribunales y quienes ante ellos acudan e intervengan deberán actuar con arreglo a lo dispuesto en esta Ley.

necesidad de una ley, sino que, además, debe ser una ley de calidad. Por ejemplo, la STJUE (Gran Sala) del 8 de abril de 2014 en los Asuntos C-293/12 y C-594/12 ("Digital Rights"), y en especial las Conclusiones de Pedro Cruz (nº 108 y ss.), resaltan la exigencia de calidad normativa, aplicable incluso a Directivas, que son por naturaleza más genéricas que el Derecho nacional que las transpone. En España, la protección de datos ha provocado las sentencias más estrictas sobre calidad legislativa. Quien suscribe precisamente participó en la petición al Defensor del Pueblo del recurso de inconstitucionalidad respecto de la Ley Orgánica 3/2018, que dio lugar a la sentencia más exigente en materia de calidad de la ley. Así, la STC 76/2019, de 22 de mayo (en especial FJ 8º), es muy rigurosa respecto de la necesidad de que la ley limitativa del derecho de protección de datos integre en su contenido no sólo el detalle de la restricción y sus presupuestos, sino que también se han de regular las garantías concretas "compensatorias" de la restricción.

El RGPD es en general aplicable a todo tratamiento automatizado de datos y cabe tener en cuenta la regulación específica de la Ley Orgánica 7/2021, de 26 de mayo, que transpone la Directiva 2016/680 para el ámbito penal y policial. En todos los casos se requiere la legitimación del tratamiento de datos por el sector público y en general debe darse no por el consentimiento, sino por contar con una base legal. A la exigencia general de ley que legitime el tratamiento de datos se añaden particulares exigencias de regulación por ley de garantías respecto de las categorías especiales de datos en los artículos 9 RGPD y 10 Directiva 2016/680, artículo 9.2 Ley Orgánica 3/2018.

Si, además, se trata de sistemas sólo automatizados sin intervención humana, se aplican exigencias de legalidad particulares para decisiones sólo automatizadas en el artículo 22.2b RGPD y 11 Directiva 2016/680. En el caso del sector público, si es un sistema sólo automatizado sin intervención humana, además, se aplicarán las especialidades del régimen jurídico del artículo 41 Ley 40/2015. Y en el ámbito de justicia, la regulación especial que luego se comenta, en general insuficiente. De igual modo, cualquier límite al derecho de protección de datos debe contar también con fuertes exigencias de legalidad en el artículo 23 RGPD.

La jurisprudencia constitucional comparada[21] también conduce a recomendar una especial habilitación legal con garantías suficientes. Así, entre otras, la sentencia de 5 de febrero de 2020 del Tribunal de Distrito de la Haya (C/09/550982/HA ZA 18-388)[22], que declaró contrario al artículo 8 CEDH el sistema "Systeem Risicoindicatie" ("SyRI"). En el ámbito policial y penal, en 2023, la sentencia del

21 He dedicado varios estudios desde 2020 sobre las diferentes sentencias de referencia, puede seguirse el más reciente "Una regulación legal y de calidad para los análisis automatizados de datos o con inteligencia artificial. Los altos estándares del Tribunal Constitucional alemán y otros tribunales, que no se cumplen ni de lejos en España", *Revista General de Derecho Administrativo*, núm. 63, 2023. acceso.

22 https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2020:1878.

Tribunal Constitucional alemán del 16 de febrero (1 BvR 1547/19, 1 BvR 2634/20) estableció requisitos y estándares de calidad legislativa muy altos (incluso excesivos) para tratamientos automatizados de datos en la prevención del delito. [23] También ha habido importantes decisiones por el Consejo Constitucional en Francia, donde se cuenta con una regulación indudablemente superior a la española. Igualmente cabe mencionar las exigencias de regulación de calidad por el TC de Eslovaquia en su decisión de 17 de diciembre de 2021. [24] Lo cierto es que en otros países se han declarado inconstitucionales normas legales que regulan tratamientos automatizados de datos por el sector público y que incluían garantías que no se alcanzan ni de lejos en España cuando se realizan tratamientos masivos de datos por la AEAT, la TGSS, CNMC o inspección de trabajo, entre otras. [25]

Para el ámbito de sistemas de identificación biométricos, y como he defendido, considero que en general no contamos con una ley habilitante y que regule las garantías, ni para el sector público ni para el sector privado. [26] A este respecto, en el ámbito criminal y policial, la Ley Orgánica 7/2021, de 26 de mayo no ha aportado prácticamente nada. En mayo de 2022, el CEPD ha recordado que si la ley nacional es una mera reiteración del artículo 10 Directiva 2016/680, no puede ser invocada como una ley que autoriza el tratamiento de datos biométricos. [27]

Así las cosas, aunque sea de variable intensidad, constitucionalmente es precisa una cobertura legal más o menos densa o intensa para el uso de sistemas automatizados, software y algoritmos en el ámbito jurisdiccional.

2. Una mayor cobertura legal si se utiliza inteligencia artificial.

Afirmada la necesidad de legalidad general para el uso jurisdiccional de sistemas automatizados, es momento de subrayar que el uso jurisdiccional de IA debe contar con un plus de regulación legal y garantías particulares añadidas y distintivas respecto del régimen del uso de software, sistemas automatizados o algoritmos. La IA presenta cualidades como la autonomía, el autoaprendizaje y la

23 https://www.bundesverfassungsgericht.de/e/rs20230216_1bvr154719.html. resulta de interés también el comunicado de prensa nº 18/2023 de 16 de febrero de 2023 en inglés y alemán. Las referencias a la misma en español son a partir de traducción automatizada.

24 Con relación a la normativa fiscal respecto de la recopilación masiva de datos de recibos y elaboración de perfiles de riesgo de las empresas, acceso completo en https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2021/492/20211217

25 Olivares Olivares, B. D.: "Law and Artificial Intelligence in the Spanish Tax Administration: the Need for a Specific Regulation", *European Review of Digital Administration* & Law-ERDAL 1 (1-2), pp. 227-234.

26 Entre otros, "Reconocimiento facial automatizado y sistemas de identificación biométrica bajo la regulación superpuesta de inteligencia artificial y protección de datos", en *Derecho público de la inteligencia artificial* (coord. por F. Balaguer Callejón y L. Cotino Hueso), F. Jiménez Abad-Marcial Pons, Madrid, 2023, pp. 347-402, acceso.

27 CEPD: *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*, Version 1.0, 12 mayo 2022, https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-052022-use-facial-recognition_en.

capacidad predictiva que implican generan mayores riesgos y posibles impactos en derechos y garantías. Todo ello en el marco del uso jurisdiccional, de máxima sensibilidad e impacto en derechos de las personas. Los riesgos de decisiones impredecibles o difíciles de entender, la limitada transparencia y en especial explicabilidad,[28] particularmente en el aprendizaje profundo dificulta saber cómo se llega a la decisión específica. Ello es especialmente preocupante en el contexto jurisdiccional, donde la motivación y justificación de las decisiones son fundamentales para el debido proceso y la confianza en el sistema judicial. O el uso y aprendizaje a partir de datos históricos, en su caso, sesgados, que pueden perpetuar y amplificar sesgos y conducir malas decisiones. Es por ello por lo que la IA requiere una regulación legal más densa, más estricta y con garantías adicionales respecto del uso de sistemas automatizados o software tradicionales.

En esta línea, afirma el CGPJ que "El uso de la inteligencia artificial constituye, ciertamente, una herramienta que puede proporcionar utilidades relevantes en términos de eficiencia al sistema de Administración de Justicia, pero también entraña riesgos severos para la garantía de principios fundamentales de nuestro Estado de Derecho. Por ello, en este campo el prelegislador debería mantener una posición de precaución y abordar el establecimiento de una regulación completa y garantista del uso de las técnicas de inteligencia artificial en el ámbito del ejercicio de la función jurisdiccional" (nº 168). [29] Critica el CGPJ que el Real Decreto-ley 6/2023 implica una aceptación del uso de IA "en el ámbito jurisdiccional acrítico o no problemático que dista mucho de ser la aproximación adecuada a esta cuestión." (nº 138, Conclusión 56). [30]

Como se ha adelantado, el TC alemán exige unas garantías legales muy elevadas respecto del tratamiento automatizado de datos en los ámbitos policial y penal. Pero es que el TC alemán directamente prohíbe el uso de IA: "El uso de sistemas de autoaprendizaje debe estar expresamente excluido en la ley" [31]. Creo que la prohibición como punto de partida es un error; para el uso jurisdiccional de IA debe haber una habilitación y regulación legal expresa y con garantías. En su caso, el legislador, si lo desea, podrá prohibir expresamente algunos usos jurisdiccionales específicos. Así, por ejemplo, el legislador podrá dar forma a ese presunto "derecho

28 Sobre el tema, cabe remitir a los distintos estudios en Cotino Hueso, L. "Transparencia y explicabilidad de la inteligencia artificial y "compañía" (comunicación, interpretabilidad, inteligibilidad, auditabilidad, testabilidad, comprobabilidad, simulabilidad…). Para qué, para quién y cuánta", en AA.VV.: *Transparencia y explicabilidad de la inteligencia artificial* (coord. por L. Cotino Hueso y P. Simó Castellanos), Tirant lo Blanch, Valencia, 2022.

29 CGPJ: *Informe,* cit.

30 CGPJ: *Informe,* cit.

31 El TC alemán expresamente obliga a que la ley limite las posibilidades e impone limitaciones a la automatización, e incluso prohibición de sistemas de autoaprendizaje: "El uso de sistemas de autoaprendizaje debe estar expresamente excluido en la ley" (&121), Sentencia de 16 de febrero de 2023.

a resoluciones de jueces humanos", esto es, delimitar el alcance de la reserva de potestad jurisdiccional a tribunales y jueces humanos.

Hoy día, la regulación española dista mucho de ser una "regulación completa y garantista del uso de las técnicas de inteligencia artificial en el ámbito del ejercicio de la función jurisdiccional", como señalaba el CGPJ (nº 168).[32] Esto, a mi juicio, es muy negativo, pues merma algunas posibilidades que podrían ser de interés.

3. El Reglamento IA no sirve como habilitación legal.

Se ha adelantado que el RIA regula diversos usos jurisdiccionales de IA como sistemas de alto riesgo. Sin embargo, esta regulación no sirve como cobertura legal. Como advierte expresamente el Considerando 63 del RIA, "El hecho de que un sistema de IA sea clasificado como un sistema de IA de alto riesgo en virtud del presente Reglamento no debe interpretarse como indicador de que su uso sea legal con arreglo a otros actos del Derecho de la Unión o del Derecho nacional compatible con el Derecho de la Unión [...] No debe entenderse que el presente Reglamento constituye un fundamento jurídico [...] salvo que el presente Reglamento disponga específicamente otra cosa." (Considerando 63). Esta regla general es clara y considero que debe aplicarse a todos los sistemas de alto riesgo del Anexo III. Ello es así pese a que, en una clara falta de técnica legislativa, sólo en tres ocasiones de ocho apartados del Anexo III se añade la expresión "en la medida en que su uso esté permitido por el Derecho de la Unión o nacional aplicable". Así sucede en el caso de los sistemas IA biométricos (1º), respecto de la garantía del cumplimiento del Derecho (6º) y el uso para migración, asilo y gestión del control fronterizo (7º). Sin embargo, no se añade esta necesidad de ley de regulación específica respecto del ámbito de Justicia (8º a).

En cualquier caso, hay que partir de que el RIA no vale como norma legal que legitime un tratamiento de datos o una restricción de derechos fundamentales o colme una exigencia de legalidad penal, sancionadora o procesal. Seguirá siendo necesaria una ley que habilite la existencia de un concreto sistema de alto riesgo de los regulados con carácter general en el RIA.

III. LA (INSUFICIENTE) HABILITACIÓN EN EL REAL DECRETO-LEY 6/2023: ORIENTACIÓN AL DATO Y ACTUACIONES AUTOMATIZADAS, PROACTIVAS Y ASISTIDAS PARA USO JURISDICCIONAL.

Según se ha concluido, es necesaria una particular habilitación legal para el uso de sistemas automatizados y en particular con IA en el ámbito más directamente

32 CGPJ: *Informe,* cit.

conectado con la función jurisdiccional o asistencia a la función judicial. Lo ideal sería regular expresamente el uso específico de IA al que se quiere dar cobertura.

El Real Decreto-ley 6/2023 está plagado de menciones heterogéneas relacionadas con el uso de algoritmos, sistemas automatizados o IA en la Administración de justicia, con expresiones como el uso de "algoritmos", "sistemas", "sistema de información", "aplicaciones", "métodos electrónicos", "actuaciones", "procesos" "automatizados", "extracción automatizada de los datos", "realización automatizada de funciones", etc. Estas expresiones permiten dotar de cierta habilitación general al uso de sistemas automatizados.

1. La regulación en España de las actuaciones judiciales automatizadas, ahora con inteligencia artificial.

En el ámbito de justicia, con la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia, ya se dio una habilitación general para la "Actuación judicial automatizada" en su artículo 42. [33] Se emulaba así al artículo 37 de la Ley 11/2007[34] que ha tenido su continuación luego en el artículo 41 Ley 40/2015 del sector público. En aquel entonces no se trataba de actuaciones íntegramente automatizadas y, ni por asomo, se vislumbraba que la regulación habría de dotar de cobertura a sistemas automatizados y, en especial, IA para realizar funciones jurisdiccionales. Se partía de que la automatización era sólo posible respecto de aspectos instrumentales y actos reglados o de solución única y en modo alguno a la función jurisdiccional de manera sustantiva. En esta línea, Palomar Olmeda daba por hecho que las funciones interpretativas de normas por secretarios judiciales y jueces "no está prevista que pueda ser suplida […] por un proceso íntegramente automatizado […] La justificación última es, por lo demás, sencilla ya que la aplicación de la norma no puede considerarse como una potestad reglada o de solución única y, por tanto, la sustitución del juicio aplicativo por uno totalmente automatizado no se presenta como posible." [35] Dicho lo anterior, lo cierto es que el artículo 25 Ley

33 Artículo 42. Actuación judicial automatizada. En caso de actuación automatizada, deberá establecerse previamente por el Comité técnico estatal de la Administración judicial electrónica la definición de las especificaciones, programación, mantenimiento, supervisión y control de calidad y, en su caso la auditoría del sistema de información y de su código fuente.
Los sistemas incluirán los indicadores de gestión que se establezcan por la Comisión Nacional de Estadística Judicial y el Comité técnico estatal de la Administración judicial electrónica, cada uno en el ámbito de sus competencias.

34 "Artículo 39. Actuación administrativa automatizada. En caso de actuación automatizada deberá establecerse previamente el órgano u órganos competentes, según los casos, para la definición de las especificaciones, programación, mantenimiento, supervisión y control de calidad y, en su caso, auditoría del sistema de información y de su código fuente. Asimismo, se indicará el órgano que debe ser considerado responsable a efectos de impugnación."

35 Palomar Olmeda, A.: "La actuación judicial automatizada", en AA.VV.: *Las tecnologías de la información y la comunicación en la administración de justicia. La Ley 18/2011 y la administración electrónica en el sistema judicial* (coord. por E. Gamero Casado y J. Valero Torrijos), Aranzadi, Cizur Menor, 2012, pp. 659-704, versión pruebas de imprenta.

18/2011, de 5 de julio ya "jugaba a despistar" y hablaba de "la aplicación de medios electrónicos a los procesos de trabajo y a la gestión de los procedimientos y de la 'actuación judicial'".

Sin embargo, ahora ya es momento de plantearse la posibilidad técnica y la cobertura jurídica del uso de sistemas automatizados y en particular de IA que influyan sustantivamente en el contenido de la actividad jurisdiccional.

La Ley 18/2011, de 5 de julio ha quedado atrás. La disolución anticipada del Congreso y el Senado en 29 de mayo de 2023 hizo decaer el Proyecto de Ley 121/000097, de medidas de eficiencia procesal del servicio público de Justicia[36] y, por lo que más interesa, el Proyecto de Ley de Medidas de Eficiencia Digital del Servicio Público de Justicia de 2022[37]. No obstante, la derogación de la Ley 18/2011 se dio en razón del Real Decreto-ley 6/2023,[38] que incorpora no pocas regulaciones de aquellos proyectos que aquí interesan, en particular, la orientación al dato (art. 35 del proyecto de eficiencia digital) y la producción de actuaciones judiciales y procesales automatizadas, asistidas y proactivas (artículos 56 y ss., Cap. VII).[39] El 10 de enero de 2024, el Congreso decidió convalidar el Real Decreto-ley y su tramitación como Proyecto de Ley (núm. expte. 121/000002).[40] Al momento de cerrar estas páginas se conocen las enmiendas presentadas al proyecto en el Congreso y la avocación al Pleno para su aprobación en marzo de 2024. Este proyecto de ley contó con amplio Informe del CGPJ de 24 de febrero de 2022[41]. Antes de analizar esta regulación actual, se señalan las exigencias constitucionales de regulación legal del uso de sistemas automatizados y de IA, así como la regulación legal de garantías, para así valorar su adecuación.

2. La habilitación general casi en blanco del artículo 35 de "orientación al dato".

En una revisión del Real Decreto-ley 6/2023 como norma de regulación legal habilitadora y con garantías, resulta destacable la mención al "Principio general de orientación al dato". Este principio puede constituir la regulación legal general

36 *Boletín Oficial de las Cortes Generales, XIV Legislatura, Serie A: Proyectos De Ley. BOCG* de 22 de abril de 2022, Núm. 97-1 https://www.congreso.es/public_oficiales/L14/CONG/BOCG/A/BOCG-14-A-97-1.PDF.

37 *Boletín Oficial de las Cortes Generales, XIV Legislatura, Serie A: Proyectos De Ley 12 de septiembre de 2022 Núm. 116,* https://www.congreso.es/public_oficiales/L14/CONG/BOCG/A/BOCG-14-A-116-1.PDF.

38 Real Decreto-ley 6/2023, de 19 de diciembre, por el que se aprueban medidas urgentes para la ejecución del Plan de Recuperación, Transformación y Resiliencia en materia de servicio público de justicia, función pública, régimen local y mecenazgo.

39 Una aproximación a estas cuestiones del proyecto en Montoro Sánchez, J. A.: "Actuaciones judiciales automatizadas en el Proyecto de Ley de eficiencia digital del servicio público de justicia", en AA.VV.: *Logros y retos de la justicia civil en España* (dir. por F. Jiménez Conde y otros), Tirant lo Blanch, Valencia, pp. 687-704. También, Fernández, C. B.: "Proyecto de Ley de Medidas de Eficiencia Digital del Servicio Público de Justicia", *Derecho Digital e Innovación. Digital Law and Innovation Review*, 2022, núm. 13 (julio-septiembre).

40 Se puede seguir su tramitación en https://www.congreso.es/es/busqueda-de-iniciativas?p_p_id=iniciativas&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&_iniciativas_mode=mostrarDetalle&_iniciativas_legislatura=XV&_iniciativas_id=121%2F000002.

41 CGPJ: *Informe,* cit.

habilitadora del uso de sistemas automatizados y, también, de IA. Sin embargo, como se precisa ahora, sería excesivamente indeterminada y debe completarse con regulaciones específicas con rango legal y, en su caso, con colaboraciones normativas y otras técnicas de participación o autorización específicas.

Este principio de orientación al dato en la Exposición de Motivos[42] y en la letra j) del artículo 35 se vincula a "la producción de actuaciones judiciales y procesales automatizadas, asistidas y proactivas, de conformidad con la ley". Además, el uso de IA en este artículo 35 del Real Decreto-ley 6/2023 enlaza con "c) La búsqueda y análisis de datos y documentos para fines jurisdiccionales y organizativos". La orientación al dato conlleva también la afirmación de los "intercambios masivos" de datos. [43] Destaca especialmente en el artículo 35 su letra k, "La aplicación de técnicas de inteligencia artificial para los fines anteriores u otros que sirvan de apoyo a la función jurisdiccional, a la tramitación, en su caso, de procedimientos judiciales, y a la definición y ejecución de políticas públicas relativas a la Administración de Justicia". El CGPJ alertaba que esta referencia al uso de IA (letra k) "puede entenderse como una habilitación en blanco", más allá de las más concretas previsiones de actuaciones automatizadas, asistidas y proactivas de los artículos 56-58 (nº 137 y Conclusión 58). [44]

Así las cosas, este artículo 35 vendría a habilitar legalmente el uso de sistemas automatizados, pero también expresamente de IA para:

- la producción de actuaciones judiciales y procesales automatizadas, asistidas y proactivas,

- la búsqueda y análisis de datos y documentos para fines jurisdiccionales y organizativos,

42 Ya se ha dicho más arriba que los datos son clave en las políticas públicas modernas. La gestión sobre los mismos posibilitará o facilitará la interoperabilidad de los sistemas, la tramitación electrónica, la búsqueda y análisis de los datos, la anonimización y seudonimización, la elaboración de cuadros de mando, la gestión de documentos y su transformación, la publicación de información en portales de datos abiertos, la producción de actuaciones automatizadas, asistidas y proactivas, la utilización de sistemas de inteligencia artificial para la elaboración de políticas públicas, y la transmisión de los datos conforme a lo que se determine.

43 Así, Exposición de motivos: "c) Intercambios masivos. Debido a las especiales características de aquellos o aquellas intervinientes que por diversas razones tienen un gran volumen de asuntos en los órganos judiciales." Y el artículo 36 ("Intercambios orientados al dato ") señala que se posibilitará el "intercambio de información […] en formato de datos estructurados […] en todo caso asegurarán su confiabilidad, su posible automatización".

44 CGPJ: *Informe,* cit. Núm. 137 "inteligencia artificial para los fines anteriores u otros que sirvan de apoyo a la función jurisdiccional, a la tramitación y conclusión, en su caso, de procedimientos judiciales, y a la definición y ejecución de políticas públicas, de acuerdo con la ley". Esta previsión puede entenderse como una habilitación en blanco para el empleo de técnicas de inteligencia artificial con incidencia en la tramitación de los procesos y el ejercicio de la función jurisdiccional, más allá de las específicas previsiones sobre actuaciones automatizadas, asistidas y proactivas que contemplan los artículos 56 a 58 del Anteproyecto."

- los intercambios masivos de datos,

- el apoyo a la función jurisdiccional, a la tramitación, en su caso, de procedimientos judiciales,

- la definición y ejecución de políticas públicas relativas a la Administración de Justicia.

Además de estas finalidades, la enmienda por el grupo que sustenta al gobierno pretende ampliar el espectro de posibles usos de IA. Así, en la tramitación como proyecto de ley del Real Decreto-ley 6/2023, la Enmienda Núm. 406 del Grupo Parlamentario Socialista propone "dar cobertura a proyectos IA como la anonimización documental, la extracción de indicadores de vulnerabilidad social y la automatización en la textualización y clasificación de documentos judiciales".

En primer lugar, el texto implica una habilitación legal para "tratar los documentos de los repositorios de la Administración de Justicia que contengan datos personales, incluidas categorías especiales de datos". Se afirma expresamente que se "habilitará el desarrollo de técnicas de inteligencia artificial". [45] Además de una variada remisión a normas vigentes como regulación de garantías, se añade que "Se requerirá de forma previa al tratamiento de los documentos, la autorización del letrado o letrada de la Administración de Justicia competente, o en su caso del superior funcional o jerárquico del servicio". Ciertamente, resulta difícil derivar una finalidad concreta y parece más una habilitación general para tratar todo tipo de información y datos con IA. Esto resulta muy insuficiente a mi juicio y puede constituir una inadmisible habilitación casi en blanco.

Asimismo, esta enmienda puede suponer la habilitación para el diseño y desarrollo de sistemas IA "cuyo objeto no esté prohibido por la normativa vigente". Parece de nuevo una habilitación general en blanco para que estos sistemas puedan "realizar acceso y procesamiento automático de documentos judiciales o procesales, siempre que se realicen labores de anonimización o pseudonimización" [46]. Como garantía para el diseño y desarrollo de sistemas IA se incluye la necesidad de una "autorización previa". También en esta enmienda se pretende habilitar de modo genérico "el uso y entrenamiento de modelos de

45 "Este tratamiento habilitará el desarrollo de técnicas de inteligencia artificial, previa adopción de las medidas de privacidad y seguridad que correspondan de conformidad con el marco normativo de protección de datos, el Esquema Nacional de Seguridad y Esquema Judicial de Interoperabilidad y Seguridad. Adicionalmente, se adoptarán medidas de mitigación de riesgos según la normativa europea vigente sobre inteligencia artificial y cualesquiera otras medidas que se establezcan obligatoriamente en la materia."

46 "4. Para el desarrollo de sistemas de inteligencia artificial cuyo objeto no esté prohibido por la normativa vigente, una vez recabada la autorización previa, se podrá realizar acceso y procesado automático de documentos judiciales o procesales, siempre que se realicen labores de anonimización o pseudonimización que impidan poder obtener datos de carácter personal de los propios documentos accedidos, o del código o productos del sistema de inteligencia artificial implementado."

inteligencia artificial de propósito general", pero sin regulación concreta alguna. [47] Finalmente, se propone los sistemas de alto riesgo según el RIA deben contar con la evaluación de conformidad, algo que es obligatorio por el RIA. [48]

A mi juicio, aunque es positiva la definición de finalidades de uso de sistemas automatizados o de IA en este artículo 35 de orientación al dato, respecto de los usos jurisdiccionales, este precepto no contiene un mínimo de densidad o intensidad normativa suficiente para determinar la finalidad concreta. Es por ello que debe complementarse con otras regulaciones legales específicas, y en su caso, con algún grado de colaboración normativa, orgánica y garantías, con sistemas de autorización. La enmienda al mismo ahonda en la finalidad habilitadora de este artículo, pero, a mi juicio, sigue requiriendo mayor precisión.

3. Inteligencia artificial y actuaciones automatizadas, proactivas y asistidas.

El Capítulo VII regula "las actuaciones automatizadas, proactivas y asistidas". Se menciona el "sistema de información adecuadamente programado" o "sistemas informáticos". El CGPJ ve claro que esta regulación "supone la incorporación de herramientas de inteligencia artificial en la producción de actuaciones procesales" (nº 124).[49] Sin embargo, no se menciona la "inteligencia artificial" en este capítulo. Pese a la referencia a la IA en el artículo 35 antes vista, sería útil una mención y habilitación específica de la IA en este capítulo. En esta línea, la Enmienda Núm. 408, del Grupo Parlamentario Socialista, aprovecha el artículo 58 para una habilitación general del uso de IA, añadiendo un apartado: "4. Podrán aplicarse técnicas de inteligencia artificial en las actuaciones automatizadas, asistidas o proactivas".

En el artículo 56 del Real Decreto-ley 6/2023 se distinguen unas actuaciones automatizadas que podemos considerar simples y no jurisdiccionales. Como afirma el CGPJ, claramente son actuaciones de trámite o resoluciones simples, que no requieren interpretación jurídica, como el enumerado o paginado de expedientes, la generación de copias y certificados, la generación de libros, la comprobación de representaciones o la declaración de firmeza, de acuerdo con la ley procesal (Conclusión 64º) [50]. Llama la atención la relativa a la "declaración de firmeza, de acuerdo con la ley procesal" (letra f), ya que una enmienda propone su supresión

47 "En el uso y entrenamiento de modelos de inteligencia artificial de propósito general en el ámbito de la Administración de Justicia, seguirán las medidas específicas establecidas en el marco normativo vigente, y se tendrán en cuenta las recomendaciones establecidas al respecto por el Ministerio para la Transformación Digital y de la Función Pública."

48 "Los sistemas de inteligencia artificial que sean categorizados como sistemas de alto riesgo según la normativa europea vigente de inteligencia artificial, superarán la correspondiente evaluación de conformidad antes de ponerse en servicio."

49 CGPJ: *Informe,* cit.

50 CGPJ: *Informe,* cit.

por no ser una cuestión simple[51] y otra enmienda aclara que sólo se trataría de "la generación y remisión de oficios sobre la declaración de firmeza". [52]

Más allá de estas actuaciones automatizadas simples que aquí poco interesan, cabe destacar las actuaciones proactivas también reguladas en este artículo 56 del Real Decreto-ley 6/2023. Este artículo habla de "actuaciones automatizadas, auto-iniciadas por los sistemas de información sin intervención humana" que sirven para "generar avisos o efectos directos a otros fines distintos, en el mismo o en otros expedientes, de la misma o de otra Administración Pública, en todo caso conformes con la ley". No falta razón al CGPJ cuando critica que estas finalidades de uso son mucho más imprecisas, su objeto "se define de forma bastante evanescente", un auténtico "arcano" difícil de descifrar (Conclus. 64). [53] Considero que tras un léxico de apariencia tecnológica se esconden finalidades de uso totalmente indeterminadas, quizá con la oscura intención de que esta regulación ampare muchos casos de uso que bien merecerían una regulación clara, específica y concreta por su impacto en derechos y garantías. Es por ello que esta regulación no sirve para dotar de legalidad el uso de sistemas automatizados con fines jurisdiccionales.

El artículo 57.1º del Real Decreto-ley 6/2023 regula las muy interesantes "actuaciones asistidas", en las que "el sistema de información […] genera un borrador total o parcial de documento complejo basado en datos, que puede ser producido por algoritmos, y puede constituir fundamento o apoyo de una resolución judicial o procesal". La Enmienda Núm. 407 del Grupo Parlamentario Socialista pretende añadir que pueden ser producidas "por algoritmos o técnicas de inteligencia artificial". No está de más. Respecto a las actuaciones asistidas, el CGPJ puso "serios reparos, desde el punto de vista de los principios constitucionales" (nº 163). Entiende el CGPJ que la generación de "borradores" por sistemas de información "constituye también, y debe subrayarse, un riesgo para la vigencia del principio de exclusividad jurisdiccional" (nº 164). La realización de borradores vulneraría "el derecho a que su caso sea resuelto por un Juez- persona" (nº 164, Conclusión 68). [54]

A mi juicio, en modo alguno puede identificarse la realización de borradores como la usurpación por la IA del papel que corresponde a jueces y tribunales

51 Enmienda Núm 248 Grupo Parlamentario Vasco (EAJ-PNV) que justifica en que "La decisión sobre la firmeza de una resolución depende siempre de una valoración jurídica en atención a las circunstancias concurrentes de cada caso; dada la trascendencia que tiene la firmeza sobre la cosa juzgada y los importantes efectos procesales y materiales que acarrea, no se considera adecuado que dicha decisión tenga el carácter automatizado que se le pretende dar."

52 En la Enmienda Núm. 460 del Grupo Parlamentario Popular en el Congreso se propone la modificación del artículo 56. 2º respecto de se aclara que sólo se trataría de "La generación y remisión de oficios sobre la declaración de firmeza de la sentencia entre órganos jurisdiccionales."

53 CGPJ: *Informe,* cit.

54 CGPJ: *Informe,* cit.

humanos. Dicho lo anterior, la realización de un borrador sí implica que la salida del sistema de IA puede influir esencialmente en la decisión jurisdiccional humana. Es decir, se da el requisito básico para que un sistema sea considerado de alto riesgo en virtud del artículo 6.3º y Anexo III.8.1º del RIA. En consecuencia, procede aplicar todas las garantías que ahí se regulan. De igual modo, estos borradores de decisiones judiciales, a mi juicio, también estarían bajo el régimen y las especiales garantías de las decisiones sólo automatizadas del artículo 22 RGPD o del artículo 11 de la Directiva (UE) 2016/680. Esto sería así pese a la necesidad de "validación" humana del borrador. En este sentido, cabe recordar que la reciente STJUE del 7 de diciembre de 2023 (caso SCHUFA c. Alemania)[55] brinda las garantías del artículo 22 RGPD a supuestos en los que la decisión formalmente parece humana, pero su base es automatizada.

IV. ADEMÁS, LA LEY DEBE REGULAR GARANTÍAS EN EL MARCO DEL RIA. UNA PROPUESTA.

Hasta ahora, se ha insistido en la necesidad de dotar de cobertura y habilitación legal al uso jurisdiccional de sistemas automatizados y algoritmos, que ha de ser más intensa en el caso de IA. Pero la exigencia de calidad legislativa no se limita a que la ley regule con suficiente detalle la finalidad y el caso de uso concreto. Además, es precisa una regulación legal de garantías específicas de ese sistema automatizado o algoritmo con la función jurisdiccional y especialmente en el caso de IA. Como se ha adelantado, la STC 76/2019, de 22 de mayo (en especial FJ 8º), es muy rigurosa respecto al respeto. Por cuanto el uso de IA en la función jurisdiccional, el CGPJ recuerda que exige "debidos controles, evaluaciones y las garantías adecuadas" (nº 51). [56]

Ahora bien, aquí hay que advertir de ciertas dificultades y particularidades. El RIA delimita los llamados sistemas de alto riesgo y regula toda una auténtica batería de garantías, medidas técnicas y organizativas antes, durante y después del desarrollo de estos sistemas IA de alto riesgo de uso jurisdiccional (análisis de riesgos, estudios de impacto, documentación de la gestión de calidad del sistema, gobernanza y calidad de los datos, generación de registros, supervisión y formación humana, robustez, precisión y ciberseguridad, etc.).[57] La duda es si estas garantías que implica el RIA son suficientes a efectos constitucionales y del RGPD. Y es que para la referida STC 76/2019, de 22 de mayo, las garantías propias y generales que ya regula el RGPD y la propia Ley Orgánica 3/2018 de protección de datos no

55 He realizado el primer estudio de la misma en "La primera sentencia del Tribunal de Justicia de la Unión Europea sobre decisiones automatizadas y sus implicaciones para la protección de datos y el Reglamento de inteligencia artificial", *Diario La Ley*, enero de 2024, https://ir.uv.es/V14YNLI.

56 CGPJ: *Informe,* cit.

57 Al respecto me remito al comentario de no pocos apartados del RIA en AA.VV.: *Tratado sobre el Reglamento*, cit.

fueron suficientes, sino que para el caso concreto, relativo a datos especialmente protegidos del artículo 9 RGPD, se precisaba una regulación legal con específicas garantías, lo que derivó en la inconstitucionalidad. Se trata de una cuestión bien difícil. Para el ámbito jurisdiccional que aquí interesa, considero que el RIA sí puede servir para "descargar", al menos parcialmente, la necesidad de que una regulación legal específica establezca garantías. No obstante, la ley nacional respecto del uso jurisdiccional de IA concreto sí que habrá de adecuar o modular las garantías del RIA.

La cuestión, no obstante, llega a lo "laberíntico". Y es que, en un "más difícil todavía", es cuestionable tanto que la ley deba como si puede introducir nuevas garantías. El RIA "impide que los Estados miembros impongan restricciones al desarrollo, la comercialización y la utilización de sistemas de IA, a menos que el presente Reglamento lo autorice expresamente" (Cons. 1).[58] Pese a lo anterior, los Estados sí que pueden establecer límites y obligaciones con fines diferentes a los del RIA o en otros ámbitos que el Derecho de la UE permite (Cons. 9).[59] Así, podría pensarse que la regulación de garantías añadidas a las del RIA para los usos jurisdiccionales de IA responde a exigencias procesales y de determinados derechos. Para admitir estas exigencias añadidas en la regulación nacional, deberían considerarse como una regulación de fines propios de competencias nacionales, o en el margen que el Derecho de la UE remite a la regulación nacional.

1. La regulación de garantías en el Real Decreto-ley 6/2023 y su difícil conjunción con las del RIA.

En el Real Decreto-ley 6/2023 las garantías en general están establecidas en el artículo 58, que regula los "requisitos comunes" a estas actuaciones. Este artículo viene a replicar las escasas garantías técnicas que contenía el antiguo artículo 42 de la Ley 18/2011, de 5 de julio, sobre actuaciones automatizadas. Incluso se da una regresión porque antes se decía que "deberá" y ahora simplemente "podrá" realizarse la definición de especificaciones y requisitos (ap. 1º). Respecto del anterior artículo 42, ahora se añade que hay que dejar "constancia" de los criterios

58 Y en esta línea, "Los Estados miembros no deben crear obstáculos injustificados a la introducción en el mercado o la puesta en servicio de sistemas de IA de alto riesgo que cumplan los requisitos establecidos en el presente Reglamento y lleven el marcado CE." (Cons. 129).

59 Cons. 9. las obligaciones impuestas a los distintos operadores que participan en la cadena de valor de la IA en virtud del presente Reglamento deben aplicarse sin perjuicio del Derecho nacional que, de conformidad con el Derecho de la Unión, tenga por efecto limitar el uso de determinados sistemas de IA cuando dicho Derecho quede fuera del ámbito de aplicación del presente Reglamento o persiga objetivos legítimos de interés público distintos de los perseguidos por el presente Reglamento. Así, por ejemplo, el presente Reglamento no debe afectar al Derecho laboral nacional ni al Derecho en materia de protección de menores."

de decisión, que "serán públicos y objetivos" (ap. 2º) [60] y que los "sistemas incluirán los indicadores de gestión" (ap. 3º). [61] Bien.

Para el CGPJ, en este artículo 58 no se tienen en cuenta las exigencias del RIA y otros documentos de "soft law" sobre el uso de IA en el ámbito de la justicia, por lo que el "marco normativo" es "poco robusto" (nº 167, Conclusión 70). [62] En la Enmienda Núm. 408 del Grupo Parlamentario Socialista, como garantía se menciona que habrá de quedar documentada una clasificación del nivel de riesgo. [63]

Quizá habría que detallar mejor esta nueva garantía.

Ya en concreto, el artículo 56 del Real Decreto-ley 6/2023 regula algunas garantías respecto de las actuaciones automatizadas simples y proactivas. Así, los sistemas "asegurarán" que "se puedan identificar como tales, trazar y justificar" (a); b) "que sea posible efectuar las mismas actuaciones en forma no automatizada" y c) "que sea posible deshabilitar, revertir o dejar sin efecto las actuaciones automatizadas ya producidas". El CGPJ, acertadamente, echa en falta entre las garantías que "el precepto debería preservar la competencia de dirección procesal, de contenido netamente jurisdiccional, que corresponde a jueces y magistrados […] que podrán establecer las instrucciones pertinentes sobre su uso o deshabilitación" (nº 160, Conclusión 65). [64]

Como garantías para las "actuaciones asistidas" (borradores de resoluciones), el artículo 57.1 del Real Decreto-ley 6/2023 regula que el usuario será el que solicite la generación del borrador y que podrá libre y enteramente modificarlo (art. 57.2). Además, se "requerirá siempre la validación del texto definitivo" por el responsable (art. 57.3).

La Enmienda Núm. 407 del Grupo Parlamentario Socialista añade como garantía que "4. Deberá conservarse registro y traza del borrador documental generado automáticamente, de manera diferenciada a la resolución judicial o procesal finalmente adoptada".

60 "2. Los criterios de decisión serán públicos y objetivos, dejando constancia de las decisiones tomadas en cada momento."

61 "Los sistemas incluirán los indicadores de gestión que se establezcan por la Comisión Nacional de Estadística Judicial y el Comité técnico estatal de la Administración judicial electrónica, cada uno en el ámbito de sus competencias."

62 CGPJ: *Informe,* cit.

63 "5. Cuando se apliquen técnicas de inteligencia artificial, se realizará en la fase de diseño una clasificación del nivel de riesgo del sistema, de conformidad con la clasificación del marco normativo europeo vigente en materia de inteligencia artificial. En concreto, se seguirán los protocolos de valoración de riesgo y catálogo de medidas a aplicar durante el desarrollo y monitorización que establezca el Ministerio para la Transformación Digital y de la Función Pública. En todo caso, dicha valoración de la clasificación del nivel de riesgo del sistema de inteligencia artificial quedará debidamente justificada y documentada."

64 CGPJ: *Informe,* cit.

Apoyándose precisamente en el informe del CGPJ, la Enmienda Núm. 10 del Grupo Parlamentario Plurinacional SUMAR "considera imprescindible establecer un sistema de revisión periódica en el uso de la inteligencia artificial para la ayuda a la emisión de resoluciones judiciales, así como la mención a la necesidad de establecer salvaguardas éticas y de respetar los derechos fundamentales de los justiciables". Es por ello que la enmienda propone que haya un "sistema de uso y gestión de riesgos" y se mencionan principios de la Carta Europea de Ética, [65] así como la supervisión del CGPJ y un informe anual. [66]

Finalmente, puede añadirse más a título anecdótico, por las dificultades de que prospere, que un diputado del Bloque Nacionalista Galego incluye un registro de algoritmos de justicia, aprovechando el texto de la regulación valenciana en el ámbito del sector público. [67] Sin duda, sería de interés un registro de algoritmos judiciales.

Así pues, el Real Decreto-ley 6/2023 recoge legalmente algunas garantías, sin especialidades para el caso de que se trate de un sistema IA el que se utilice para los usos jurisdiccionales. Como se ha explicado, si se trata de sistemas IA para las finalidades de alto riesgo del ámbito jurisdiccional, se sumarán en bloque las garantías que establece el RIA. El conjunto normativo del Real Decreto-ley 6/2023 con el RIA se puede considerar suficientemente robusto a efectos de la legalidad exigible. Aunque se puede mejorar como a continuación se propone.

2. Una propuesta de regulación de garantías.

Me atrevo a señalar algunos mínimos que habría de incorporar la regulación legal, siempre que se consideraran requisitos añadidos no contrarios al RIA. Estos requerimientos los extraigo de diversos supuestos enjuiciados en Derecho comparado, teniendo en cuenta las garantías con las que contaban los sistemas automatizados, además de aquellas que la jurisprudencia comparada consideró necesarias para su admisión constitucional. Estas garantías podrían recogerse en el artículo 58 Real Decreto-ley 6/2023, que podría incluir un texto como el siguiente:

65 "El Comité Técnico Estatal de la Administración Judicial Electrónica deberá desarrollar un sistema de uso y gestión de riesgos en las actuaciones asistidas que permita salvaguardar el derecho a una resolución fundada en Derecho dictada por un juez o tribunal, así como el respeto de los cinco principios de la Carta Europea de Ética".

66 "El Consejo General del Poder Judicial deberá supervisar el funcionamiento (algoritmos) y uso de las actuaciones asistidas y emitirá un informe anual público con los resultados que arroje la evaluación del sistema, proponiendo cuantas mejoras se consideren oportunas para preservar los derechos de los justiciables".

67 Lo cierto es que ni se adapta la redacción para el ámbito de justicia. Se trata de la Enmienda Núm. 565, de Néstor Rego Candamil: "La administración pública responsable en cada caso deberá publicar la relación de sistemas algorítmicos o de inteligencia artificial que tengan impacto en los procedimientos administrativos o la prestación de los servicios públicos con la descripción de manera comprensible de su diseño y funcionamiento, el nivel de riesgo que implican y el punto de contacto al que poder dirigirse en cada caso, de acuerdo con los principios de transparencia y explicabilidad".

A tales efectos, se adoptarán las garantías adecuadas, técnicas y organizativas, incluyendo exigencias de transparencia, tutela jurídica individual y control de supervisión, [68] que correspondan para cada caso de uso según la normativa aplicable y especialmente las exigencias de seguridad y protección de datos, así como las derivadas de la regulación de los sistemas de IA de alto riesgo conforme a la normativa europea.

Asimismo, y en general, deberán aplicarse las siguientes garantías, adecuadas a la naturaleza y especialidad del supuesto concreto de uso del sistema, sus riesgos y posibles impactos:

- Determinación del uso o usos específicos, justificando que se han considerado otras alternativas y técnicas, así como la posibilidad de uso de datos sintéticos.

- Tipo y alcance de los datos o información que se utilizarán.

- Métodos de procesamiento de datos que se emplearán.

- Delimitación de qué órganos, unidades o tipo de servidores públicos podrán realizar los tratamientos o, en su caso, acceder a los datos o información resultante.

- Usos permitidos para los datos resultantes del sistema.

- Prohibición de realizar rastreos indiscriminados o no delimitados en relación con el caso de uso específico autorizado.

- Fecha de inicio prevista y duración.

- Adopción de medidas de seudonimización y de división funcional, justificando si su adopción pudiera comprometer la finalidad del caso de uso.

- Conservación y, en su caso, destrucción de los datos resultantes.

68 A este respecto el TCF alemán añade garantías técnicas y organizativas. Así, "en cualquier caso, el principio de proporcionalidad se traduce en exigencias de transparencia, tutela jurídica individual y control de supervisión (& 103): "un diseño apropiado del control es de gran importancia. En vista del número posiblemente alto de medidas, esto se puede dividir entre delegados de protección de datos independientes y oficiales de acuerdo con un concepto de control graduado y también regulado como un procedimiento aleatorio. Para un control efectivo, es esencial que se proporcionen razones formuladas de forma independiente sobre por qué ciertas bases de datos se analizan por medios automatizados para prevenir ciertos delitos penales. Si se utiliza software, lo que permite formas más complejas de comparación automatizada de datos, también se requieren precauciones para evitar errores que están específicamente asociados con esto, lo que también puede requerir regulaciones legales sobre el estado de seguimiento del desarrollo del software utilizado. [no obstante] Los requisitos específicos que deben imponerse a la protección de acompañamiento no son objeto de este procedimiento." (&109).

- Auditorías externas e independientes de los sistemas utilizados; la posibilidad de subcontratación del uso quedará limitada en la autorización específica.

- Transparencia de los elementos básicos del sistema utilizado y, en su caso, la lógica del sistema, con parámetros de referencia e indicadores.

- En el caso de tratarse de datos resultantes que contribuyan sustancialmente a la decisión procesal o jurisdiccional a adoptar, deberá quedar registrado y trazable el grado de correspondencia entre la decisión automatizada y la decisión finalmente adoptada o, en su caso, validada.

A partir de esta regulación, podrán dictarse normativas para casos de uso particulares o detallar requerimientos específicos[69] para limitar el tipo y alcance de los datos, qué bases de datos se pueden incluir, métodos de procesamiento de datos, supuestos de reutilización de datos de vigilancia, o algunas precauciones técnicas y organizativas, así como detallar las obligaciones de documentación, publicación y transparencia. [70] La adecuación de estas garantías a cada caso concreto se realizará a través del sistema de autorización previa del caso de uso por parte de la autoridad competente. Dicha autorización habrá de publicarse, y sus determinaciones deberán ser comprensibles y contener las especificaciones oportunas.

69 El TCF alemán sí que indica los mínimos que sí que ha de regular la ley. Así:
- "la propia ley deberá regular qué bases de datos se pueden incluir y en qué medida se puede automatizar" (&116),
- "el legislador también debe asegurarse de limitar el uso automatizado al que solo tienen acceso los empleados policiales debidamente calificados […no obstante] Los detalles técnicos pueden ser regulados en reglamentos administrativos a ser publicados." (&117)
- "la propia ley debe regular que los datos obtenidos de la vigilancia domiciliaria o búsquedas en línea se utilicen en un análisis o evaluación de datos que sirva para evitar que se cometan delitos (&118),
- el "uso posterior debe limitarse […] a partir de enfoques de investigación concretos […] de importancia comparable" (&118),
- "también debe regular […] precauciones técnicas y organizativas apropiadas" (&118),
- "la información procedente de la recopilación intensiva de datos debe marcarse o separarse con antelación para impedir el acceso en caso necesario y no debe identificarse posteriormente". (&118),
- "respecto al tipo y alcance de los datos que se pueden utilizar en el análisis o evaluación de datos automatizados […] la reserva legal también se aplica a este respecto" (&119)
- "Si el legislador desea reducir la intensidad de la intervención del análisis o evaluación de datos […] también debe hacer especificaciones restrictivas para el método de los datos automatizados." (&120)

70 Cabe apuntar que el TCF alemán permite la colaboración normativa y remisión legal a las autoridades (&110 y ss.). Así, "En principio, el legislador puede dividir esta tarea normativa entre él mismo y la administración (1). Sin embargo, debe asegurarse de que, cumpliendo con la disposición legal, se establezcan suficientes regulaciones, en particular para limitar el tipo y el alcance de los datos (2) y para limitar los métodos de procesamiento de datos (3)." (&110). Se afirma que "el legislador puede exigir a las autoridades administrativas que especifiquen con mayor precisión las determinaciones abstractas […] la especificación mediante normas administrativas requiere en todo caso una base legal […] el legislador debe asegurarse de que las autoridades documenten y publiquen de manera comprensible las determinaciones de precisión y uniformidad que regirán en última instancia la aplicación de las disposiciones en el caso particular […] puede exigir a las autoridades administrativas que especifiquen más las determinaciones abstractas y generales (&113).

V. PARA TERMINAR: SÓLO EL CGPJ PUEDE SER LA AUTORIDAD DE SUPERVISIÓN DE LOS SISTEMAS DE IA JURISDICCIONALES DE ALTO RIESGO.

1. Las autoridades de vigilancia del Reglamento de IA y sus facultades.

El RIA sigue el esquema establecido por el llamado "nuevo marco legislativo" de la UE, un conjunto normativo que establece unas bases comunes sobre la comercialización, evaluación y vigilancia de productos en la Unión Europea. [71] Se trata de una estructura para que los productos y bienes de cierta peligrosidad se pongan en el mercado de modo fiable y seguro, sin generar daños a las personas o lesiones de derechos fundamentales. Para ello deben contar con una evaluación de conformidad y demostrar el cumplimiento de normas y estándares técnicos. En nuestro caso y como se ha analizado, el "producto peligroso" son los sistemas IA de alto riesgo del Anexo III. 6º y 8º de uso jurisdiccional. Además del propio RIA como norma especial, cabe tener especialmente en cuenta el Reglamento (UE) 2019/1020 sobre vigilancia del mercado como norma general. Por lo que ahora interesa, una vez un sistema de IA de alto riesgo se pone en el mercado, las llamadas "autoridades de vigilancia del mercado" (AVM) tienen la competencia para supervisar que esos sistemas de IA cumplen con el RIA. Cada Estado debe designar una o varias AVM de IA, de las que solo una actúa como oficina de enlace con la Comisión Europea para tareas de coordinación (art. 10.1º Reglamento (UE) 2019/1020, art. 70 RIA). [72] Asimismo, los Estados miembros deben proporcionar a las AVM las facultades, los recursos y la pericia necesarios para desempeñar efectivamente sus funciones (art. 14.1º Reglamento (UE) 2019/1020). Han de contar con "recursos técnicos, financieros y humanos adecuados, y de infraestructuras", así como personal con conocimientos específicos (art. 70.3º RIA). [73] Será obligatorio informar a la Comisión sobre el establecimiento en un año desde la entrada en

71 Dicho Nuevo Marco Legislativo se rige por tres normas: el Reglamento (CE) núm.º 765/2008 del Parlamento Europeo y del Consejo por el que se establecen los requisitos de acreditación y vigilancia del mercado de los productos; la Decisión núm.º 768/2008/CE del Parlamento Europeo y del Consejo sobre un marco común para la comercialización de los productos y; el Reglamento (UE) 2019/1020 del Parlamento Europeo y del Consejo relativo a la vigilancia del mercado y la conformidad de los productos.

72 En el caso del RIA "Los Estados miembros comunicarán a la Comisión la identidad de las autoridades notificantes y de las AVM y las funciones de dichas autoridades, así como cualquier cambio posterior al respecto. […] Los Estados miembros designarán una AVM que actúe como punto de contacto único para el presente Reglamento y notificarán a la Comisión la identidad de dicho punto." (art. 70. 2º RIA).

73 3. Los Estados miembros garantizarán que sus autoridades nacionales competentes dispongan de recursos técnicos, financieros y humanos adecuados, y de infraestructuras para el desempeño de sus funciones de manera efectiva con arreglo al presente Reglamento. En concreto, las autoridades nacionales competentes dispondrán permanentemente de suficiente personal cuyas competencias y conocimientos técnicos incluirán un conocimiento profundo de las tecnologías de IA, datos y computación de datos; la protección de los datos personales, la ciberseguridad, los riesgos para los derechos fundamentales, la salud y la seguridad, y conocimientos acerca de las normas y requisitos legales vigentes. Los Estados miembros evaluarán y, en caso necesario, actualizarán anualmente los requisitos en materia de competencias y recursos a que se refiere el presente apartado.

vigor del RIA (art. 70.6º RIA).[74] Para que las AVM puedan realizar la evaluación y comprobación del cumplimiento normativo de los sistemas de IA, deben contar con unos poderes mínimos (art. 14.4º Reglamento (UE) 2019/1020):

- Los responsables u operadores de los sistemas IA deben facilitar acceso a información, declaraciones de conformidad o documentación técnica, incluso el acceso al código fuente.

- Las AVM deben poder realizar sin previo aviso inspecciones "in situ" y comprobaciones, obtener pruebas, acceder a establecimientos, iniciar investigaciones.

- Deben poder exigir que se adopten medidas, así como la facultad de imponer medidas correctivas y sanciones.

- Deben poder adquirir de forma encubierta muestras para detectar incumplimientos y obtener pruebas.

- Suprimir contenidos de interfaces en línea o exigir a proveedores de servicios de la sociedad de la información que restrinjan el acceso.

- Funciones específicas en supuestos de exención de evaluación de la conformidad, así como respecto de las pruebas de los sistemas IA en condiciones reales.

2. La AESIA no podría ser la autoridad de vigilancia para el ámbito judicial por falta de independencia.

Cada Estado designa a las diferentes AVM, pero el RIA fija algunos condicionamientos especialmente importantes en el ámbito de nuestro interés. Respecto de los sistemas de IA de alto riesgo para el cumplimiento de la ley, inmigración y asilo o administración de justicia, así como para sistemas de IA de identificación biométrica, el Reglamento de IA exige que las AVM que supervisen estos sistemas sean las autoridades nacionales de protección de datos. Si no son estas autoridades, deben ser autoridades que cuenten con un nivel de independencia similar (art. 74.8 RIA).[75] Es necesario explicar que el RIA exige para

74 6. A más tardar el … [un año a partir de la fecha de entrada en vigor del presente Reglamento] y cada dos años a partir de entonces, los Estados miembros presentarán a la Comisión un informe acerca del estado de los recursos financieros y humanos de las autoridades nacionales competentes, que incluirá una evaluación de su idoneidad. La Comisión remitirá dicha información al Comité para que mantenga un debate sobre ella y, en su caso, formule recomendaciones.

75 8. En el caso de los sistemas de IA de alto riesgo enumerados en el anexo III del presente Reglamento, punto 1 [identificación biométrica], en la medida en que los sistemas se utilicen a los efectos de la garantía del cumplimiento del Derecho, la gestión de fronteras y la justicia y la democracia, y en el caso de los sistemas de IA de alto riesgo enumerados en el anexo III, puntos 6, 7 y 8, del presente Reglamento [precisamente estos ámbitos], los Estados miembros designarán como autoridades de vigilancia del mercado a efectos del presente Reglamento bien a las autoridades de control encargadas de la protección de datos competentes con arreglo al Reglamento (UE) 2016/679 o a la Directiva (UE) 2016/680, bien a cualquier otra autoridad

las AVM un nivel de independencia general y, para los casos que ahora interesan, un nivel de independencia especial. En España, en principio, habría de ser la AEPD la autoridad de supervisión respecto de estos sistemas, porque la Autoridad Española de Supervisión de la Inteligencia Artificial (AESIA) ni de lejos cuenta con este especial nivel de independencia.

España ha sido el primer país de la UE en establecer una AVM, la AESIA.[76] La AESIA dudosamente cumple con los generales requisitos de "independencia" que exige el RIA. A este respecto, el RIA originalmente no requería la independencia e imparcialidad de la AVM. Sin embargo, el éxito de la enmienda 123 del Parlamento al considerando 77 y la enmienda 558 con el nuevo artículo 59.4º RIA, lleva a que finalmente se exija en general la "total independencia", y se caracteriza a la AVM como "independiente, imparcial y objetiva". En la versión final, la "independencia" se aclara en los considerandos (76, 77 bis y 80-x) y en el artículo 59.2º RIA. Es de cuestionable que este nivel general de independencia lo cumpla la AESIA. La AESIA se creó como un organismo público bajo el artículo 91 de la Ley 40/2015 y no como una agencia estatal independiente de acuerdo con los artículos 108 bis y siguientes de esta Ley. En sus estatutos regulados por el Real Decreto 729/2023, de 22 de agosto, el artículo 8 menciona como "Principios de actuación de la Agencia" la "Autonomía" y la "Independencia técnica" y señala que "la Agencia actuará con plena autonomía".[77] No obstante, estas afirmaciones parecen insuficientes, especialmente dada una evidente falta de independencia orgánica que afecta a la independencia funcional. Incluso se establece explícitamente la "dependencia" de la Dirección de un órgano político como el Secretario de Estado, quien es el Presidente y desempeña algunas funciones materiales (art. 23.1º).

En Derecho de la UE se puede afirmar que cuanto más vinculada esté una autoridad al ámbito de los derechos fundamentales o a la protección del consumidor, mayor independencia se requiere, hasta el máximo nivel, que es el exigido para la protección de datos.[78] Aunque no exista una doctrina jurisprudencial

designada con arreglo a las mismas condiciones establecidas en los artículos 41 a 44 de la Directiva (UE) 2016/680. Las actividades de vigilancia del mercado no afectarán en modo alguno a la independencia de las autoridades judiciales ni interferirán de otro modo en sus actividades en el ejercicio de su función judicial." Cabe recordar que los artículos 41 a 44 de la Directiva (UE) 2016/680 imponen la "total independencia" de la autoridad de control, orgánica y funcional.

76 La creación legal y habilitación fue por la Ley 28/2022, de 21 de diciembre, en concreto, su D.A 7ª reguló la creación. Asimismo, según Ley 28/2022, la AESIA está adscrita orgánica al Ministerio de Asuntos Económicos y Transformación Digital, a través de su Secretaría-o SEDIA. El Real Decreto 729/2023, de 22 de agosto, por el que se aprueba el Estatuto.

77 "a) Autonomía, entendida como la capacidad de la Agencia de gestionar, en los términos previstos en su Estatuto, los medios puestos a su disposición para alcanzar los objetivos comprometidos."

"b) Independencia técnica, basada en la capacitación, especialización, profesionalidad y responsabilidad individual del personal al servicio de la Agencia que deberá observar los valores de competencia, ética profesional y responsabilidad pública que son de aplicación. En el desempeño de sus funciones y en el ejercicio de sus competencias, la Agencia actuará con plena autonomía."

78 Así lo afirma el abogado General del TJUE: "125. Por lo demás, también en otros sectores del Derecho de la Unión en los que ha sido necesario instituir autoridades independientes con obligaciones destinadas a

muy consolidada en casos que no involucran derechos fundamentales, el TJUE es bastante exigente en cuanto a la independencia y que "El sistema del Derecho de la Unión privilegia una concepción amplia de la independencia respecto a las competencias específicas asignadas a las autoridades independientes." [79]

Lo que de verdad interesa ahora es que en el terreno de aplicación de la ley, inmigración y asilo, administración de justicia, procesos electorales, así como el uso de sistemas de IA de identificación biométrica en estos ámbitos, el RIA deja muy claro que el estándar que se exige expresamente es el más alto. El estándar máximo de independencia es el de las autoridades de protección de datos, que ha alcanzado estatus "constitucional" en el derecho de la UE. [80] El RGPD establece una regulación muy exhaustiva, [81] también los artículos 41 y siguientes de la Directiva (UE) 2016/680 en el ámbito penal y judicial. En ningún caso la AESIA podría ser la AVM para los ámbitos de interés judicial que aquí ocupan. La AESIA solo podría ser la AVM si contase una nueva ley la estableciera como "Autoridad administrativa independiente" según el artículo 109 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

3. La AEPD tampoco puede ser la autoridad para la inteligencia artificial de uso jurisdiccional, sólo el CGPJ.

En principio, la AEPD sería la AVM para el ámbito de uso jurisdiccional de sistemas de alto riesgo. Ello sería así por su independencia y porque ya tiene competencias en el tratamiento de datos en estos ámbitos. Sin embargo, tampoco lo puede ser en España.

Actualmente, respecto de los tratamientos de datos relativos a las actividades de aplicación de la ley (Anexo III.6 RIA) o gestión de migraciones y asilo (Anexo III.7 RIA), la AEPD es la autoridad independiente de protección de datos (art. 48 Ley Orgánica 7/2021, de 26 de mayo). [82] Ahora bien, esto solo aplica cuando estas

crear un mercado competitivo que sea capaz de tutelar de forma simultánea otros objetivos, expresamente indicados y regulados por el legislador europeo, como por ejemplo la protección de derechos fundamentales específicos y de los derechos del consumidor, la interpretación del concepto de independencia proporcionada por el Tribunal de Justicia ha sido lo más amplia posible." Conclusiones del Abogado General Giovanni Pitruzzella, presentadas el 14 de enero de 2021, Asunto C-718/18, Comisión Europea contra República Federal de Alemania, para un supuesto no relativo a protección de datos, con análisis de diversas sentencias sobre la independencia de las autoridades independientes. https://curia.europa.eu/juris/document/document.jsf?text=%2522autoridades%2Bindependientes%2522%2B%2522independencia%2Bfuncional%2522%2B%2522derechos%2Bfundamentales%2522&docid=236435&pageIndex=0&doclang=ES&mode=req&dir=&occ=first&part=1&cid=1817917#ctx1.

79 Cabe acudir a las Conclusiones referidas, ver en especial 104, 105, 127 y la cita de 128.

80 Artículo 8 Carta derechos fundamentales UE, "3. El respeto de estas normas estará sujeto al control de una autoridad independiente."

81 Capítulo VI. Autoridades de control independientes, Sección 1, Independencia: Artículo 51 Autoridad de control; Artículo 52 Independencia; Artículo 53: Condiciones generales aplicables a los miembros de la autoridad de control, Artículo 54, Normas relativas al establecimiento de la autoridad de control.

82 Artículo 48. Autoridades de protección de datos: A los efectos de esta Ley Orgánica son autoridades de protección de datos independientes: a) La Agencia Española de Protección de Datos. b) Las autoridades

actividades las realizan los Cuerpos y Fuerzas de Seguridad, pues el escenario cambia cuando estos tratamientos de datos en estas áreas son realizados en el ejercicio de la función jurisdiccional. En estos casos, ni la AESIA ni la AEPD pueden ser la autoridad de control o supervisión.

La autoridad de protección de datos personales con fines jurisdiccionales debe ser el CGPJ. Esto es así por razones constitucionales que se reflejan en la regulación específica desde 2005, luego en la LOPJ desde 2015, y más recientemente actualizada en 2021. Veámoslo.

A efectos de la protección de datos, [83] el artículo 236 bis 1º LOPJ distingue entre tratamientos de datos personales realizados con fines jurisdiccionales y no jurisdiccionales, según "se encuentren incorporados a los procesos que tengan por finalidad el ejercicio de la actividad jurisdiccional". [84] Respecto de las actividades jurisdiccionales, según los artículos 236 octies y 236 nonies LOPJ y el artículo 53.3 LOPD, [85] la autoridad de control de protección de datos en el ámbito de la Administración de Justicia es el CGPJ. Dentro del CGPJ, estas funciones están asignadas a la Dirección de Supervisión y Control de Protección de Datos. [86] Sin embargo, "los tratamientos de datos con fines no jurisdiccionales estarán sometidos a la competencia de la AEPD" (artículo 236 octies 2º LOPJ).

La competencia es del CGPJ no solo porque la LOPJ lo exija, sino porque constitucionalmente no puede ser la AEPD la autoridad en el ámbito jurisdiccional. Para ello hay que acudir a la STS 2 diciembre 2011, [87] que aborda si la AEPD tiene competencia para actuar como autoridad de control respecto al poder judicial, en particular, sobre los órganos judiciales y sus ficheros de datos de carácter personal. El TS fue claro en su amplio FJ 3º: la AEPD, pese a su independencia funcional, es parte del poder ejecutivo, con potestades de intervención y sanción en materia de protección de datos, pero estas potestades no incluyen la capacidad para imponer sanciones a las administraciones públicas directamente, sino solo establecer medidas correctoras o promover responsabilidad disciplinaria. Considera el TS que

autonómicas de protección de datos, exclusivamente en relación a aquellos tratamientos de los que sean responsables en su ámbito de competencia, y conforme a lo dispuesto en el artículo 57.1 de la Ley Orgánica 3/2018, de 5 de diciembre, y en la normativa autonómica aplicable.

83 Una descripción de la situación normativa en CGPJ: *Ley Orgánica del Poder Judicial. Dirección de supervisión y control de protección de datos*, https://www.poderjudicial.es/cgpj/es/Temas/Autoridad-de-control-de-proteccion-de-datos/Normativa/LOPJ/#:~:text=El%20art%C3%ADculo%20236%20bis%20distingue,ejercicio%20de%20la%20actividad%20jurisdiccional.

84 Artículo 236 bis: "1. El tratamiento de los datos personales podrá realizarse con fines jurisdiccionales o no jurisdiccionales. Tendrá fines jurisdiccionales el tratamiento de los datos que se encuentren incorporados a los procesos que tengan por finalidad el ejercicio de la actividad jurisdiccional."

85 "3. Cuando se trate de órganos judiciales u oficinas judiciales el ejercicio de las facultades de inspección se efectuará a través y por mediación del Consejo General del Poder Judicial."

86 Al respecto de esta Dirección, https://www.poderjudicial.es/cgpj/es/Temas/Direccion-de-supervision-y-control-de-proteccion-de-datos/.

87 STS 2 diciembre 2011 (ECLI:ES:TS:2011:8497).

la intervención de la AEPD en asuntos internos del poder judicial, incluyendo los ficheros de datos personales gestionados por los órganos judiciales, podría vulnerar el principio de independencia judicial. La función de garantizar la protección de los datos personales en este ámbito recae exclusivamente en el CGPJ. Así, el CGPJ es reconocido por la Constitución y la LOPJ como el órgano de gobierno exclusivo del poder judicial y por ello le corresponde sólo a él la supervisión y el control de la actividad no jurisdiccional de jueces y magistrados, así como la administración de los ficheros de datos de carácter personal bajo responsabilidad judicial.[88] Esto implica la exclusión de la competencia de la AEPD.

Por lo tanto, considero que procede replicar los mismos argumentos del TS respecto de la competencia del CGPJ -y no de la AEPD- en la supervisión de los sistemas de IA en toda actividad propiamente jurisdiccional en los ámbitos de aplicación de la ley, inmigración o asilo, u otros jurisdiccionales (apartados 6, 7 y especialmente 8º del Anexo III RAI). El Estado debe designar al CGPJ. Cabe señalar que el CGPJ ya alertó de la necesidad de especificar sus funciones en el Real Decreto-ley 6/2023.[89] Aunque esta cuestión excede el presente estudio, puede intuirse que la asignación se realice a la Dirección de Supervisión y Control de Protección de Datos y que para poder desarrollarla ésta deberá mutar su nombre, finalidades y capacidades. Las actuales capacidades y medios de esta Dirección pueden ser discutibles. Se requerirá una colaboración entre el CGPJ con la AEPD y la AESIA -sin duda más dotados y especializados en la materia-para asegurar estas autoridades puedan aportar su expertise específico, obviamente, sin comprometer la independencia y eficacia del CGPJ. Algo similar procedería señalar respecto del uso de IA de alto riesgo por la Fiscalía. La regulación actual de la LOPJ asigna la competencia de protección de datos a la propia Fiscalía y no a la AEPD. No obstante, desconozco si esto es simplemente una opción legislativa o se debe a una interpretación de la Constitución como en el caso de la referida STS sobre el CGPJ.

88 En el caso concreto, la AEPD carecía de competencia para declarar la infracción por parte de un órgano judicial, en este caso, el Juzgado de lo Contencioso-Administrativo núm. 1 de A Coruña, y, por tanto, anuló la resolución.

89 El CGPJ, *Informe*, cit., alertaba de que "nada se dice acerca de la posición que corresponde al CGPJ en la evaluación, supervisión y control de este tipo de sistemas que impactan directamente sobre el núcleo de la función jurisdiccional." (núm. 167).

BIBLIOGRAFÍA

[s.a]: *Opinions on Regulating and Strengthening the Application of Artificial Intelligence in Judicial Fields*, diciembre de 2022, https://www-old.ciftis.org/article/14978341100187648.html.

AA. VV.: *Tratado sobre el Reglamento de Inteligencia Artificial de la Unión Europea* (coord. por L. Cotino Hueso y P. Simó Castellanos), Aranzadi, 2024.

AA. VV.: *El impacto de las tecnologías disruptivas en el derecho procesal* (dir. por F. Bueno de Mata), Aranzadi Thomson Reuters, 2022.

Amoni Reverón, G. A.: "Libertad, presunción de inocencia y defensa ante la irrupción de la inteligencia artificial en el ámbito policial y judicial penal", en AA.VV.: *Derechos y garantías ante la inteligencia artificial y las decisiones automatizadas* (ed. por L. Cotino Hueso), Thompson-Reuters Aranzadi, Cizur, 2022, pp. 193-236.

Barona Vilar, S.: "La seductora algoritmización de la justicia. Hacia una justicia poshumanista (Justicia+) ¿utópica o distópica?", en AA.VV.: *Justicia poliédrica en periodo de mudanza: Nuevos conceptos, nuevos sujetos, nuevos instrumentos y nueva intensidad* (ed. por S. Barona Vilar), Tirant lo Blanch, Valencia, 2022, pp. 36-47.

Barona Vilar, S.: "La seductora algoritmización de la justicia. Hacia una justicia poshumanista (Justicia+) ¿utópica o distópica?", *El Cronista del Estado Social y Democrático de Derecho*, 2022, núm. 100, pp. 36-47.

Barona Vilar, S.: "Una justicia 'digital' y 'algorítmica' para una sociedad en estado de mudanza", en *Justicia algorítmica y neuroderecho. Una mirada multidisciplinar* (ed. por S. Barona Vilar), Tirant lo Blanch, Valencia, 2021.

Barona Vilar, S.: *Algoritmización del Derecho y de la Justicia. De la Inteligencia Artificial a la Smart Justice*, Tirant lo Blanch, Valencia, 2021.

CEPD: *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*, Version 1.0, 12 mayo 2022, https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-052022-use-facial-recognition_en.

Cernada Badía, R.: "De la digitalización a la inteligencia artificial: el porvenir de la justicia en la Unión Europea", en AA.VV.: *Algoritmos abiertos y que no discriminen en el sector público* (coord. por Cotino Hueso y P. Simó Castellanos), Tirant lo Blanch, Valencia, 2023, pp. 239-264.

CGPJ: *Informe al Anteproyecto de ley de eficiencia digital del Servicio público de justicia, Acuerdo adoptado por el Pleno*, de, 24 de febrero de 2022, https://www.poderjudicial.es/stfls/CGPJ/COMISI%C3%93N%20DE%20ESTUDIOS%20E%20INFORMES/INFORMES%20DE%20LEY/FICHERO/20220224%20Informe%20al%20anteproyecto%20de%20Ley%20de%20Eficiencia%20Digital%20del%20Servicio%20P%C3%BAblico%20de%20Justicia.pdf.

CGPJ: *Ley Orgánica del Poder Judicial. Dirección de supervisión y control de protección de datos*, https://www.poderjudicial.es/cgpj/es/Temas/Autoridad-de-control-de-proteccion-de-datos/Normativa/LOPJ/#:~:text=El%20art%C3%ADculo%20236%20bis%20distingue,ejercicio%20de%20la%20actividad%20jurisdiccional.

Comisión Europea: *Comunicación de la Comisión al Parlamento europeo, al Consejo, al Comité Económico y Social europeo y al Comité de las Regiones: La digitalización de la justicia en la UE: Un abanico de oportunidade*s {SWD(2020) 540 final}, de 2 de diciembre de 2020.

Comisión Europea: *Study on the use of innovative technologies in the justice field – Final report*, Dirección General de Justicia y Consumidores Publications Office, Bruselas, septiembre de 2020, https://data.europa.eu/doi/10.2838/58510

Corvalán, J. G.: "Inteligencia artificial: retos, desafíos y oportunidades-Prometea: la primera inteligencia artificial de Latinoamérica al servicio de la Justicia", *Revista de Investigações Constitucionais*, 2018, vol. 5, pp. 295-316.

Cotino, L.: "Transparencia y explicabilidad de la inteligencia artificial y "compañía" (comunicación, interpretabilidad, inteligibilidad, auditabilidad, testabilidad, comprobabilidad, simulabilidad…). Para qué, para quién y cuánta", en AA.VV.: *Transparencia y explicabilidad de la inteligencia artificial* (coord. por Cotino Hueso y P. Simó Castellanos), Tirant lo Blanch, Valencia, 2022.

Cotino, L.: "Reconocimiento facial automatizado y sistemas de identificación biométrica bajo la regulación superpuesta de inteligencia artificial y protección de datos", en AA.VV.: *Derecho público de la inteligencia artificial* (coord. por F. Balaguer Callejón y L. Cotino Hueso), F. Jiménez Abad-Marcial Pons, Madrid, 2023, pp. 347-402, acceso

Cotino, L.: "Una regulación legal y de calidad para los análisis automatizados de datos o con inteligencia artificial. Los altos estándares del Tribunal Constitucional alemán y otros tribunales, que no se cumplen ni de lejos en España", *Revista General de Derecho Administrativo*, núm. 63, 2023. acceso

Cotino, L.: "Cómo abordar jurídicamente el impacto de la inteligencia artificial en los derechos fundamentales", en *Derecho y Tecnologías*, Fundación Ramón Areces, Madrid, 2024.

Cotino, L.: "La primera sentencia del Tribunal de Justicia de la Unión Europea sobre decisiones automatizadas y sus implicaciones para la protección de datos y el Reglamento de inteligencia artificial", *Diario La Ley*, enero de 2024, https://ir.uv.es/V14YNLI

Estevez, E. y otros: *PROMETEA: Transformando la Administración de Justicia con herramientas de inteligencia artificial*, BID, Washington, 2020.

Fernández, C. B.: "Proyecto de Ley de Medidas de Eficiencia Digital del Servicio Público de Justicia", *Derecho Digital e Innovación. Digital Law and Innovation Review*, 2022, núm. 13 (julio-septiembre).

IALAB: *Directrices de uso de la IA generativa de texto y ChatGPT en la Justicia* (dir. por J.G. Corvalán y M. Sánchez Caparrós), Thomson Reuters-La Ley- IALAB, 2023, https://ialab.com.ar/wp-content/uploads/2023/11/Guia-de-directrices-usos-de-ChatGPT-e-IA-generativa-en-la-justicia.pdf.

Le Fevre Cervini: *Uso estratégico de datos e inteligencia artificial en la justicia. Informe 6.* Caracas: CAF. 2022, https://scioteca.caf.com/handle/123456789/1932.

Martínez Garay, L. y García Ortiz A. M.: "Paradojas de los algoritmos predictivos utilizados en el sistema de justicia penal", *El Cronista del Estado Social y Democrático de Derecho*, 2022, núm. 100, pp. 160-173.

Ministerio de Modernización de la Nación: "Kit de Innovación", https://acortar.link/WRqYxg.

Miró Llinares, F.: "Inteligencia artificial, delito y control penal: nuevas reflexiones y algunas predicciones sobre su impacto en el derecho y la justicia penal", *El Cronista del Estado Social y Democrático de Derecho*, 2022, núm. 100, pp. 174-183.

Montesinos García, A.: "Afectación de los derechos y garantías procesales por el empleo de algoritmos predictivos", en AA.VV.: *El proceso como garantía* (dir. por J. M. Asencio Mellado y O. Fuentes Soriano.), Atelier, Madrid, 2023, pp. 703-714.

Montesinos García, A.: "Empleo de la inteligencia artificial en algunas fases del proceso judicial civil: prueba, medidas cautelares y sentencia", *Actualidad civil*, 2022, núm. 11.

Montoro Sánchez, J. A.: "Actuaciones judiciales automatizadas en el Proyecto de Ley de eficiencia digital del servicio público de justicia", en AA.VV.: *Logros y retos de la justicia civil en España* (dir. por F. Jiménez Conde y otros), Tirant lo Blanch, Valencia, pp. 687-704.

Nieva Fenoll, J.: *Inteligencia artificial y proceso judicial*, Marcial Pons, 2018.

Nieva Fenoll, J.: "Perder el control digital: ¿hacia una distopía judicial?", en AA.VV.: *El proceso judicial en un marco cultural y digital* (dir. por S. Calaza López), Colex, 2023.

Olivares Olivares, B. D.: "Law and Artificial Intelligence in the Spanish Tax Administration: the Need for a Specific Regulation", *European Review of Digital Administration* & Law-ERDAL 1 (1-2), pp. 227-234.

Palomar Olmeda, A.: "La actuación judicial automatizada", en AA.VV.: *Las tecnologías de la información y la comunicación en la administración de justicia. La Ley 18/2011 y la administración electrónica en el sistema judicial* (coord. por E. Gamero Casado y J. Valero Torrijos), Aranzadi, Cizur Menor, 2012, pp. 659-704.

Ponce Solé, J.: "Inteligencia artificial, Derecho administrativo y reserva de humanidad: algoritmos y procedimiento administrativo debido tecnológico", en Monográfico sobre IA (coord. por A. Boix y L. Cotino), *Revista General de Derecho Administrativo*, 2019, núm. 50.

Roberto Granero, H.: "Derechos y garantías concretas frente al uso de inteligencia artificial y decisiones automatizadas, especialmente en el ámbito judicial y de aplicación de la ley", en AA.VV.: *Derechos y garantías ante la inteligencia artificial y las decisiones automatizadas* (ed. por L. Cotino Hueso), Thomson-Reuters Aranzadi, Cizur, 2022, pp. 107-137.

Simón Castellano, P. y Pérez Domínguez, S.: "Attitudes and perceptions regarding algorithmic judicial judgement: barriers to innovation in the judicial system?, *IDP: revista de Internet, derecho y política*, 2023, núm. 39 ("Digitalització y algoritmització de la justicia").

Stern R.E. y otros: "Automating Fairness? Artificial Intelligence in the Chinese Court", *Columbia Journal of Transnational Law,* 2021, núm. 59, pp. 515-553, https://scholarship.law.columbia.edu/faculty_scholarship/2940.

EL USO DE SISTEMAS DE INTELIGENCIA ARTIFICIAL (IA) DE IDENTIFICACIÓN BIOMÉTRICA REMOTA EN ESPACIOS PÚBLICOS EN LA LEY EUROPEA DE IA*

THE USE OF ARTIFICIAL INTELLIGENCE (AI) SYSTEMS FOR REMOTE BIOMETRIC IDENTIFICATION IN PUBLICLY ACCESSIBLE SPACES IN THE EUROPEAN AI LAW

Actualidad Jurídica Iberoamericana Nº 21, agosto 2024, ISSN: 2386-4567, pp. 528-565

* Este trabajo ha sido redactado en el marco del Proyecto de investigación "Claves para una justicia digital y algorítmica con perspectiva de género" (expediente: PID2021-123170OB-I00) financiado por MCIN/AEI/10.13039/501100011033.

José Francisco
ETXEBERRIA
GURIDI

ARTÍCULO RECIBIDO: 29 de mayo de 2023
ARTÍCULO APROBADO: 1 de julio de 2024

RESUMEN: El uso de la biometría para el esclarecimiento y persecución de hechos criminales y, sobre todo, de su autor tiene un largo recorrido histórico. La aplicación de sistemas de inteligencia artificial con tales fines de identificación biométrica multiplica exponencialmente su eficacia. Pero, a su vez, se incrementa la afectación en los derechos de los ciudadanos. El texto de la Ley Europea de Inteligencia Artificial aborda esta delicada cuestión no sin dejar de suscitar una viva polémica.

PALABRAS CLAVE: Artificial Intelligence; remote biometric identification; personal data; private life.

ABSTRACT: *The use of biometrics to clarify and prosecute criminal acts and, above all, their perpetrator has a long. The application of artificial intelligence systems for such biometric identification purposes multiplies their effectiveness exponentially. But, at the same time, the impact on citizens' rights increases. The text of the European Artificial Intelligence Act addresses this delicate issue, but without failing to spark lively controversy.*

KEY WORDS: *Inteligencia Artificial; identificación biométrica remota; datos personales; vida privada.*

I. INTRODUCCIÓN.

La biometría en cuanto estudio de los fenómenos o procesos biológicos, ha estado muy presente a lo largo de la evolución del Derecho. Usualmente del Derecho Penal o Procesal Penal, pero no de forma exclusiva. Dejando ahora al margen los extremos de las teorías de LOMBROSSO, las aportaciones extraordinarias de la criminalística tienen con frecuencia como fundamento precisamente el análisis de vestigios de carácter biológico como es el caso de las pruebas de ADN o de las huellas dactilares, entre otros[1]. No hay que perder de vista que una de las funciones del proceso penal consiste justamente en acreditar la autoría de los hechos criminales, esto es, determinar el elemento subjetivo del objeto que se va a juzgar en dicho proceso.

Los rasgos físicos, fisiológicos o de naturaleza similar que resultan adecuados al efecto de identificar a personas concretas pueden ser tratados con sistemas de Inteligencia Artificial (IA) potenciando exponencialmente su eficacia individualizadora, mediante el tratamiento algorítmico de los datos de carácter biométrico[2]. De este modo, estos sistemas se tornan en eficaces instrumentos que admiten múltiples aplicaciones. Sobre este punto, ya hace más de una década el Grupo de Trabajo del Art. 29 de la Directiva 95/46/CE, de 24 de octubre de 1995, sobre tratamiento de datos personales y a la libre circulación de estos

1 Vid. sobre algunos antecedentes al respecto Richard González, M.: "Los sistemas biométricos de reconocimiento facial en la Unión Europea en el marco del desarrollo de la Inteligencia Artificial", *Justicia*, 2023, núm. 1, pp. 158-160.

2 El desarrollo de la tecnología permitiría que la obtención, registro y cotejo de datos biométricos se produzca con una rapidez y eficacia no vista hasta ahora. Vid. Richard González, M.: "Los sistemas", cit., p. 153; Cotino Hueso, L.: "Reconocimiento facial automatizado y sistemas de identificación biométrica bajo la regulación superpuesta de inteligencia artificial y protección de datos", en AA.VV.: *Derecho Público de la Inteligencia Artificial*, (coord. por F. Balaguer Callejón y L. Cotino Hueso), Fundación Manuel Giménez Abad, Madrid, 2023, pp. 354 y ss.

• José Francisco Etxeberria Guridi
Catedrático de Derecho Procesal. Universidad del País Vasco/Euskal Herriko Unibertsitatea. Correo electrónico: patxi.etxeberria@ehu.eus

datos[3], distinguía su uso como: a) Medio de autenticación/verificación biométrica ("one-to-one comparison"). En este supuesto se comparan dos plantillas biométricas pertenecientes supuestamente a la misma persona para determinar si, efectivamente, la persona que aparece en ambas es la misma. Este proceso de búsqueda de correspondencias "uno-a-uno" admite varias modalidades. Por ejemplo, lo usual resulta que una de las plantillas biométricas se halle previamente almacenada y en el momento en que interese se obtenga la segunda plantilla. Pero no siempre resulta necesario el almacenamiento de dicha plantilla en un fichero[4]; b) Medio de identificación biométrica ("one-to-many comparison"). En estos supuestos, la plantilla biométrica que se obtiene se compara con otras plantillas biométricas almacenadas en uno o en varios ficheros o bases de datos, esto es, se trataría de un proceso de búsqueda de correspondencias "uno-a-varios". En esta modalidad de identificación se pueden distinguir aquellos supuestos en los que la comparación se realiza frente a un fichero o base de datos en el que conste que figura la plantilla biométrica de la persona a identificar ("closed-set identification"), de aquéllos en los que la búsqueda de correspondencia se realiza sin tener constancia de dicha circunstancia ("open-set identification"); y c) Medio de categorización/segregación biométrica ("matching general characteristics"). En esta modalidad el sistema biométrico actúa como un proceso que permite extraer características de un individuo con el objeto de determinar su pertenencia a un grupo con características predefinidas a fin de adoptar una medida específica. En este caso, lo importante no es identificar o verificar a un individuo, sino asignarle automáticamente una categoría determinada (la pertenencia a un grupo étnico, la edad, el sexo, etc.).

Siendo numerosos los ámbitos en los que resultan susceptibles de aplicación los sistemas IA indicados, también son amplios los espectros de derechos e intereses de los ciudadanos que pueden resultan afectados de la aplicación de tales sistemas. El tratamiento de datos de carácter personal ya implica, de por sí, una incidencia en el derecho a la vida privada de los sujetos afectados en esta nueva dimensión de la privacidad que comienza a adquirir sustantividad propia como derecho fundamental autónomo en la década de los ochenta del siglo pasado y que tiene reflejo en esa precisa época en el art. 18.4 CE. Pero, además, los datos personales que sirven de fundamento a estas técnicas de identificación

3 Vid. "Documento de trabajo sobre biometría" del GT29; Dictamen 3/2012 GT29 sobre la evolución de las tecnologías biométricas (WP193).

4 La FRA (European Union Agency for Fundamental Rights) se refiere, por ejemplo, a la posibilidad de que las características biométricas se incorporen a un documento de identidad o a un pasaporte, de modo que en los controles fronterizos se escanee la imagen que aparece en el documento y se compare mediante tecnologías de reconocimiento facial con la imagen que se obtiene en momento real en el punto de control, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 2020, p. 7. Utilizado en los servicios móviles y en línea (reconocimiento facial, de voz, de huella dactilar) puede funcionar conforme a esta modalidad "en lugar de un nombre de usuario y contraseña" para acceder a un servicio o a un dispositivo en línea o móvil (Dictamen 2/2012, de 22 de marzo, sobre reconocimiento facial en los servicios en línea y móviles, p. 3).

poseen unas particularidades especiales que los hacen merecedores de una especial protección: se trata de los datos biométricos. Según el Reglamento (UE) 2016/679, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD en adelante) y la Directiva (UE) 2016/680, de 27 de abril de 2016, también sobre protección de las personas físicas en lo que respecta al tratamiento de datos personales pero para fines de prevención y represión penal, estos datos biométricos pertenecen a la "categoría especial de datos" (arts. 9 y 10 respectivamente) y por este motivo están sujetos a restricciones en su tratamiento y a garantías adicionales en los supuestos excepcionales en que sea posible[5].

Por otro lado, el empleo de esos datos biométricos con fines de identificación que es objeto de este estudio es el que se materializa en espacios públicos ("one-to-many comparison"). Ello implica la afectación a un número cuantioso de ciudadanos cuyos datos biométricos serán objeto de tratamiento. Esta implementación debe ajustarse, por consiguiente, de una manera rigurosa al principio de proporcionalidad de la medida, para evitar en lo posible situaciones abusivas. Pero la incidencia en los derechos de los ciudadanos va más allá de un tratamiento masivo de unos datos por muy especiales que sean. El empleo de esos sistemas implica sujetar a vigilancia y control determinados espacios públicos, en los que, siquiera de forma más atenuada, también se desarrollan aspectos de la vida privada de los ciudadanos. Y en los que también se desarrollan, por constituir el lugar idóneo para ello, otras expresiones de la libertad del individuo como el derecho de reunión o el de manifestación. La vigilancia de tales espacios utilizando sistemas que permiten identificar a quienes participan en esas demostraciones puede producir un efecto disuasorio innegable en la libertad de los ciudadanos.

No se agotan en los mencionados los riesgos que implica el uso de sistemas IA de reconocimiento biométrico. Estos sistemas se basan usualmente, pero no exclusivamente, en el tratamiento de imágenes faciales (reconocimiento facial) que ya han sido objeto de aplicación práctica en no pocos lugares. La experiencia ha demostrado que los índices de error, en forma de falso positivo o de falso negativo, no son desdeñables, ni mucho menos. El uso de algoritmos sesgados es la causa esencial de tales deficiencias. Lo preocupante son las graves consecuencias asociadas a tales errores y que se han traducido en ciertas ocasiones en privaciones de libertad de las personas erróneamente identificadas.

Todo lo anterior explica que, el que nos ocupa, sea un tema vinculado a la polémica, pero no artificiosa, sino fruto de una preocupación real por la incidencia que en los derechos de los ciudadanos tiene el uso de tales sistemas. Polémica

5 Cano Ruiz, I.: "Artículo 9. Categorías especiales de datos", en AA.VV.: *Protección de Datos: Comentarios a la Ley Orgánica de Protección de Datos y Garantías Digitales (en relación con el RGPD)* (dir. por M. Arenas Ramiro y A. Ortega Giménez), Sepín, Madrid, 2019, p. 82.

que se ha evidenciado, de otra parte, durante la tramitación de la trascendental Ley Europea de IA. La posición de las instituciones europeas implicadas en el procedimiento legislativo ha sido encontrada. Sobre este punto en especial. La Propuesta inicial de la Comisión (Propuesta de Reglamento IA) de 2021, de la que hace un seguimiento sin separarse en lo esencial el Consejo, ha sido enmendada de forma radical por el Parlamento Europeo, que ha llegado a proponer una prohibición casi absoluta de los sistemas IA que nos van a ocupar. Aunque no hayan sido atendidas en el texto definitivo consensuado, ha de reconocerse que venían precedidas de serias objeciones planteadas al respecto por las máximas autoridades institucionales sobre protección de datos de la propia UE[6].

Este trabajo se centrará en el análisis de este trascendental texto europeo, limitando el mismo desde una óptica procesal al empleo de los sistemas IA de identificación biométrica con fines de lo que, en el texto, se denomina aplicación de la ley ("law enforcement"), esto es, lo relacionado con la prevención y la represión penal.

II. PREVIA ACLARACIÓN CONCEPTUAL.

Según lo adelantado, el uso de los sistemas IA que nos ocupan ha generado un encendido debate con posiciones encontradas incluso en el seno de las propias instituciones europeas. Se trata, pues, de una cuestión compleja que afecta, como se ha dicho, a un amplio abanico de derechos y libertades, y de un numeroso grupo de personas. La primera cuestión a tratar ha de ser, por consiguiente, la de aclarar qué ha de entenderse por sistemas IA de identificación biométrica remota en tiempo real y en espacios públicos, con los fines de prevención y represión penal.

Esta necesidad de definir de la manera más precisa posible el significado de esta modalidad de sistema IA se hace más evidente, si cabe, en el caso de una disposición normativa llamada a ser aplicada y a ser vinculante en un espacio como el europeo en el que conviven ordenamientos jurídicos diversos y con particularidades propias significativas. Es el ámbito de la justicia penal el último reducto que los Estados miembros suelen querer preservar en el ejercicio de su soberanía y es el más refractario a las ideas de cooperación y armonización, de ahí las diferencias institucionales y normativas. Afortunadamente, este instrumento normativo que nos ocupa contiene, como nos tiene acostumbrados el legislador europeo en normas trascendentales, un capítulo relativo a las definiciones de los

6 Aunque no se ha publicado aún oficialmente el texto definitivo de la Ley de IA, se hizo público que el pasado 8 de diciembre de 2023 se alcanzó un acuerdo entre las tres instituciones implicadas (trílogos) que fue aprobado por el Parlamento Europeo el 13 marzo de 2024 en primera lectura [P9_TA(2024)0138] y al que nos referiremos, con las debidas precauciones, como "texto definitivo".

conceptos fundamentales objeto de regulación. Otra afortunada costumbre con la que nos regala con frecuencia el legislador europeo, sobre todo en casos como el presente, en el que se aborda una materia novedosa y con gran repercusión económica, comercial y jurídica, es la de acompañar el texto de la norma de una amplia exposición de considerandos explicativos, no sólo de las razones que la impulsan, sino también aclaratorios del significado de las disposiciones que se contienen. En ocasiones, como esta que nos ocupa, de una extensión considerablemente amplia, pero las más de las veces, también en ésta, justificada.

1. La identificación biométrica.

El texto inicial de Propuesta remitido por la Comisión (21.04.2021) comienza el abordaje de la materia con alusiones y definiciones de lo que ha de entenderse por "sistemas IA de identificación biométrica", pero prescinde del significado de identificación biométrica en sí mismo. Este silencio resulta llamativo en la medida en que ya resultaba usual y admitida la clasificación de las aplicaciones de la biometría con fines de: autenticación o verificación biométrica, por un lado; identificación biométrica, por otro lado; y categorización biométrica, por último. Esta omisión ha sido colmada en posteriores versiones del texto.

Tampoco contiene una referencia expresa a la "identificación biométrica" el texto del Consejo (Orientación general de 06.12.2022), pero sí aclara que quedan excluidos de la definición los "sistemas de verificación o autenticación cuyo único propósito es confirmar que una determinada persona física es la persona que afirma ser y los sistemas que se utilizan para confirmar la identidad de una persona física con el único fin de tener acceso a un servicio, un dispositivo o un local" [considerando (8)].

Sin embargo, el texto enmendado que presenta el Parlamento Europeo (de 14.06.2023 y que utiliza la denominación de Ley de IA) contiene muy relevantes aportaciones en el tema que nos ocupa y una de ellas es la expresa contraposición entre identificación, verificación y categorización biométricas. Además, el texto enmendado del Parlamento, no sólo define lo que ha de entenderse por identificación biométrica, sino que también amplía el elenco de rasgos humanos que constituyen los datos biométricos sobre los que se fundamenta la identificación. Esto es relevante, pues parece ser que tales aportaciones han sido atendidas en el texto definitivo de la Ley IA.

Conforme al texto del Parlamento, ha de entenderse por identificación biométrica "el reconocimiento automatizado de características humanas de tipo físico, fisiológico, conductual y psicológico para determinar la identidad de una persona comparando sus datos biométricos con los datos biométricos de personas almacenados en una base de datos (identificación `uno respecto a

varios´)" [nuevo art. 3.33 ter)]. Esta propuesta del Parlamento ha sido asumida en el texto definitivo. También la definición expresa de "verificación biométrica" en contraposición a la identificación, que con anterioridad a las enmiendas no se recogía en el texto. Ahora sí.

Resulta de esencial relevancia esta precisión conceptual. Los sistemas de identificación biométrica remota representan la especie de la categoría de identificación biométrica, pero esta última es una categoría más amplia, pues la identificación biométrica a distancia solo resulta posible en determinados supuestos o expresiones de la identificación biométrica, pero no en todo caso.

En la definición del Parlamento, incorporada al texto definitivo, sobresale no sólo el hecho mismo de definir el concepto, sino los términos en los que lo hace. De la anterior definición resulta que la identificación biométrica tiene lugar comparando los datos biométricos de la persona cuya identidad se quiere determinar, con los datos biométricos de personas que se encuentran almacenados en bases de datos. El concepto o definición de "dato biométrico" resulta esencial a tales efectos, pues constituye la esencia de esos sistemas. Y aquí la sorpresa.

Según la definición de identificación biométrica arriba recogida, los rasgos o características biométricas humanas que se utilizan con tal finalidad identificativa son las de "tipo físico, fisiológico, conductual y psicológico". La referencia a las características psicológicas de la persona con fines identificativos es nueva. No estaba recogida en el texto originario de la Comisión. Pero lo que resulta más relevante, no se corresponde exactamente con la definición de datos biométricos".

Sin perjuicio de que ahondemos más adelante en el concepto de dato biométrico sobre el que descansa la identificación biométrica, resulta oportuna una parada en los siempre ilustrativos considerandos que, también en este caso, muestran ejemplos o supuestos de lo que de forma más genérica se indica en la definición. El texto enmendado del Parlamento Europeo añadió un nuevo considerando (7 bis) -enmienda núm. 22- en el que tras la definición del concepto "identificación biométrica" en los términos indicados arriba, menciona ejemplos de los rasgos humanos susceptibles de tratamiento automatizado, así, la cara, el movimiento ocular, las expresiones faciales, la forma del cuerpo, la voz, el habla, el modo de andar, la postura, la frecuencia cardíaca, la presión arterial, el olor, las pulsaciones de tecla, las reacciones psicológicas (ira, angustia, dolor, etc.)".

Llama la atención, como se ha indicado, la referencia a las reacciones psicológicas (ira, angustia, dolor, etc.) en el listado de rasgos o características humanas susceptibles de tratamiento automatizado. No tanto por constituir algo novedoso, sino, más bien, por contraposición al texto inicial de Propuesta de la Comisión que no hacía referencia a ello. Novedoso no lo es tanto, pues ya el

Dictamen 3/2012, de 27 de abril de 2012, del Grupo de Trabajo del Artículo 29 hacía alusión a las mismas. Este último Dictamen mencionaba entre las técnicas biométricas las relativas al patrón de venas, a las impresiones dactilares o a la firma biométrica, además de las expresamente citadas en el considerando (7 bis) del texto del Parlamento. Pero también contenía menciones a los aspectos psicológicos. Así, distinguía entre las técnicas biométricas dos categorías principales, las basadas en aspectos físicos y fisiológicos, por un lado, y las basadas en aspectos comportamentales o conductuales, por otro lado. Pero, a su vez, no olvidaba hacer referencia al, en ese momento, "reciente ámbito de las técnicas basadas en elementos psicológicos, que incluyen la medición de la respuesta a situaciones concretas o pruebas específicas que se ajusten a un perfil psicológico"[7].

La mención de las reacciones psicológicas entre la relación de características humanas susceptibles de tratamiento con fines de identificación biométrica que incorporan las enmiendas del Parlamento Europeo han pasado al texto definitivo de la Ley IA. Al menos en la definición del concepto de identificación biométrica del art. 3.35. Sin embargo, existe una cierta disfunción con lo previsto en el nuevo considerando (15), pues en el mismo sí se hace mención a los rasgos físicos, fisiológicos y conductuales, con mención expresa de los mismos ejemplos que los citados en el texto del Parlamento Europeo, pero no así a las características psicológicas. Parece que se trata de un mero olvido, al hacer mención de las características psicológicas en el articulado del texto definitorio de la identificación biométrica, pero no en los considerandos.

No podemos dejar pasar la oportunidad al menos de aludir a dos cuestiones estrechamente vinculadas a la identificación biométrica. Por un lado, la formulación por parte del Parlamento Europeo en su texto enmendado de un nuevo concepto próximo pero diferenciado del de datos biométricos, se trata de los denominados "datos de base biométrica", esto es, "los datos obtenidos a partir de un tratamiento técnico específico relativos a las señales físicas, fisiológicas o conductuales de una persona física" [33 bis)]. Los elementos en común son incuestionables, sobre todo la base biométrica de ambos conceptos. Sin embargo, falta en estos últimos la referencia a la aptitud identificadora unívoca de las personas propia de los datos biométricos en sentido estricto. Nos referiremos más adelante al respecto, sólo dejar señalado que este nuevo concepto no ha sido asumido en el texto definitivo.

7 Dicho Dictamen 3/2012 contiene otras referencias al respecto, así, la posibilidad de que de las características de la cara (reconocimiento facial) se pueda determinar, no solo la identidad, sino también "las características fisiológicas y psicológicas" de la persona; o la incorporación de una nueva categoría de datos biométricos -de segunda generación- en los que lo determinante no es tanto la identidad, sino otras circunstancias igualmente útiles: "Los avances en tecnologías y redes informáticas están propiciando asimismo la subida de lo que se considera la segunda generación de datos biométricos basada en la utilización de los rasgos de comportamiento y psicológicos solos o combinados con otros sistemas clásicos que conforman sistemas multimodales". Dictamen 3/2012, pp. 4, 17 y 23.

La otra cuestión vinculada al tema que nos ocupa es la relativa a los sistemas de reconocimiento de emociones. La deducción de emociones tiene lugar, también en este caso, a partir de los datos biométricos. Además, de lo que se entienda por reconocimiento de emociones dependerá la existencia de más elementos en común con la identificación biométrica, y consiguientes dificultades de deslinde. Si nos ajustamos a la definición inicial contenida en el texto de la Comisión, y que coincide con la finalmente asumida en el texto definitivo, se entiende por sistema de reconocimiento de emociones "un sistema de IA destinado a detectar o deducir las emociones o las intenciones de personas físicas a partir de sus datos biométricos" [arts. 3.34) y 3.39) respectivamente].

Entre ambas versiones se han sucedido, no obstante, otros textos con definiciones que presentan ciertas diferencias. Así, la Orientación general del Consejo de la UE añadía a la finalidad de detección o deducción de emociones o de intenciones de personas físicas, la de los "estados mentales" de las mismas [también art. 3.34)]. Más amplia aún es la definición recogida en el texto del Parlamento Europeo, que a la inferencia de emociones e intenciones, añade la de los pensamientos y estados de ánimo. Estas incorporaciones aproximan más los sistemas de reconocimiento de emociones a los rasgos psicológicos dirigidos a la identificación biométrica.

Como se ha dicho, el texto definitivo de la Ley IA vuelve a la versión más restrictiva correspondiente al texto inicial de la Comisión, eliminando las referencias a los estados mentales o de ánimo y a los pensamientos. En todo caso, cuando se dispone a enumerar ejemplos, lo hace en un sentido amplio similar al del texto del Parlamento, y así podemos comprobarlo en su considerando (18) al afirmar que el reconocimiento de emociones "se refiere a emociones o intenciones como la felicidad, la tristeza, la indignación, la sorpresa, el disgusto, el entusiasmo, la vergüenza, la satisfacción y la diversión. No incluye estados físicos, como el dolor o el cansancio".

2. El concepto de dato biométrico.

El concepto de dato biométrico resulta esencial y fundamento de la identificación biométrica. Como recoge el texto definitivo de la Ley IA en su considerando (14) los datos biométricos permiten una pluralidad de aplicaciones al hacer posible la autenticación, la identificación y la categorización de las personas físicas y, a su vez, el reconocimiento de sus emociones. Creemos nosotros que también los polígrafos o instrumentos similares a los que igualmente se refiere la Ley de IA, podrían incluirse en esa categoría, pues tienen un indudable fundamento biométrico.

Conviene aclarar su significado, pues, al menos aparentemente, existen disfuncionalidades en los textos analizados en torno al concepto señalado. El texto originario de la Comisión definía los datos biométricos como "los datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos" [art. 3.33)]. Esto es, de manera absolutamente idéntica a la definición contenida en el RGPD y en la Directiva (UE) 2016/680. Esta coincidencia nada tiene de extraño, más bien lo contrario, como además lo recuerda el considerando (7) del texto original con una llamada a la definición contenida en ambos textos normativos sobre protección de datos personales y a la necesidad de que se "interprete en consonancia con ella".

De la definición destacamos, por un lado, que los datos obtenidos mediante el tratamiento técnico correspondiente tienen una nítida aptitud para la identificación unívoca de las personas, y pone como ejemplos de ello la imagen facial y los datos dactiloscópicos; por otro lado, que el tratamiento recae sobre rasgos o características físicas, fisiológicas o conductuales. Curiosamente, la referencia a la capacidad identificadora única característica de los datos biométricos desaparece en la definición que de este concepto se recoge en el art. 3.33) del texto del Consejo de la UE (Orientación general de 06.12.2022). El resto de la definición no varía. Esta falta de sintonía podría salvarse con lo contenido en el considerando (7) antes mencionado, que es muy similar al del texto original de la Comisión, pero tampoco absolutamente idéntico. Ya no dice, evidentemente, que la noción de dato biométrico "coincide" con el concepto del RGPD y la Directiva (UE) 2016/680, pero sí que la misma "debe interpretarse" en consonancia con el recogido en estos textos. Algo similar ocurre con el texto definitivo de la Ley IA, pues al definir el dato biométrico alude al tratamiento automatizado de características físicas, fisiológicas y conductuales de una persona física, pero sin mencionar tampoco aquí la eficacia identificadora única del dato personal resultante. En cualquier caso, la definición de dato biométrico en el texto definitivo de la Ley de IA sí se refiere a los ejemplos paradigmáticos de datos de tal naturaleza presentes en todas las definiciones normativas de los mismos, a saber, a las imágenes faciales y a los datos dactiloscópicos. La ausencia de referencia al potencial identificativo de los datos biométricos también puede salvarse con lo dispuesto en el considerando (14). En el mismo, se afirma que la noción de dato biométrico de la Ley de IA se ha de "interpretar" en consonancia con lo dispuesto al respecto en los textos esenciales sobre protección de datos [RGPD, Directiva (UE) 2016/680 y Reglamento (UE) 2018/1725]. Pero no se llega a sostener, a diferencia por ejemplo de la inicial Propuesta de la Comisión, que la noción de dato biométrico "coincida" con la recogida en las normas de referencia sobre protección de datos.

Creemos que la posición del Parlamento Europeo cuando aborda la cuestión de la identificación biométrica es la más coherente desde un plano sistemático con el contexto conceptual de lo que ha de entenderse por datos biométricos en el espacio de la UE. Por comenzar, en el texto de enmiendas del Parlamento se opta por no definir el concepto de dato biométrico y por hacer una remisión al concepto de los datos biométricos "tal como se definen en el artículo 4, punto 14, del Reglamento (UE) 2016/679". Resulta llamativo que solamente se haga alusión al concepto de dato biométrico contenido en el RGPD y no en otros textos de la UE igualmente relevantes en materia de protección de datos. Por ejemplo, en la Directiva (UE) 2016/680 o el Reglamento (UE) 2018/1725. Llama igualmente la atención que el considerando (7) no corrija la omisión de esos textos normativos, máxime cuando eran ya mencionados en la Propuesta inicial de la Comisión y lo son en el texto definitivo de la Ley de IA. En todo caso, ignorando esas circunstancias, la definición de dato biométrico recogido en el RGPD coincide plenamente con la contenida en los instrumentos normativos omitidos.

Ahora bien, en nuestra opinión, la principal aportación del texto del Parlamento es la incorporación de un concepto nuevo, próximo al de dato biométrico, pero no coincidente totalmente con él. Además, este nuevo concepto adquiere pleno sentido en un contexto en el que datos relativos a la biometría pueden ser valiosos para múltiples finalidades, sin necesidad de reunir las condiciones de los datos biométricos en sentido estricto, y que pueden implicar igualmente serias amenazas para los derechos y libertades de las personas. Sobre todo, cuando esos datos "relativos" a la biometría pueden ser objeto de tratamiento mediante sistemas de IA.

Cabía solucionar este entuerto mediante dos alternativas posibles, factibles al menos: modificar el concepto de dato biométrico, dotándolo de un contenido más extenso, por un lado, o introducir un nuevo concepto diferente al de dato biométrico en sentido estricto, pero con fundamento igualmente en rasgos biométricos y con múltiples virtualidades cuando son objeto de tratamiento automatizado. El Parlamento Europeo se decantó por esta segunda opción con un nuevo concepto que denomina "datos de base biométrica".

3. Los datos de base biométrica.

El nuevo concepto de "datos de base biométrica" se define en el texto enmendado del Parlamento Europeo como "los datos obtenidos a partir de un tratamiento técnico específico relativos a señales físicas, fisiológicas o conductuales de una persona física" [art. 3.33 bis)]. Conforme a esta definición, los datos de base biométrica presentan un incuestionable sustrato común compartido con los datos biométricos en sentido estricto, pues en ambos casos son datos resultantes de un tratamiento técnico de señales físicas, fisiológicas o conductuales de una persona

física. El principal elemento diferenciador es que desaparece de la definición la idoneidad para identificar de forma única a las personas físicas, característica de los datos biométricos en sentido estricto. Sin perjuicio de otras diferencias menos relevantes[8]. Aunque, como se ha comprobado, también desaparece esta particularidad identificativa unívoca de la definición de dato biométrico en el texto definitivo de la Ley IA[9].

Parece evidente que el legislador europeo (en este caso el Parlamento con sus enmiendas) ha pretendido con este novedoso concepto que no quedaran fuera del ámbito regulatorio posibles aplicaciones de sistemas de IA que tuvieran por objeto datos que, sin pertenecer a la categoría de biométricos en sentido estricto, poseen un innegable fundamento biométrico. No es de extrañar si reparamos un poco en los supuestos en los que en la Ley de IA los sistemas de IA se utilizan para el tratamiento de los mencionados "datos de base biométrica".

En efecto, según el texto propuesto por el Parlamento Europeo, los datos basados en la biometría pueden conducir a la identificación de una persona física, pero no necesariamente. De este modo, añade en el considerando (7) -enmienda núm. 21- tras la referencia a lo que ha de entenderse por datos biométricos en sentido estricto, que "los datos basados en técnicas biométricas son nuevos datos resultantes de un procesamiento técnico específico relativo a señales físicas, fisiológicas o conductuales de una persona física, como las expresiones faciales, los movimientos, la frecuencia cardíaca, la voz, las pulsaciones de tecla o el modo de andar, que pueden, en algunos casos, permitir identificar o confirmar la identificación unívoca de una persona física". La alusión a que sólo en "algunos casos" este tipo de datos puede conducir a la identificación unívoca de una persona adquiere pleno sentido si nos atenemos a algunos de los ejemplos citados -expresiones faciales, movimientos, frecuencia cardíaca- que difícilmente pueden considerarse dotados de tal aptitud.

8 El texto del Parlamento Europeo, por ejemplo, ha optado por referirse a las "señales" ("signals") físicas, fisiológicas y conductuales de las personas, en lugar de a las "características" ("features") de idéntica clase que sigue utilizando con motivo de la identificación biométrica o, por remisión, de los datos biométricos. Seguramente tiene que ver con la capacidad individualizadora o identificativa de las "características", mayor que la de las "señales". Otro elemento diferenciador lo hallamos en que omite al referirse a estos datos de base biométrica hacerlo como "datos personales", pero no nos cabe duda de que sí nos hallamos ante datos de esa naturaleza considerando la amplitud con la que se definen los datos personales en los textos normativos al respecto, pues se refieren no sólo a la información relativa a una persona física identificada, sino también "identificable", entendiendo por esto último "toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona [art. 4.1) RGPD y art. 3.1) Directiva (UE) 2016/680]. Vid. sobre la definición de persona identificable los comentarios de Romeo Casabona, C.M.: "Datos personales (comentario al artículo 4.1 RGPD)", en AA.VV.: *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales* (dir. por A. Troncoso Reigada), Tomo I, Thomson-Aranzadi, Cizur Menor, 2021, pp. 585-589.

9 Aunque con remisión en su considerando (14) al RGPD, al Reglamento (UE) 2018/1725 y a la Directiva (UE) 2016/680 en cuanto a la necesidad de interpretar dicho concepto conforme a estos textos normativos.

Dos son los ámbitos en los que el texto del Parlamento Europeo emplea este nuevo concepto de "datos de base biométrica". Por un lado, en relación con la denominada "categorización biométrica" y, por otro, en relación con los "sistemas de reconocimiento de emociones". En el primer caso, la "asignación de personas físicas a categorías concretas, o inferencia de sus características y atributos" puede realizarse "en función de sus datos biométricos y sus datos de base biométrica, o que puedan inferirse a partir de dichos datos" [art. 3.35)]. En el segundo caso, se define al sistema de reconocimiento de emociones como aquél destinado a detectar o deducir las emociones, los pensamientos, los estados de ánimo o las intenciones de individuos o grupos a partir de sus datos biométricos y sus "datos de base biométrica" [art. 3.34)].

Estos datos de base biométrica, aparentemente inocuos por carecer por sí mismos de esa capacidad de individualizar de forma unívoca a las personas, pueden adquirir, en cambio, una nueva y más amplia dimensión cuando son tratados mediante IA, pues a partir de ellos pueden inferirse rasgos o características afectantes a la vida privada o tener contenido sensible. Particularmente llamativa es la circunstancia de que el texto del Parlamento Europeo es partidario de una amplia prohibición de los sistemas de reconocimiento de emociones -con fines de persecución penal o gestión de fronteras, en lugares de trabajo y centros educativos- [art. 5.1.d quinquies)][10] y de una prohibición casi absoluta de los sistemas de categorización biométrica -salvo cuando se destinen a fines terapéuticos basados en el consentimiento informado de la persona expuesta- [art. 5.1.b bis)][11]. Y al margen de estos supuestos prohibidos, los sistemas de IA que utilicen datos biométricos "o basados en la biometría" para extraer conclusiones sobre las características personales de las personas físicas "deben clasificarse de alto riesgo" [considerando (33 bis) y Anexo III.1.a bis)].

Con todo, pese a la relevancia que implica en nuestra opinión este nuevo concepto de datos de base biométrica, lo cierto es que el texto del Parlamento Europeo no es siempre claro al referirse a los rasgos o características que pueden servir de fundamento a tales datos frente a los datos biométricos en sentido

10 Los argumentos empleados por el Parlamento Europeo para fundamentar la amplia prohibición de los sistemas de IA de reconocimiento de emociones descansan en la escasa fiabilidad científica de los mismos y el consiguiente riesgo de abusos que puede derivarse. Así, afirma en sus considerandos que "las emociones o sus formas de expresión y su percepción varían de forma considerable entre culturas y situaciones, e incluso en una misma persona. Algunas de las deficiencias principales de estas tecnologías son la fiabilidad limitada (las categorías de emociones no se expresan de forma coherente a través de un conjunto común de movimientos físicos o psicológicos ni se asocian de forma inequívoca a estos), la falta de especificidad (las expresiones físicas o psicológicas no se corresponden totalmente con las categorías de emociones) y la limitada posibilidad de generalizar (los efectos del contexto y la cultura no se tienen debidamente en cuenta)" [considerando (26 quater)].

11 Las razones por las que conforme al texto del Parlamento habían de prohibirse los sistemas de IA que clasifican a las personas físicas asignándolas a categorías específicas, en función de ciertas características sensibles o protegidas, ya sean conocidas o inferidas, radica en su carácter "especialmente intrusivos" y en que "vulneran la dignidad humana y presentan un gran riesgo de discriminación" contraria al art. 21 de la Carta de Derechos Fundamentales de la UE (CDFUE), y al art. 9 del RGPD [considerando (16 bis)].

estricto. En este sentido, el considerando (7) del texto enmendado menciona refiriéndose a los datos de base biométrica a "señales" físicas, fisiológicas y conductuales tales como las expresiones faciales, los movimientos, la frecuencia cardíaca, la voz, las pulsaciones de tecla o el modo de andar. Pero, a su vez, el considerando (7 bis) relativo a la "identificación biométrica" basada en la comparación de datos biométricos en sentido estricto, vuelve a repetir algunos de los "rasgos" humanos citados en el considerando precedente como susceptibles de tratamiento automatizado -en concreto el movimiento ocular, las expresiones faciales, la voz, el modo de andar, la frecuencia cardíaca-.

Resulta evidente que muchos de estos rasgos o características no son por sí solos suficientes para determinar la identificación indubitada de una persona física. Este argumento resulta válido para las características humanas de tipo psicológico -auténtica novedad incorporada en el concepto de identificación biométrica, basada, insistimos, en la comparación de datos biométricos en sentido estricto- pues escasa o nula virtualidad han de tener por sí solas a efectos de establecer la identidad de una persona las reacciones psicológicas (ira, angustia, dolor, etc.) que se mencionan como ejemplo en el considerando (7 bis).

Se ha de concluir, pues, que junto a los rasgos de la persona que permiten identificarla de forma indubitada -patrón de venas, iris, retina, huella dactiloscópica, imagen facial, ADN, etc.- existen otras características, como las mencionadas más arriba y que incluirían los relativos a los datos de base biométrica, que carecen por sí mismas de tal eficacia, pero que pueden contribuir a ello. Ya se anticipó en tal sentido el Grupo del Art. 29 en su Dictamen 3/2012, sobre evolución de las tecnologías biométricas, con referencia a las nuevas tendencias sobre biometría mencionando la utilización de las denominadas "tecnologías biométricas ligeras" ("soft biometrics") que se caracterizan, precisamente, por "el uso de rasgos muy comunes no aptos para distinguir claramente o identificar a un individuo, pero que permiten mejorar los resultados de otros sistemas de identificación".

No puede negarse que los rasgos más comunes mencionados, si bien pueden resultar útiles, no son por lo general atribuibles a una sola persona. Esta deficiencia es la que puede resultar de la opción por una concepción excesivamente amplia de dato biométrico. En tal sentido, el Dictamen 4/2007 del Grupo de Trabajo del Art. 29 (WP 136), sobre el concepto de datos personales, de 20 de junio de 2007, definía los datos biométricos como propiedades biológicas, características fisiológicas, pero también "rasgos de la personalidad o tics", exigiendo a todos ellos que fueran al mismo tiempo "atribuibles a una sola persona y mensurables"[12].

12 Esta definición se reproduce en el apartado de las definiciones del Dictamen 3/2012 (WP193) en el que se añade que "los datos biométricos cambian irrevocablemente la relación entre el cuerpo y la identidad, ya que hacen que las características del cuerpo humano sean legibles mediante máquinas y estén sujetas a un uso posterior".

Como puede fácilmente entenderse, las dificultades de atribución a una sola persona de los rasgos indicados no siempre son idénticas, siendo mayores en el caso de los de personalidad o tics.

Esto último ha de vincularse con la posibilidad de combinar diversas tecnologías biométricas que hagan más eficaz el objetivo de identificación unívoca, en su caso. Esto es, se trataría de los denominados sistemas multimodales o biometría muldimodal que es definida por el Dictamen 3/2012 reiterado como la "combinación de diversas tecnologías biométricas con el fin de aumentar la exactitud o rendimiento del sistema (también se denomina biometría a varios niveles)". Este Dictamen añade que estos sistemas pueden funcionar de distintas maneras, bien recogiendo datos biométricos diferentes con distintos sensores, bien realizando múltiples lecturas del mismo elemento biométrico o bien utilizando algoritmos múltiples para la extracción de características de la misma muestra biométrica.

4. Sistema de identificación biométrica "remota".

Como se ha dicho anteriormente, la identificación biométrica consiste en comparar los datos biométricos obtenidos de una persona física con los conservados previamente en bases de datos o ficheros con la finalidad de identificar a aquélla (a diferencia de la verificación). La obtención de los rasgos o características de la persona física tiene lugar, en el caso que nos ocupa, de forma "remota". ¿Qué significa esto último? La definición que al respecto recoge el texto definitivo de la Ley IA nos procura no pocas pistas. Así, se define el sistema de identificación biométrica remota como "un sistema de IA destinado a identificar a personas físicas generalmente a distancia, sin su participación activa, comparando sus datos biométricos con los que figuran en un repositorio de datos de referencia" [art. 3.41)]. Dos elementos de esa definición pueden servir para entender el calificativo: por un lado, que la identificación se produce "generalmente a distancia"; y, por otro lado, que la misma tiene lugar "sin su participación activa". Esta definición coincide plenamente con la recogida en la Orientación general del Consejo de la UE. No así con las definiciones que contienen el texto original de la Comisión y el del Parlamento Europeo. En estos últimos, no se hace expresamente referencia a que no sea precisa la participación activa de la persona afectada y se da por hecho que la identificación será siempre a distancia. En ambos, a diferencia del texto definitivo que guarda silencio al respecto, se añade que el usuario o implementador del sistema desconoce de antemano si la persona en cuestión se encontrará en las bases de datos de referencia y podrá, por lo tanto, ser identificada.

El carácter remoto del uso de estos sistemas de identificación biométrica limita en extremo los datos biométricos susceptibles de ser capturados para su comparación con los existentes en las bases de datos de referencia. Queremos

decir que la captura de datos biométricos para su posterior comparación con otros almacenados requiere, en la mayoría de los supuestos, el conocimiento y la colaboración de la persona afectada. Por ejemplo, las huellas dactilares, muestras de ADN, el iris o la retina. Resulta complicado imaginar de qué modo se pueden obtener a distancia los datos biométricos procedentes de esas "fuentes de datos biométricos". Esto nos induce a pensar que la identificación biométrica "remota" se reducirá en la mayoría de los casos al tratamiento de la imagen facial mediante las tecnologías de reconocimiento facial, considerando la facilidad en la captura de dichas imágenes[13], dejando ahora al margen los sistemas de categorización biométrica que constituyen, igualmente, un ámbito propicio para el tratamiento de datos biométricos a distancia o remotamente.

Esta misma idea puede inferirse de la referencia al posible uso simultáneo de los sistemas de identificación biométrica que hace el texto definitivo de la Ley IA en su considerando (17). En este último se afirma que los sistemas de identificación biométrica remota se usan para detectar "simultáneamente" varias personas con fines de identificación sin necesidad de la colaboración activa de las mismas. Por ahora se nos ocurre, casi exclusivamente, la tecnología de reconocimiento facial remota o a distancia.

5. Sistema de identificación biométrica remota "en tiempo real".

El sistema de identificación biométrica ante el que se plantean serias prevenciones es, no sólo el que tiene lugar a distancia, sino también de manera inmediata. Tiene que ver con el hecho de que, siendo el resultado de la comparación positivo, se adoptarán decisiones con seria repercusión en la esfera del individuo y de sus derechos (proceder, por ejemplo, a la inmediata detención del identificado sin opción de una supervisión humana con el intervalo de tiempo suficiente). Con esta finalidad de una mejor protección del individuo se ha pretendido incluir una definición del término "en tiempo real" que no se limite exclusivamente al instantáneo momento. En tal sentido, se define la expresión que encabeza este apartado como "un sistema de identificación biométrica remota en el que la recogida de los datos biométricos, la comparación y la identificación se producen sin una demora significativa. Este término engloba no solo la identificación instantánea, sino también demoras mínimas limitadas, a fin de evitar su elusión"

13 En efecto, al tratar la Agencia de los Derechos Fundamentales de la Unión Europea (FRA) de las ventajas atribuibles al reconocimiento facial como sistema de identificación, afirma que la imagen facial es más o menos única, no puede ser alterada, no puede ser ocultada con facilidad y, a diferencia de otros datos biométricos como la huella dactilar o el ADN, es fácil de obtener, de manera que resulta de ordinario imposible que una persona pueda evitar que su imagen facial sea obtenida y monitorizada en un espacio público, FRA, *Facial recognition,* cit., p. 5.

[art. 3.42)]. Dicho en otras palabras, los sistemas en tiempo real implican el uso de material "en directo" o "casi en directo" [considerando (17)][14].

Siendo clara la intencionalidad del legislador europeo, la manera en la que se ha expresado su idea en el texto ha variado en las diferentes versiones del mismo. Curiosamente, la versión definitiva es calcada a la del texto originario de la Comisión. La Orientación general del Consejo (06.12.2022) optó, sin embargo, por referirse a la recogida de los datos biométricos, la comparación y la identificación que tiene lugar "instantáneamente o casi instantáneamente". El texto del Parlamento Europeo prefirió, sin embargo, referirse a la ausencia de demora significativa en términos de instantaneidad o de demora limitada, suprimiendo la alusión al carácter mínimo de la demora cuando no sea instantánea. En conclusión, lo relevante es evitar toda posibilidad de eludir la aplicación de las normas contempladas en la Ley de IA en relación con el uso "en tiempo real" de los sistemas de identificación biométrica remota –prohibiéndolo o condicionando dicho uso a una serie de restricciones- generando fraudulentamente demoras mínimas.

Las prevenciones vinculadas al uso de sistemas de IA de identificación biométrica remota no serían aplicables, por consiguiente, cuando las actuaciones de obtención, comparación e identificación no tienen lugar "en tiempo real". Esto es, el uso de tales sistemas sería considerado como de alto riesgo, como muchos otros, y sujeto a una serie de condiciones, pero no recaería sobre ellos la prohibición de partida y la admisibilidad excepcional, en su caso, aplicables a los sistemas de identificación en tiempo real. A esta modalidad de sistema de identificación biométrica que no tiene lugar en tiempo real la Ley de IA las denomina "en diferido", aunque la definición de la misma se formula por simple exclusión, esto es, todo sistema de identificación biométrica remota "que no sea un sistema de identificación biométrica remota `en tiempo real´" [art. 3.43)]. En los sistemas de identificación biométrica "en diferido" los datos biométricos se han recabado previamente, a partir de imágenes o grabaciones que pueden proceder de diversas fuentes, y que han sido generadas con anterioridad a la aplicación del sistema. Es la comparación de esos datos biométricos con los que se disponen en

14 De hecho, una de las objeciones que al uso de los sistemas de IA de identificación biométrica que nos ocupan plantea el importante Dictamen 5/2021, de 18 de junio de 2021, sobre la inicial Propuesta de Reglamento de IA, aprobado conjuntamente por el Comité Europeo de Protección de Datos (CEPD) y el Supervisor Europeo de Protección (SEPD), máximas autoridades en protección de datos en la UE, consiste precisamente en que no está claro qué deberá entenderse por "demora significativa". Pero no sólo eso, sino que, además, resta importancia a la dicotomía entre tiempo real o no, pues la intrusión del tratamiento no depende de que la identificación se produzca de un modo u otro; y por ello mismo se critica que se considere como un factor atenuante el hecho de que la identificación biométrica pueda tener lugar con "demora significativa". Se objeta al respecto en dicho Dictamen, que un sistema de identificación masiva es capaz de identificar a miles de personas en solo unas horas o la probabilidad de que la identificación biométrica a distancia en el contexto de una protesta política tenga un efecto disuasorio significativo en el ejercicio de los derechos y libertades fundamentales, como la libertad de reunión y asociación y, más en general, en los principios fundacionales de la democracia [apartado (31)].

bases de datos de referencia y, en su caso, la identificación la que tiene lugar con una demora significativa.

En estos supuestos, los riesgos antes mencionados –inmediatez en las consecuencias, escasas oportunidades para realizar comprobaciones o correcciones adicionales- no tendrían idéntica envergadura. En todo caso, tampoco pueden ignorarse los riesgos inherentes a los sistemas de IA destinados a la identificación a la identificación biométrica remota de las personas físicas, con independencia de si su uso es en tiempo real o en diferido. Ambas modalidades adolecen de imprecisiones técnicas que pueden dar lugar a resultados sesgados y tener consecuencias discriminatorias. Siendo esto especialmente importante en lo que respecta a la edad, la etnia, la raza, el sexo o la discapacidad. No es baladí, como tendremos ocasión analizar, que el texto del Parlamento Europeo propusiera extender la prohibición del uso de los sistemas de IA de identificación biométrica remota "en tiempo real" también al empleo "diferido" de los mismos. Aunque en este segundo supuesto la prohibición podría exceptuarse mediante la concurrencia de rigurosos presupuestos.

6. Sistema de identificación biométrica remota en tiempo real en "espacio de acceso público".

Las cautelas que contempla la Ley de IA sobre el uso de los sistemas de IA de identificación biométrica remota y en tiempo real se justifican igualmente por el lugar físico o espacio en el que tiene lugar aquella identificación biométrica. El texto se refiere a la identificación biométrica de personas físicas en espacios de acceso público. Dos cuestiones han de ser destacadas al respecto. Por un lado, que el uso de dispositivos tecnológicos que posibilitan la identificación biométrica de personas físicas en los indicados espacios incrementa exponencialmente la posibilidad de afección de una infinidad de sujetos. Es decir, de una manera indiscriminada en el sentido literal del término. Esto es, sin discernir ni diferenciar a las personas físicas concretas susceptibles de identificación biométrica en función de su condición de sospechosas de infracciones ya cometidas, de peligrosas en relación a futuras infracciones, de víctimas desaparecidas, etc. Cualquier persona física que transite por el espacio sometido a observación puede ser objeto de los sistemas de IA de identificación biométrica. Por otro lado, así como los espacios más vinculados a la privacidad –vivienda o espacios cerrados- han merecido la protección incuestionable por parte del Derecho, no ha ocurrido lo mismo en relación a la posible afectación de los derechos de los ciudadanos cuando la "vida privada" se desarrolla en espacios públicos. Al menos ha acontecido así hasta fechas recientes.

Sobre este punto, la intencionalidad de la Ley de IA en la protección de los derechos de los sujetos afectados es evidente. Para ello utiliza una concepción

amplia del significado de espacio de acceso público. Préstese atención a que dicha amplitud definitoria no debe ser interpretada como una posibilidad igualmente extensa de injerencia en los derechos de los ciudadanos. Al contrario, siendo el punto de partida, como veremos, el de la prohibición de los sistemas de IA de identificación biométrica remota cuanto más amplio sea el espacio objeto de prohibición mejor tutelados resultarán los derechos de las personas afectadas por tales sistemas.

Como decíamos, el texto de la Ley de IA opta por un concepto amplio de espacio de acceso público, priorizando la condición pública del acceso sobre la condición pública de la titularidad de dicho espacio. Así, define la noción de "espacio de acceso público" como "cualquier lugar físico, de propiedad privada o pública, al que pueda acceder un número indeterminado de personas físicas, con independencia de que deban cumplirse determinadas condiciones de acceso y con independencia de las posibles restricciones de capacidad" [art. 3.44)].

Esto ya supone una diferencia notable con lo establecido en otras disposiciones normativas cuya aplicación pueda solaparse por coincidir en mayor o menor grado en el ámbito de aplicación. Así, la LO 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos, se refiere en cuanto a su objeto a la grabación de imágenes y sonidos "en lugares públicos, abiertos o cerrados" (art. 1.1). De igual modo, la LO 7/2021, de 26 de mayo, por la que se transpone la Directiva (UE) 2016/680, regula la instalación de sistemas de videocámaras fijas en "las vías o lugares públicos" (art. 16.1). Conforme a la primera norma citada la cuestión no podría ser resuelta de forma distinta, considerando la finalidad preventiva de la misma y que las Fuerzas Policiales sólo pueden actuar en espacios públicos. La LO 7/2021, por su parte, tiene un ámbito de aplicación mucho más amplio, pues comprende la protección de datos personales obtenidos, no sólo para la prevención, sino también para la persecución y enjuiciamiento de infracciones penales. Aunque el precepto concreto referido sí tenga connotaciones de claro contenido preventivo.

Como se ha dicho, la Ley de IA utiliza un concepto amplio de lugar de acceso público. Dicha definición nos da ya unas claves concretas para su delimitación. Al tratarse de un lugar "físico" quedan excluidos los espacios en línea[15]. Por otro lado, resulta indiferente, por ejemplo, que se trate de propiedad privada o pública. Otro elemento delimitador importante es el del carácter indeterminado del número de personas físicas con acceso. De modo que no puede considerarse de acceso

15 Considerando (19). Sobre esta segunda dimensión pueden consultarse, entre otros, el Dictamen 02/2012, de 22 de marzo de 2012, sobre reconocimiento facial en los servicios en línea y móviles del GT29 (WP 192). No es del mismo parecer el recogido en el Dictamen conjunto 5/2021 del CEPD y del SEPD, al afirmar que, por razones de coherencia, los sistemas de IA para la identificación remota a gran escala en espacios en línea deberán prohibirse en virtud del art. 5 de la Propuesta [apartado (32)].

público el espacio al que únicamente pueden acceder determinadas personas físicas definidas. Los siempre ilustrativos considerandos ponen como ejemplos de lugar excluido del acceso público los locales de empresas y fábricas, así como las oficinas y lugares de trabajo a los que solo se pretende que accedan los empleados y proveedores de servicios pertinentes [considerando (19)].

El lugar físico no pierde su condición de espacio de acceso público por la circunstancia de que tenga una capacidad limitada o restringida. Tampoco, y esto es más relevante a los efectos de su delimitación, si dicho acceso está sujeto al cumplimiento de determinadas condiciones que pueden satisfacer un número indeterminado de personas, por ejemplo, según el considerando (19), adquiriendo una entrada o título de transporte, registrándose previamente o teniendo una determinada edad. También es importante destacar que resulta indiferente a los efectos de atribuir el carácter de accesibilidad pública al lugar, la naturaleza de la actividad que se desarrolle en el mismo, siempre que se cumplan los anteriores requisitos. En todo caso, la suma de los anteriores condicionantes en la delimitación del espacio de acceso público no termina de despejar todas las interrogantes concebibles, de ahí que el considerando correspondiente, el (19), concluya afirmando que "no obstante, se debe determinar caso por caso si un espacio es de acceso público o no teniendo en cuenta las particularidades de la situación concreta".

7. Sistema de identificación biométrica remota en tiempo real en espacio de acceso público "con fines de aplicación de la ley".

Las prevenciones a que venimos refiriéndonos en relación al uso de sistemas de IA de identificación biométrica se centran en dicho uso con fines de aplicación de la ley. Dicho ámbito es de por sí apto para generar situaciones de riesgo que pueden pugnar con los derechos fundamentales de los ciudadanos. Muy explícitamente, podemos encontrar en el texto de la Ley de IA aserciones en las que se constata que, atendiendo a su función y responsabilidad, las actuaciones de las autoridades encargadas de la aplicación de la ley que implican determinados usos de sistemas de IA "se caracterizan por un importante desequilibrio de poder y pueden dar lugar a la vigilancia, la detención o la privación de libertad de una persona física, así como a otros efectos negativos sobre los derechos fundamentales que garantiza la Carta" [considerando (59)]. Por consiguiente, se trata de un ámbito en el que serán considerados como de alto riesgo múltiples sistemas de IA diseñados para usarse con los mencionados fines.

Ahora bien, esto nos conduce a tener que precisar qué ha de entenderse por fines de aplicación de la ley. Aquí claramente se ha optado en la versión española de la expresión por una traducción literal de la expresión inglesa "law enforcement" que por sí misma, esta última, tiene una incuestionable connotación

de que la ley que se aplica es la penal. No así en la traducción literal española. Hubiera sido preferible una expresión análoga en la traducción a las de otras versiones en las que se enfatiza el elemento de la "criminalidad" (así, "à des fines répressives" francesa o "zu Strafverfolgungszwecken" alemana). Para entender, pues, el verdadero significado de la expresión que nos ocupa hemos de acudir nuevamente al apartado de las definiciones conforme a las cuales, se entiende por tales "las actividades realizadas por las autoridades encargadas de la aplicación de la ley, o en su nombre, para la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluidas la protección y prevención frente a amenazas para la seguridad pública" [art. 3.46)].

Nos hallamos nuevamente ante una definición muy amplia de la expresión "fines de aplicación de la ley". La misma contempla actuaciones de prevención de infracciones penales, así como de represión de las ya cometidas. Amplitud que se acrecienta con la referencia a las amenazas para la seguridad pública. En todo caso, esta extensión del término es coincidente con el objeto a que se refieren, tanto la Directiva (UE) 2016/680, como la LO 7/2021 por la que se transpone.

III. PUNTO DE PARTIDA: PROHIBICIÓN DE LOS SISTEMAS DE IDENTIFICACIÓN BIOMÉTRICA REMOTA EN ESPACIOS DE ACCESO PÚBLICO CON FINES DE APLICACIÓN DE LA LEY.

La Ley de IA opta por un enfoque normativo basado en los riesgos. Conforme al mismo, se diferencian, por un lado, prácticas prohibidas de IA, por otro lado, sistemas de IA de alto riesgo, sujetos a obligaciones y requisitos específicos, y, por último, sistemas de IA sujetos a normas armonizadas de transparencia (art. 1). Pues bien, el régimen jurídico de los sistemas de identificación biométrica que nos ocupan es bastante particular. En principio se integran en el Título II correspondiente a las prácticas de IA prohibidas [art. 5.1.h)]. Pero no se trata de una prohibición absoluta, pues acto seguido, el mismo precepto admite su uso condicionado a la observación de unos estrictos requisitos orientados a que el mismo resulte excepcional y proporcionado y rodeado de ciertas garantías. En estos casos excepcionales los sistemas de IA de identificación biométrica remota pasarían a formar parte de los sistemas IA de alto riesgo contemplados en el Anexo III por remisión del art. 6. 2).

Las razones por las que el texto de la Ley de IA adopta como punto de partida la prohibición de los sistemas de IA de identificación biométrica remota que nos ocupan –prohibición no absoluta, como veremos- están recogidas en el propio texto. Ya se ha indicado que, sin necesidad de descender todavía al concreto caso que nos ocupa, con carácter general las actuaciones de las autoridades encargadas

de la aplicación de la ley que implican determinados usos de sistemas de IA "se caracterizan por un importante desequilibrio de poder y pueden dar lugar a la vigilancia, la detención o la privación de libertad de una persona física, así como a otros efectos negativos sobre los derechos fundamentales que garantiza la Carta" [considerando (59)]. Conforme a dicho considerando, estos riesgos pueden derivarse de diversos factores vinculados a la precisión, fiabilidad y transparencia del sistema de IA. Así, pueden ser consecuencia de la cuestionable calidad de los datos utilizados en el entrenamiento, del no cumplimiento de los requisitos oportunos en términos de precisión o solidez, o del indebido diseño y prueba previos a su introducción en el mercado o puesta en servicio. Además, añade este mismo considerando, "podría impedir el ejercicio de importantes derechos procesales fundamentales, como el derecho a la tutela judicial efectiva y a un juez imparcial, así como los derechos de la defensa y la presunción de inocencia, sobre todo cuando dichos sistemas de IA no sean lo suficientemente transparentes y explicables ni estén bien documentados".

Siendo los anteriores los riesgos genéricos derivados del uso de sistemas de IA en el ámbito de la persecución penal, los concretos que se derivan para la identificación biométrica y que motivarían una inicial prohibición también son reconocidos de forma expresa por el texto de la Ley de IA. Así, se afirma que el uso de tales sistemas de IA invade especialmente los derechos y las libertades de las personas afectadas, en la medida en que "puede afectar a la vida privada de una gran parte de la población, provocar la sensación de estar bajo una vigilancia constante y disuadir indirectamente a los ciudadanos de ejercer su libertad de reunión y otros derechos fundamentales" [considerando (32)][16]. Se vuelve a insistir, además, en que las imprecisiones técnicas de los sistemas de inteligencia artificial destinados a la identificación biométrica remota de personas físicas "pueden dar lugar a resultados sesgados y entrañar efectos discriminatorios", siendo esto particularmente relevante cuando se trata de edad, etnia, raza, sexo o discapacidad[17]. Y a ello hay que añadir, como se ha dicho, que el riesgo para

16 La LO 4/1997 ya contemplaba en relación a la videovigilancia en espacios públicos, su incidencia en derechos como el de reunión. También sobre los efectos disuasorios de la videovigilancia en otros derechos como la libertad ideológica, el derecho de reunión y de manifestación y la libertad sindical y el derecho de huelga, vid. Arzoz Santisteban, X: "Videovigilancia y derechos fundamentales", en AA.VV.: *Videovigilancia: Ámbito de aplicación y derechos fundamentales afectados. En particular la protección de datos personales* (dir. por J.F. Etxeberria Guridi), Tirant lo Blanch, Valencia, 2011, pp. 177-179.

17 Son numerosos los estudios sobre la existencia de sesgos y su repercusión en la elaboración de algoritmos, en concreto la presencia de diferenciales demográficos ("demographic differentials") en los algoritmos de reconocimiento facial. Vid. Buolamwini, J. y Gebru, T.: "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classication", *Proceedings of Machine Learning Research*, 2018, núm. 81, pp. 1-15; Grother, P.; Ngan, M. y Hanaoka, K.: *Face Recognition Vendor Test (FRVT). Part 3: Demographic Effects*, U.S. Department of Commerce, 2019, [https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf]. Con carácter más general vid. Martínez Martínez, R.: "Inteligencia artificial desde el diseño", *Revista catalana de dret públic*, 2019, núm. 58, p. 73; Fernández Hernández, C.: "La nueva estrategia europea sobre el dato y la inteligencia artificial. Foto fija de un diseño en evolución", *Derecho Digital e Innovación*, 2020, núm. 5, p. 2; Guzmán Fluja, V.: "Sobre la aplicación de la inteligencia artificial a la solución de conflictos", en AA.VV.: *Justicia civil y penal en la era global* (ed. por S. Barona Vilar), Tirant lo Blanch, Valencia, 2017, p. 70.

los derechos y las libertades de las personas afectadas se incrementa cuando los sistemas operan "en tiempo real", debido a la inmediatez de las consecuencias y las escasas oportunidades para realizar comprobaciones o correcciones adicionales [considerandos (32) y (54)].

A los anteriores argumentos que justificarían la prohibición del uso de estos sistemas de IA de identificación biométrica en espacios públicos, añade el texto de enmiendas del Parlamento Europeo que los mismos pueden otorgar a las partes que los implementan "una posición de poder incontrolable" [considerando (8)]. No es ésta, sin embargo, la principal contribución del Parlamento Europeo, sino su propuesta de prohibición absoluta de tales sistemas de IA, sin excepción. El único supuesto que resultaría admisible en opinión de Parlamento, pero también condicionado, sería el relativo a los sistemas de IA de identificación biométrica remota en espacios de acceso público, pero no "en tiempo real", sino "en diferido".

Las enmiendas del Parlamento Europeo en el sentido prohibitivo mencionado, traen causa de antecedentes previos como la Resolución del Parlamento Europeo, de 6 de octubre de 2021[18], que a su vez arranca de un previo Informe de la Comisión de Libertades Civiles, Justicia y Asuntos de Interior de dicho Parlamento, de 13 de julio de 2021[19]. En su Resolución, el Parlamento insta en su apartado (26), la "prohibición permanente" del uso de "análisis automatizados o el reconocimiento en espacios accesibles al público de otras características humanas, como los andares, las huellas dactilares, el ADN, la voz y otras señales biométricas y de comportamiento". No resulta fácil identificar el verdadero alcance de la "prohibición permanente" instada, pues en otros apartados, y referido al empleo de sistemas de reconocimiento facial para la identificación biométrica con fines coercitivos prefiere hacer referencia a una "moratoria" al despliegue de tales sistemas, más que a una prohibición, hasta que se den al menos determinados requisitos y condiciones.

Igualmente crítico, y partidario de la prohibición de los sistemas de IA de identificación biométrica remota que analizamos, es el Dictamen conjunto 5/2021 del CEPD y del SEPD, relativo a la Propuesta de Reglamento inicial de la Comisión. En el mismo se subraya que la identificación biométrica remota de las personas en espacios de acceso público supone un riesgo elevado de intrusión en la vida privada, por lo que se reclama la necesidad de un enfoque más estricto. Se pone el acento en la cuestionable necesidad y proporcionalidad de la aplicación de tales sistemas de IA. Así, el uso de sistemas de IA podría plantear graves problemas de proporcionalidad, ya que podría implicar el tratamiento de datos de un número

18 Sobre la inteligencia artificial en el Derecho penal y su utilización por las autoridades policiales y judiciales en asuntos penales [P9_TA(2021)0405].

19 A9-0232/2021.

indiscriminado y desproporcionado de personas para la identificación de solo unas pocas [apartado (30)]. Por todas estas razones, el CEPD y el SEPD piden una "prohibición general" del uso de la IA para el reconocimiento automatizado de rasgos humanos en espacios de acceso público, como los rostros, pero también la marcha, las huellas dactilares, el ADN, la voz, las pulsaciones de teclas y otras señales biométricas o conductuales, "en cualquier contexto" [apartado (32)][20].

IV. EXCEPCIONES A LA PROHIBICIÓN DE LOS SISTEMAS DE IDENTIFICACIÓN BIOMÉTRICA REMOTA EN ESPACIOS DE ACCESO PÚBLICO CON FINES DE APLICACIÓN DE LA LEY.

Se ha reiterado a lo largo de este trabajo que los numerosos y trascendentes riesgos para los derechos fundamentales que se encuentran vinculados al uso de los sistemas de IA de identificación biométrica a los que nos referimos, han derivado en la opción de su prohibición por parte del legislador europeo. Sin embargo, también se ha insistido, esta prohibición no es absoluta, sino que bajo determinadas condiciones su uso resulta admisible. En efecto, comienza el art. 5 del Título II de la Ley de IA (titulado este último como "prácticas de IA prohibidas") disponiendo de forma categórica que "estarán prohibidas" una serie de prácticas de IA, procediendo a continuación a enumerar las mismas hasta alcanzar en la letra h) de dicho precepto la referencia, como práctica prohibida, al "uso de sistemas de identificación biométrica remota `en tiempo real´ en espacios de acceso público por las autoridades encargadas de la aplicación de la ley, o en su caso en su nombre". Pero una vez enumerado el supuesto de uso proscrito, continúa acto seguido el enunciado normativo con la expresión "salvo y en la medida en que (…)". Esto es, la prohibición no es terminante, sino que admite excepciones, que es lo que veremos.

1. Objetivos legítimos.

Para que el empleo de sistemas de identificación biométrica remota a que nos referimos, en principio prohibidos, resulte justificado es preciso que el mismo esté dirigido a la consecución de unos fines expresamente determinados en dicha letra h). La concurrencia de tales objetivos no es por sí sola suficiente para justificar el empleo de los mencionados sistemas de identificación biométrica al exigir el precepto que concurra una "estricta necesidad" de unos (medios) respecto de los

20 Como ya se ha recogido "supra", el CEPD y el SEPD consideran que no existen razones para excluir de la prohibición la identificación biométrica remota masiva que tiene lugar en línea, o la identificación biométrica remota producida con "demoras significativas"; pero, además, incluye en esa propuesta de "prohibición general" la de la identificación biométrica remota con fines distintos a los de persecución penal al afirmar que el carácter intrusivo del tratamiento no depende necesariamente de su finalidad, pues "el uso de este sistema para otros fines, como la seguridad privada, representa las mismas amenazas para los derechos fundamentales al respeto de la vida privada y familiar y a la protección de los datos personales".

otros (fines). Esto último ya nos remite al carácter extraordinario de tal posibilidad de empleo[21].

El primero de los objetivos contemplados como justificativos sería el de la "búsqueda selectiva de víctimas específicas de secuestro, trata de seres humanos y explotación sexual de seres humanos y la búsqueda de personas desaparecidas" [h).i)]. Se aprecia en el enunciado de dicho supuesto la aspiración por concretar al máximo el marco y límites que hacen posible su admisibilidad, cumpliendo con las exigencias derivadas de que el tratamiento de los datos personales lo sean para fines determinados, explícitos y legítimos[22]. La búsqueda no sólo ha de ser "selectiva" -en contraposición a indiscriminada-, sino también de víctimas "específicas", esto es, ya determinadas. Otro tanto ha de decirse de la concreción expresa de los delitos por los que pasan a ser víctimas (secuestro, etc.) conforme al enunciado del precepto. No se trata de la búsqueda de víctimas de cualquier delito. Las infracciones mencionadas tienen en común que la víctima tiene restringida e impedida su libertad ambulatoria. La diferencia es notable con la versión inicial de la Propuesta de Reglamento de la Comisión y con la versión (Orientación general) del Consejo de la UE que se referían, sin más, a "un delito", sin dar mayor relevancia a la modalidad del mismo.

Junto a las víctimas, este concreto supuesto se refiere al empleo de sistemas de identificación biométrica en la búsqueda de personas desaparecidas. En este caso se amplía el ámbito subjetivo contemplado en el texto original de la Comisión que se refería exclusivamente a los menores desaparecidos. Se ha de entender, a los efectos de evitar la incidencia indiscriminada, que se trata también de una búsqueda selectiva de personas concretas.

El segundo de los objetivos que la Ley de IA estima admisibles en el empleo de sistemas de identificación biométrica, es el de prevención de una amenaza específica, importante e inminente para la vida o la seguridad física de las personas físicas o de una amenaza real y actual o real y previsible de un atentado terrorista [h).ii)]. Claramente se perfilan de nuevo en este segundo supuesto los límites que marcan la excepcionalidad del mismo, por un lado, en relación a la naturaleza de la amenaza -específica, importante, inminente, real, actual o previsible, por lo tanto, de cierta entidad y gravedad, y con proximidad temporal, lo que reduce razonablemente la duración cronológica en el uso de los sistemas de identificación

21 El art 52.1 de la CDFUE condiciona cualquier limitación en el ejercicio de los derechos en ella reconocidos a que la misma sea, entre otros requisitos, respetuosa con el principio de proporcionalidad y, por lo tanto, "necesaria" para alcanzar objetivos de interés general reconocidos por la UE. Es constante la doctrina del TJUE cuando afirma que tales limitaciones exceden de lo "estrictamente necesario" cuando el objetivo de interés general "puede alcanzarse razonablemente de manera tan eficaz por otros medios menos atentatorios respecto de los derechos fundamentales de los interesados" (vid., entre otras, la STJUE, de 30 de enero de 2024, en el asunto C-118/22).

22 Arts. 5.1.b) RGPD y 4.1.b) Directiva (UE) 2016/680 (principios relativos al tratamiento).

biométrica-, por otro lado, en la relevancia de los bienes jurídicos a proteger que pueden verse afectados.

El tercer y último objetivo que podría justificar excepcionalmente el uso de los sistemas de identificación biométrica que nos ocupan consistiría en la localización o identificación de una persona sospechosa de haber cometido un delito a efectos de una investigación, enjuiciamiento o ejecución de sanciones penales por alguno de los delitos mencionados en el nuevo Anexo II que sea punible en el Estado miembro de que se trate con una pena o medida de seguridad privativa de libertad cuya duración máxima sea al menos de cuatro años [h).iii)][23]. Esta tercera salvedad refleja igualmente las consecuencias del proceso negociador entre las tres instituciones europeas competentes.

La versión inicial de la Comisión y el texto del Consejo (Orientación general) contemplaban esta salvedad a la prohibición de los sistemas analizados de forma tan amplia que difícilmente resultaba conciliable con la excepcionalidad ("estrictamente necesario") y el carácter restringido de los supuestos de admisión. Esto es, su proporcionalidad era cuestionable. Además, como se ha dicho, el Parlamento Europeo era partidario de una prohibición absoluta de estos sistemas de identificación biométrica, salvo que se tratara de una identificación en diferido y, también en estos casos, con relevantes limitaciones. Finalmente se ha optado por una solución intermedia, aunque más próxima a la de los postulados del texto en su versión original.

La Propuesta original de la Comisión permitía excepcionar la prohibición con la finalidad de detectar, localizar o identificar a sospechosos de haber cometido cualquiera de los delitos comprendidos en el art. 2.2 de la Decisión Marco 2002/584/JAI, de 13 de junio de 2002, relativa a la orden europea de detención y entrega. Esto es, los que se han venido a denominar "eurodelitos" en la medida en que se han reproducido por remisión en numerosos instrumentos normativos europeos relativos a la cooperación judicial penal y al reconocimiento mutuo de resoluciones judiciales. La amplitud de la excepción era aún mayor en el texto del Consejo, pues a los anteriores añadía cualquier "otro delito" para el que la normativa del Estado miembro de que se trate imponga una pena o medida de seguridad privativa de libertad cuya duración máxima sea de al menos 5 años.

23 Los delitos que comprende el Anexo II son los siguientes: terrorismo; tráfico de seres humanos; explotación sexual de niños y pornografía infantil; tráfico ilícito de estupefacientes y sustancias psicotrópicas; tráfico ilícito de armas, municiones y explosivos; asesinato, lesiones corporales graves; comercio ilícito de órganos y tejidos humanos; tráfico ilícito de materiales nucleares o radiactivos; secuestro, retención ilegal y toma de rehenes; crímenes dentro de la jurisdicción de la Corte Penal Internacional; apoderamiento ilícito de aeronaves/buques; violación; delitos ambientales; robo organizado o a mano armada; sabotaje; participación en una organización criminal involucrada en uno o más delitos enumerados anteriormente.

Estas excepciones a la prohibición de los sistemas de identificación biométrica como punto de partida son de tal amplitud que existía un riesgo evidente de que lo excepcional fuera precisamente la prohibición. El texto definitivo reduce, por un lado, el listado de infracciones inicial de forma considerable (justamente a la mitad). Quedan al margen muchos de los delitos contemplados en la Decisión Marco 2002/584/JAI que tienen en común su carácter patrimonial o económico (fraudes, estafas, falsificaciones, etc.), manteniéndose en esencia los delitos más relacionados con bienes jurídicos como la vida, la libertad, la integridad, la libertad e indemnidad sexuales, etc. Por otro lado, se ha aumentado el umbral punitivo justificativo de los tres a los 4 años de duración. En todo caso, el listado resulta todavía excesivamente amplio en nuestra opinión considerando el elevado número de personas que pueden verse afectadas por la vigilancia e identificación biométrica de forma indiscriminada y puede derivar en desproporcionalidad.

En su descargo hay que matizar que se trata de un objetivo o finalidad justificativa, pero no por sí mismo legítimo, pues han de darse otras muchas condiciones y requisitos al objeto de asegurar la proporcionalidad de la medida.

2. Principio de proporcionalidad.

El alcance de los objetivos legítimos indicados a través de los sistemas de identificación biométrica ha de sujetarse a determinados presupuestos en aras de garantizar su proporcionalidad tal como exige el art. 52.1 CDFUE[24]. Concretados los primeros, el texto de la Ley de IA fija, a su vez, una serie de criterios orientados sin duda a que sirvan a la ponderación de la proporcionalidad de dicho uso en el caso concreto. Así, el apartado 2 del art. 5 dispone que los sistemas de identificación biométrica que nos ocupan, prohibidos en principio, "sólo podrán desplegarse" conforme a los legítimos objetivos analizados y para confirmar la identidad de la persona que constituya el objetivo específico teniendo en cuenta, para ello, una serie de aspectos.

Por un lado, la naturaleza de la situación que dé lugar al posible uso, y en particular la gravedad, probabilidad y magnitud del perjuicio que se produciría de no utilizarse el sistema. Por otro lado, las consecuencias que la utilización del sistema tendría para los derechos y las libertades de las personas implicadas, y en particular la gravedad, probabilidad y magnitud de dichas consecuencias. Nos

24 Dice así el precepto: "Cualquier limitación del ejercicio de los derechos y libertades reconocidos por la presente Carta deberá ser establecida por la ley y respetar el contenido esencial de dichos derechos y libertades. Sólo se podrán introducir limitaciones, respetando el principio de proporcionalidad, cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás".

encontramos ante criterios de ponderación que resultan habituales en el juicio sobre la proporcionalidad de la medida[25].

El art. 5.2 hace igualmente referencia expresa a la proporcionalidad en las condiciones de uso de los sistemas de identificación biométrica remota y de forma también expresa se citan en el mismo con gran acierto las limitaciones temporales, geográficas y personales[26]. En efecto, resulta obvio que si han de ponderarse las consecuencias que para los derechos y libertades de los ciudadanos se han de derivar de los sistemas de identificación biométrica (gravedad, probabilidad y magnitud) la fijación de límites temporales a su uso resulta determinante, pues mayor será la incidencia cuanto más se extienda cronológicamente la aplicación de aquéllos (mayor será el número de personas que transiten en dicho espacio de acceso público). Igualmente trascendental resulta la necesidad de establecer limitaciones al espacio de acceso público afectado (geográficas). Ello obliga a no utilizar de forma indiscriminada desde una visión espacial los sistemas de identificación biométrica, sino limitar su uso a los espacios en los que indiciariamente pudieran hallarse las víctimas o personas desaparecidas o donde pudieran localizarse también indiciariamente las personas sospechosas de haber cometido los delitos arriba relacionados o los espacios correspondientes a las infraestructuras críticas concretas afectadas. Las limitaciones que proceden desde el ámbito subjetivo también resultan significativas. Si la víctima, persona desaparecida o presunto autor del delito cuya identidad biométrica se pretenda establecer presentan determinadas características o rasgos específicos, el sistema de IA se debería limitar a centrarse en aquellas personas físicas que presentan tales rasgos descartando las restantes respecto de las cuales no se procederá a la obtención de la plantilla biométrica correspondiente, ni a la comparación con los datos biométricos almacenados previamente.

Al hilo de lo anterior, resulta igualmente esencial a efectos de ponderar la proporcionalidad de la medida, la expresa obligación que condiciona la autorización del uso de los sistemas de identificación biométrica remota a que las autoridades competentes para la represión penal realicen con carácter previo a su aplicación una evaluación de impacto relativa a los derechos fundamentales (art. 5.2.III). El art. 27 de la Ley de IA ya contempla con carácter general la obligación que corresponde al implementador de sistemas de IA de alto riesgo de llevar a cabo una evaluación de impacto relativa a la protección de datos impuesta por el art. 35 del RGPD y el art.

25 Estos criterios ya existen en nuestro ordenamiento procesal penal bajo la denominación de los principios de excepcionalidad y necesidad y con análogo significado (art. 588 bis.a.5 LECrim).

26 Iglesias Canle, I.C.: "Registros biométricos y su aplicación al proceso penal en España e Italia", en AA.VV.: *Inteligencia Artificial legal y Administración de Justicia* (dir. por S. Calaza López y M. Llorente Sánchez-Arjona), Aranzadi, Cizur Menor, 2022, p. 348.

27 de la Directiva (UE) 2016/680[27]. Ahora, se incorpora en el texto definitivo una nueva obligación de evaluar en el uso de sistemas de identificación biométrica el impacto, no sólo respecto de la protección de datos, sino que de forma conjunta a esta, respecto de los "derechos fundamentales", contemplada en el art. 27 de la Ley de IA. Esta evaluación de impacto ha de realizarse con anterioridad a la implementación del sistema. También se ha de proceder por parte de las autoridades competentes en la persecución penal al registro del sistema en la base de datos de la UE para sistemas de alto riesgo contemplados en el Anexo III (art. 49 Ley de IA). El art. 5.2.III contempla como única salvedad que en casos de urgencia debidamente justificados, podrá comenzarse a usar el sistema, sin perjuicio de que se proceda al registro posteriormente sin demora indebida.

3. Autorización judicial o de una autoridad administrativa independiente.

Junto a los requisitos hasta ahora señalados, añade el art. 5.3 como justificativo del mismo, que cualquier uso concreto de un sistema de identificación biométrica remota "en tiempo real" en un espacio de acceso público con fines represivos "estará supeditado a la concesión de una autorización previa por parte de una autoridad judicial o una autoridad administrativa independiente del Estado miembro donde vaya a utilizarse dicho sistema". Aunque el texto constitucional español no imponga expresamente la reserva jurisdiccional para este tipo de actuaciones, no cabe duda de que se ha pretendido con la exigencia de dicha autorización judicial establecer un marco de garantías suficiente ante la entidad de las injerencias en un amplio grupo de afectados. Las dudas surgen a la hora de concretar qué órgano jurisdiccional concreto será el competente para autorizar, en su caso, el empleo de los sistemas de identificación biométrica que nos ocupan.

En efecto, algunas de las finalidades que legitiman el uso de tales sistemas tienen indudablemente una clara naturaleza procesal penal. Así la búsqueda selectiva de víctimas de los delitos graves citados más arriba o la localización e identificación de personas sospechosas de haber cometido los delitos que figuran en el Anexo II de la Ley de IA. Siendo esto así, la autorización podría corresponder al órgano jurisdiccional del orden penal que resulte competente, es decir, usualmente el Juez de Instrucción o el Juez Central de Instrucción pues algunos de los delitos del Anexo II se encuadrarían en el listado de los del art. 65 LOPJ competencia de la Audiencia Nacional. Sin embargo, otras finalidades legitimadoras se corresponden con una naturaleza preventiva de carácter administrativo, así la búsqueda de

27 Para ello se utilizará, dice el mencionado precepto, la información facilitada conforme al art. 13 de la Ley de IA, también relativo a los sistemas de IA de alto riesgo (transparencia y comunicación de información a los implementadores). Vid. con carácter general sobre la evaluación de impacto Miralles López, R.: "La evaluación de impacto relativa a la protección de datos (comentario al artículo 35 RGPD)", en AA.VV.: *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales*, (dir. por A. Troncoso Reigada), Tomo I, Civitas, Cizur Menor, 2021, pp. 2137-2162.

personas desaparecidas no relacionadas con un hecho delictivo o la prevención de amenazas de terrorismo u otras graves cuando sean específicas, importantes e inminentes. Ya se ha visto que los fines de aplicación de la ley ("law enforcement"), tal como vienen definidos en la Ley de IA, comprenden un amplio abanico de actividades que van desde la prevención del delito hasta su enjuiciamiento y ejecución, pero incluye también la protección y prevención frente a amenazas para la seguridad pública [art. 3 (46)]. De naturaleza administrativa algunas, por lo tanto, y procesal penal otras. Igual amplitud encontramos en la definición de autoridades encargadas de la aplicación de la ley, que ostentan una u otra naturaleza dependiendo de las funciones que tengan atribuidas.

En el caso de que una autoridad jurisdiccional debiera de autorizar el empleo de sistemas de identificación biométrica remota que se vincula con fines preventivos, podría corresponder dicha competencia a los Juzgados de lo Contencioso-administrativo, que ya cuentan en la actualidad con facultad para autorizar la entrada en domicilios u otros edificios cuyo acceso requiera el consentimiento de su titular para la ejecución forzosa de actos de la Administración (art. 91.2 LOPJ).

La alternativa a la autorización judicial podría ser, según el texto de la Ley de IA, la autorización previa de una "autoridad administrativa independiente" del Estado miembros donde vaya a utilizarse el sistema en cuestión. Aunque pareciera un contrasentido calificar como independiente a una autoridad administrativa, lo cierto es que no constituye para nada una realidad absolutamente extraña. En materia de protección de datos, sin ir más lejos, se exige que en cada Estado miembro de la UE exista una autoridad de control independiente, que no deja de tener naturaleza administrativa. La LO 3/2018, de Protección de Datos Personales y garantía de los derechos digitales, dispone sobre este punto que "la Agencia Española de Protección de Datos es una autoridad administrativa independiente de ámbito estatal" (art. 44.1)[28]. No con ello queremos sugerir que estas autoridades de control independiente sean las más adecuadas para autorizar el uso de sistemas de identificación biométrica remota en casos puntuales. Ya tienen reconocidas otras facultades importantes en la materia que nos ocupa.

En el ordenamiento jurídico español bien podrían satisfacer esa condición de autoridad administrativa independiente las Comisiones de Videovigilancia contempladas en la LO 4/1997, de videovigilancia en espacios públicos por las FF. y CC. de Seguridad. Se trata esta Comisión de un órgano colegiado presidido por un Magistrado (art. 3.1) que ha de ser el Presidente del Tribunal Superior de

28 Las autoridades administrativas independientes de ámbito estatal están mencionadas en la Ley 40/2015, de Régimen Jurídico del Sector Público y son definidas como "entidades de derecho público que, vinculadas a la Administración General del Estado y con personalidad jurídica propia, tienen atribuidas funciones de regulación o supervisión de carácter externo sobre sectores económicos o actividades determinadas, por requerir su desempeño de independencia funcional o una especial autonomía respecto de la Administración General del Estado, lo que deberá determinarse en una norma con rango de Ley" (art. 109).

Justicia de la Comunidad Autónoma respectiva (art. 3.2) y en "cuya composición no serán mayoría los miembros dependientes de la Administración autorizante" (art. 3.1). La composición y funcionamiento de la Comisión, así como la participación de los municipios en ella, se determinan reglamentariamente, y en la medida en que determinadas Comunidades Autónomas tienen competencias en materia de seguridad pública, dicha composición es diversa en cada caso, pero respetando en la misma el requisito de no resultar mayoría la administración autorizante. Estas Comisiones no autorizan el uso de sistemas de videovigilancia, sino que informan al respecto de modo preceptivo y vinculante (art. 3.3). Aunque estas Comisiones de Videovigilancia pudieran satisfacer la demanda de ser autoridad independiente[29], no por ello desaparecerían todos los inconvenientes que se plantean si trasladamos este escenario al contexto de la identificación biométrica remota sin las oportunas reformas legales. Ya hemos visto, por ejemplo, que la Ley de IA contempla una definición muy amplia de los espacios de acceso público que incluyen incluso los de naturaleza privada o los que sirven para fines muy diversos (ocio, mercantiles, etc.). La LO 4/1997 contempla una definición mucho más restrictiva de tales espacios, de los que se excluyen, entre otros muchos, los privados.

La autorización arriba indicada irá precedida de una solicitud de la autoridad competente para la aplicación de la ley ("law enforcement") conforme a las normas detalladas del derecho nacional interno a las que haremos referencia después. Sin embargo, cuando en casos de urgencia no sea posible obtener dicha autorización[30], podrá comenzar a hacerse uso de los sistemas de identificación biométrica remota sin la misma, siempre y cuando sea solicitada aquélla a la mayor brevedad y en todo caso antes de las 24 horas. Si fuera denegada la autorización, se procederá inmediatamente a interrumpir el uso de los sistemas de identificación biométrica y a desechar suprimir todos los datos y resultados de salida que se hayan obtenido (art. 5.3.I)[31]. La solicitud de las autoridades competentes en la aplicación de la ley

29 Ver acerca de las Comisiones de Videovigilancia: De la Iglesia Chamarro, A.: "Las Comisiones de Garantías de la Videovigilancia", *Revista de Derecho Político*, 2007, núm. 68, pp. 217; Etxeberria Guridi, J.F.: "La Comisión de Videovigilancia y Libertades del País Vasco: funciones y experiencias", en AA.VV.: *Videovigilancia. Ámbito de aplicación y derechos fundamentales afectados. En particular la protección de los datos personales*, (dir. por J.F. Etxeberria Guridi), Tirant lo Blanch, Valencia, 2011, pp. 107-142.

30 Se refieren los considerandos como tales a las situaciones en las que "la necesidad de utilizar los sistemas en cuestión sea tan imperiosa que imposibilite, de manera efectiva y objetiva, obtener una autorización antes de iniciar el uso". Aunque no lo diga expresamente la Ley de IA en su articulado, sí se especifica en los considerandos, cerrando al máximo los resquicios a una actuación inadecuada, que en la solicitud de autorización ex post habrán de indicar los motivos por los que no se ha realizado la solicitud con anterioridad. Además, para estas situaciones de urgencia, el uso de tales sistemas de IA debería limitarse "al mínimo imprescindible" y cumplir las salvaguardias y las condiciones oportunas, conforme a lo estipulado en el Derecho interno y según corresponda en cada caso concreto de uso urgente por parte de las autoridades encargadas de la aplicación de la ley [considerando (35)].

31 La expresión "todos los datos", viene a significar todos los vinculados con el uso del sistema concreto cuya autorización ha sido denegada, así los datos de entrada directamente obtenidos mediante el uso del sistema de IA en cuestión y los resultados y datos de salida directamente vinculados con la autorización denegada. Quedarían excluidos de esta drástica solución los datos de entrada que hubieran sido legalmente adquiridos conforme a otra norma nacional o de la UE [considerando (35)]

ha de ser motivada, pues se habrá de justificar la concurrencia de los requisitos por los que un uso prohibido en principio resulta admisible. Por las mismas razones habrá de ser motivada la autorización judicial o de la administración independiente, aunque no se diga nada al respecto[32]. Lo que sí queda claro de forma reiterada en la versión definitiva del texto es el carácter vinculante de la decisión que adopte la autoridad judicial o la administrativa independiente.

Aunque no resulte precisa ninguna otra autorización, sí se requiere a efectos de transparencia (gobernanza) la intervención de otras autoridades. En concreto, dispone el art. 5.4 que cada uso que de sistemas de identificación biométrica remota se haga se deberá notificar a las respectivas, autoridad nacional de protección de datos, por un lado, y autoridad nacional de vigilancia del mercado, por otro. Estas autoridades habrán, a su vez, de remitir anualmente un informe a la Comisión respecto de los usos de sistemas de identificación biométrica remota en espacios públicos que les hayan sido notificados. A su vez, la Comisión publicará informes anuales al respecto (art. 5.6).

4. La previsión legislativa en el Derecho interno.

La primera de las garantías que contempla el art. 52.1 CDFUE a los efectos de que resulte admisible cualquier limitación en el ejercicio de los derechos y libertades reconocidos por dicha Carta, es que la misma esté establecida por la ley. El texto de la Ley de IA parte, como se ha dicho, de la prohibición del uso de los sistemas de identificación biométrica remota a que nos referimos, pero fija a continuación una serie de requisitos y condiciones que pueden excepcionar dicha prohibición. El art. 5 que hemos ido analizando hasta ahora constituye el marco regulatorio en el que tienen cabida las salvedades a la prohibición general. Constituiría un marco de máximos, que en principio no podría ser rebasado por el ordenamiento concreto de cada Estado miembro, pero que deja a éstos un margen de actuación soberano dentro de aquellos límites. De ahí que la Ley de IA apremie a los Estados miembros a que aborden la regulación de la materia ajustando cada uno la misma a sus particularidades normativas e institucionales. El apremio es, por otra parte, específico. No se trata de regular la materia, sino de que se dote en cada caso de las "reglas detalladas necesarias" (art. 5.5).

32 El deber de motivación se deriva de los requisitos que condicionan la concesión de la autorización según el texto de la Ley, esto es, que con fundamento en las pruebas objetivas o los indicios claros expuestos ante la autoridad judicial o administrativa, se acredita que el uso del sistema de identificación biométrica remota en cuestión resulta necesario y proporcionado para alcanzar algunos de los objetivos legítimos especificados en el apartado 1 y determinados en la solicitud, y en particular que queda limitada a lo que resulte estrictamente necesario en relación al alcance temporal, geográfico y personal. La ley impone igualmente que la autoridad competente para la autorización considere en su decisión las circunstancias y criterios mencionados en el apartado 2 -gravedad, probabilidad y alcance de los perjuicios de no emplear el sistema de IA en cuestión; gravedad, probabilidad y alcance de los perjuicios en los derechos y libertades de las personas afectadas, etc.- (art. 5.3.II).

La primera expresión del margen de actuación autónoma de los Estados miembros reside en la opción de incorporar o no el posible uso de los sistemas de identificación biométrica remota en el ordenamiento interno. Comienza el precepto mencionado indicando que los Estados miembros "podrán decidir contemplar la posibilidad de autorizar" el uso de sistemas de identificación biométrica remota. Más contundente, afirma el considerando (37) que aquéllos "siguen siendo libres de no ofrecer esa posibilidad en absoluto". Si los Estados miembros optan en su ordenamiento por incorporar la posibilidad excepcional contemplada en la Ley de IA, mantienen igualmente el margen de actuación para decidir si lo hacen en toda su extensión o "parcialmente", como también contempla el texto de la Ley. En cualquier caso, esa libertad de opción no puede exceder, como se ha dicho, del marco permisivo de la Ley de IA, esto es, "dentro de los límites y en las condiciones que se indican en los apartados 1.h), 2 y 3". Las "reglas detalladas" del derecho interno habrán de especificar respecto de cuales objetivos legítimos a perseguir del apartado h) -búsqueda selectiva de víctima, de persona desaparecida, etc.- podrán las autoridades competentes autorizar el uso de sistemas de identificación biométrica remota, y respecto de cuales delitos mencionados en el subapartado iii). Esas mismas "reglas detalladas" habrán de especificar, igualmente, los pormenores del procedimiento de solicitud, concesión y ejercicio de las autorizaciones concedidas, así como lo relativo a la supervisión y notificación relacionadas con aquéllas.

Hacemos hincapié, con el entrecomillado, en la exigencia de una regulación pormenorizada en el derecho nacional de los Estados miembros. Esta es una cuestión que se le resiste con frecuencia al legislador español[33], que usualmente regula lo relativo a la necesaria previsión legal de actuaciones restrictivas de derechos y libertades con retraso y al albur de previa jurisprudencia de los tribunales[34]. E insistimos en ello, precisamente, porque no podemos sustraernos al deber de denunciar que el único precepto que actualmente podría resultar aplicable en este sentido en cumplimiento de la exigencia de previsión legal habilitante, no puede estimarse que cumple con tales exigencias de precisión y suficiencia, ni para el caso concreto que analizamos ahora -identificación biométrica remota-, ni para ningún otro.

Nos referimos a la lamentable disposición que sobre el uso de datos biométricos se contempla en la LO 7/2021, de protección de datos personales tratados para fines de prevención y represión penal. El art. 13 de dicha LO, relativo al tratamiento

33 Se trata ésta de una exigencia particularmente destacada en la materia que nos ocupa. Vid. Cotino Hueso, L.: "Una regulación legal y de calidad para los análisis automatizados de datos o con inteligencia artificial. Los altos estándares que exigen el Tribunal Constitucional alemán y otros tribunales, que no se cumplen ni de lejos en España", *Revista General de Derecho Administrativo,* 2023, núm. 63, pp. 1-22.

34 Ejemplo ilustrativo, la LO 13/2015, de 5 de octubre, que modifica la LECrim para regular medidas de investigación tecnológicas.

de categorías especiales de datos personales -entre los que se incluyen los datos biométricos dirigidos a identificar de manera unívoca a una persona física-, dispone que dicho tratamiento "sólo se permitirá" cuando resulte estrictamente necesario, con sujeción a las garantías adecuadas para los derechos y libertades del interesado y cuando se cumplan alguna de las circunstancias que se mencionan, entre las que se incluye que se "encuentre previsto por una norma con rango de ley o por el Derecho de la Unión Europea". Esta es una reproducción literal de la exigencia de previsión legal contemplada en el art. 10 de la Directiva (UE) 2016/680. Por ese mismo motivo estimamos que resulta absolutamente insuficiente, y una parodia a la exigencia de regulación detallada, la previsión contemplada en el apartado 2 del precepto indicado cuando dispone que "las autoridades competentes, en el marco de sus respectivas funciones y competencias, podrán tratar datos biométricos dirigidos a identificar de manera unívoca a una persona física con los fines de prevención, investigación, detección de infracciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública"[35].

Queda pendiente, por lo tanto, de perfilar cuál es la opción del legislador español en cuanto al uso de los sistemas de identificación biométrica remota, una vez denunciada la insuficiente previsión del art. 13.2 LO 7/2021 contemplada desde las exigencias reclamadas por el art. 5.5 de la Ley de IA. Con qué extensión pretende que resulten admisibles los sistemas de identificación biométrica en el marco, siempre, de lo previsto en la Ley de IA. En todo caso, procede ahora ya señalar que la libertad limitada reconocida a los Estados miembros a la hora de regular la materia puede derivar en una regulación jurídica dispar en los distintos Estados miembros y resultar un inconveniente desde el punto de vista de la cooperación judicial en materia penal y del reconocimiento mutuo de resoluciones judiciales -sería el caso de la orden europea de investigación, que podría experimentar asimetrías desde el punto de vista de los derechos fundamentales afectados y de la posibilidad o no de restricciones en los mismos-.

V. BREVES CONCLUSIONES.

Los sistemas de identificación biométrica remota en tiempo real en espacios de acceso público con fines de aplicación de la ley (penal) repercuten sobremanera en un amplio abanico de derechos fundamentales y conllevan aparejados elevados riesgos de actuación sesgada y discriminatoria. Ante esta tesitura, la recientemente aprobada Ley de IA está llamada a desempeñar un papel esencial. Reflejo de la situación descrita, ha quedado patente la distinta sensibilidad para con los derechos de los ciudadanos afectados entre las distintas instituciones europeas llamadas a

35 Vid. igualmente al respecto las críticas de Suárez Xavier, P.R.: *Informe sobre aspectos bioéticos, legales y procesales del derecho a la intimidad y el uso de procedimientos de reconocimiento facial por las fuerzas y cuerpos de seguridad*, Colex, Madrid, pp. 68 y ss.

participar en el procedimiento legislativo. La posición del Parlamento Europeo ha resultado esencial, poniendo freno a las iniciales propuestas de la Comisión y del Consejo al respecto.

Como resultado de los riesgos expresados, la Ley de IA europea adopta como punto de partida la prohibición del uso de los sistemas de identificación biométrica señalados. Sin embargo, esta prohibición no es absoluta y en el marco de determinados presupuestos y conforme a los principios de estricta necesidad y proporcionalidad puede resultar admisible. Ha de entenderse que los límites fijados en la Ley de IA para que el uso de tales sistemas resulte admisible han de considerarse de máximos y que corresponde a los Estados miembros concretar en cada ordenamiento y mediante "reglas detalladas" los criterios y parámetros mencionados. Esta cuestión resulta esencial, bajo el riesgo de que la regla general de la prohibición se pervierta y se convierta en excepción.

BIBLIOGRAFIA

Arzoz Santisteban, X: "Videovigilancia y derechos fundamentales", en AA.VV.: *Videovigilancia: Ámbito de aplicación y derechos fundamentales afectados. En particular la protección de datos personales* (dir. por J.F. Etxeberria Guridi), Tirant lo Blanch, Valencia, 2011.

Buolamwini, J. y Gebru, T.: "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classication", *Proceedings of Machine Learning Research*, 2018, núm. 81.

Cano Ruiz, I.: "Artículo 9. Categorías especiales de datos", en AA.VV.: *Protección de Datos: Comentarios a la Ley Orgánica de Protección de Datos y Garantías Digitales (en relación con el RGPD)* (dir. por M. Arenas Ramiro y A. Ortega Giménez), Sepín, Madrid, 2019.

Cotino Hueso, L.: "Reconocimiento facial automatizado y sistemas de identificación biométrica bajo la regulación superpuesta de inteligencia artificial y protección de datos", en AA.VV.: *Derecho Público de la Inteligencia Artificial* (coord. por F. Balaguer Callejón y L. Cotino Hueso), Fundación Manuel Giménez Abad, Madrid, 2023.

Cotino Hueso, L.: "Una regulación legal y de calidad para los análisis automatizados de datos o con inteligencia artificial. Los altos estándares que exigen el Tribunal Constitucional alemán y otros tribunales, que no se cumplen ni de lejos en España", *Revista General de Derecho Administrativo,* 2023, núm. 63.

De la Iglesia Chamarro, A.: "Las Comisiones de Garantías de la Videovigilancia", *Revista de Derecho Político,* 2007, núm. 68.

Escajedo San-Epifanio, L.: *Tecnologías biométricas, identidad y derechos fundamentales,* Aranzadi, Cizur Menor, 2017.

Etxeberria Guridi, J.F.: "La Comisión de Videovigilancia y Libertades del País Vasco: funciones y experiencias", en AA.VV.: *Videovigilancia. Ámbito de aplicación y derechos fundamentales afectados. En particular la protección de los datos personales* (dir. por J.F. Etxeberria Guridi), Tirant lo Blanch, Valencia, 2011.

European Union Agency for Fundamental Rights (FRA): *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 2020.

Fernández Hernández, C.: "La nueva estrategia europea sobre el dato y la inteligencia artificial. Foto fija de un diseño en evolución", *Derecho Digital e Innovación*, 2020, núm. 5.

Grother, P.; Ngan, M. y Hanaoka, K.: *Face Recognition Vendor Test (FRVT). Part 3: Demographic Effects*, U.S. Department of Commerce, 2019, [https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf].

Guzmán Fluja, V.: "Sobre la aplicación de la inteligencia artificial a la solución de conflictos", en AA.VV.: *Justicia civil y penal en la era global* (ed. por S. Barona Vilar), Tirant lo Blanch, Valencia, 2017.

Iglesias Canle, I.C.: "Registros biométricos y su aplicación al proceso penal en España e Italia", en AA.VV.: *Inteligencia Artificial legal y Administración de Justicia* (dir. por S. Calaza López y M. Llorente Sánchez-Arjona), Aranzadi, Cizur Menor, 2022.

Martínez Martínez, R.: "Inteligencia artificial desde el diseño", *Revista catalana de dret públic*, 2019, núm. 58.

Miralles López, R.: "La evaluación de impacto relativa a la protección de datos (comentario al artículo 35 RGPD)", en AA.VV.: *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales* (dir. por A. Troncoso Reigada), Tomo I, Civitas, Cizur Menor, 2021.

Richard González, M.: "Los sistemas biométricos de reconocimiento facial en la Unión Europea en el marco del desarrollo de la Inteligencia Artificial", *Justicia*, 2023, núm. 1.

Romeo Casabona, C.M.: "Datos personales (comentario al artículo 4.1 RGPD)", en AA.VV.: *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales* (dir. por A. Troncoso Reigada), Tomo I, Thomson-Aranzadi, Cizur Menor, 2021.

Suárez Xavier, P.R.: *Informe sobre aspectos bioéticos, legales y procesales del derecho a la intimidad y el uso de procedimientos de reconocimiento facial por las fuerzas y cuerpos de seguridad*, Colex, Madrid.

INTELIGENCIA ARTIFICIAL EN LA JUSTICIA CON PERSPECTIVA DE GÉNERO: AMENAZAS Y OPORTUNIDADES*

ARTIFICIAL INTELLIGENCE WITH GENDER PERSPECTIVE: THREATS AND OPPORTUNITIES

Actualidad Jurídica Iberoamericana Nº 21, agosto 2024, ISSN: 2386-4567, pp. 566-597

* Estudio redactado en el marco del Proyecto "Claves para una justicia digital y algorítmica con perspectiva de género", PID2021-123170OB-I00 financiado por MCIN/ AEI/10.13039/501100011033.

Ana
MONTESINOS
GARCÍA

ARTÍCULO RECIBIDO: 29 de mayo de 2023
ARTÍCULO APROBADO: 1 de julio de 2024

RESUMEN: Comienza a instaurarse, aunque todavía de manera incipiente, el uso de aplicaciones y herramientas basadas en inteligencia artificial en la Justicia. En este trabajo analizamos sus riesgos y beneficios desde una perspectiva de género. En primer lugar, estudiamos las amenazas que suponen los sesgos algorítmicos que refuerzan los estereotipos de género, así como la posible incorporación en el acervo probatorio de un proceso de los denominados deepfakes, nuevas formas de violencia ejercida a través de la IA cuyas principales víctimas son las mujeres. En segundo lugar, abordamos el empleo de herramientas algorítmicas en la lucha contra el mayor exponente de la desigualdad como es la violencia de género. En concreto, para atender a las víctimas, investigar determinados delitos y prevenir su ejecución mediante técnicas predictivas que valoran el riesgo de reincidencia.

PALABRAS CLAVE: Inteligencia artificial; justicia; perspectiva de género; sesgos; deepfakes y herramientas de valoración del riesgo.

ABSTRACT: *The use of applications and tools based on artificial intelligence in the justice system is beginning to be implemented, although it is still in its infancy. In this paper, we analyse their risks and benefits from a gender perspective. First, we examine the threats posed by algorithmic biases that reinforce gender stereotypes, as well as deepfakes as new forms of violence perpetrated by AI, whose main victims are women. Second, we look at the use of algorithmic tools in the fight against the greatest exponent of inequality, such as gender-based violence. Specifically, to support victims, to investigate certain crimes and to prevent their execution through predictive techniques that assess the risk of recidivism.*

KEY WORDS: *Artificial intelligence, justice, gender perspective, biais, deepfakes, risk assessment instruments.*

I. INTRODUCCIÓN: JUSTICIA ALGORÍTMICA CON PERSPECTIVA DE GÉNERO.

La inteligencia artificial (en adelante, IA[1]) ha experimentado un significativo progreso, convirtiéndose en una de las tecnologías estratégicas del siglo XXI. En concreto y en lo que a este trabajo se refiere, en los últimos años se ha constatado la oportunidad de su utilización en la Administración de Justicia. Posee la capacidad de generar notables beneficios en términos de eficiencia, eficacia y precisión, pero no se puede obviar que también conlleva riesgos sustanciales para los derechos fundamentales. Precisamente a sus bondades y peligros dedicamos este trabajo, en el que vamos a analizar ambas vertientes desde una perspectiva de género.

Para ello, partiremos de una doble premisa. Por un lado, la IA comienza, aunque todavía de manera incipiente, a instaurarse en la Administración de Justicia. Distintas herramientas computacionales, sistemas algorítmicos y softwares informáticos de última generación empiezan a utilizarse para cumplir múltiples objetivos. Desde simples tareas instrumentales de gestión procesal, burocráticas, organizativas y rutinarias (donde inicialmente se han implantado), hasta otras funcionales de mayor complejidad. Entre estas últimas, cabría distinguir aquellas herramientas asistenciales o colaboradoras, de aquellas otras que directamente ofrecen la solución (propositiva o imperativa)[2]. Consciente nuestro legislador del amplio abanico de posibilidades que pueden brindar a la Justicia, recientemente se ha regulado el empleo de nuevas herramientas algorítmicas para fines que sirvan de apoyo a la función jurisdiccional y a la tramitación de procedimientos judiciales en el Real Decreto-ley 6/2023, de 19 de diciembre, por el que se aprueban

1 Aunque somos conocedoras de que no todos los softwares son IA, vamos a utilizar el término IA en sentido amplio, sin ajustarnos a la definición del Reglamento de IA, que es mucho más estricta "Sistema de IA: un sistema basado en una máquina diseñado para funcionar con distintos niveles de autonomía, que puede mostrar capacidad de adaptación tras el despliegue y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar información de salida, como predicciones, contenidos, recomendaciones o decisiones, que puede influir en entornos físicos o virtuales" (art. 3.1).

2 Barona Vilar, S.: "Datización de la justicia (Algoritmos, Inteligencia Artificial y Justicia, ¿el comienzo de una gran amistad?)", *Revista Boliviana de Derecho*, 2023, núm. 36, p. 26.

• Ana Montesinos García
Profesora titular de Derecho Procesal, Universitat de València. Correo electrónico: ana.montesinos@uv.es.

medidas urgentes para la ejecución del Plan de Recuperación, Transformación y Resiliencia en materia de servicio público de justicia, función pública, régimen local y mecenazgo[3].

Por otro lado, nuestro legislador, incitado por compromisos internacionales y europeos[4], aboga por la incorporación de la perspectiva de género en la Justicia en aras de remover los obstáculos que dificultan la consecución de la igualdad efectiva entre hombres y mujeres[5]. En este sentido, la Ley Orgánica 3/2007, de 22 de marzo, para la igualdad efectiva de mujeres y hombres califica expresamente la igualdad de trato y de oportunidades entre mujeres y hombres, como principio informador del ordenamiento jurídico y, como tal, se integrará y observará en la interpretación y aplicación de las normas jurídicas (art. 4)[6]. Se interpela así a los operadores jurídicos a aplicar la perspectiva de género. Además, su artículo 15 dispone que el principio de igualdad de trato y oportunidades entre mujeres y hombres informará, con carácter transversal, la actuación de todos los Poderes Públicos. Las Administraciones públicas lo integrarán, de forma activa, en la adopción y ejecución de sus disposiciones normativas, en la definición y presupuestación de políticas públicas en todos los ámbitos y en el desarrollo del conjunto de todas sus actividades. De ahí que, como defiende Barona Vilar, "una de las claves de desarrollo de la Justicia en el siglo XXI es indudablemente la feminización de la misma"[7].

Nos encaminamos, por consiguiente, hacia un modelo de Justicia cada vez más digital y algorítmico, cuya transformación debe necesariamente llevarse a cabo desde un enfoque de género, pues solo así podrá garantizarse la igualdad consagrada en el artículo 14 de nuestra Carta Magna[8]. Sin embargo, la intersección

3 BOE núm. 303, de 20.12.2023.

4 Tanto el Tratado de Ámsterdam como el Tratado de Lisboa establecen como objetivo de la Unión la eliminación de las desigualdades entre el hombre y la mujer y promueven su igualdad (art. 3.2 y art 8, respectivamente). A lo que debemos añadir que la Carta de Derechos Fundamentales de la UE proclama como valor fundamental la igualdad y reconoce la no discriminación por razón de sexo (art. 21) así como la igualdad entre mujeres y hombres (art. 23). Por su parte, el Convenio de Estambul, ratificado por España, en su art.4, condena "todas las formas de discriminación contra las mujeres" de manera que el Estado "tomará, sin demora, las medidas legislativas y de otro tipo para prevenirla, en particular: indicando en sus constituciones nacionales o en cualquier otro texto legislativo adecuado el principio de la igualdad entre mujeres y hombres, garantizando la aplicación efectiva del mencionado principio; prohibiendo la discriminación contra las mujeres, recurriendo incluso, en su caso, a sanciones; derogando todas las leyes y prácticas que discriminan a la mujer".

5 Puede definirse la perspectiva de género como un mecanismo o metodología que permite identificar, cuestionar y valorar la discriminación y la desigualdad en el trato entre hombres y mujeres en aras a implementar acciones positivas con el ánimo de avanzar y alcanzar la tan anhelada igualdad material. *Guía de actuación con perspectiva de género en la investigación y enjuiciamiento de los delitos de violencia de género*, Unidad de coordinación de violencia sobre la mujer de la FGE, diciembre 2020.

6 BOE núm. 71, de 23.03.2007.

7 Barona Vilar, S.: "La necesaria deconstrucción del modelo patriarcal de justicia", en AA.VV.: *Análisis de la Justicia desde la perspectiva de género*, Tirant Lo Blanch, Valencia, 2018, p. 32.

8 En esta línea, el Comité consultivo para la igualdad de oportunidades entre mujeres y hombres de la Comisión Europea ha elaborado un Dictamen sobre la IA que analiza, entre otras cuestiones, las repercusiones de esta última en la igualdad de género (*AI – opportunities and challenges for gender equality*,

entre la perspectiva de género, la inteligencia artificial y la Justicia, todavía está en ciernes[9], por lo que deviene imperativo adoptar medidas y precauciones para prevenir un impacto indeseado sobre los derechos fundamentales, especialmente sobre los derechos a la no discriminación e igualdad.

Al respecto se pronuncia la Ley 15/2022, de 12 de julio, integral para la igualdad de trato y la no discriminación, que contiene la primera regulación positiva en nuestro ordenamiento del empleo de la IA por las Administraciones Públicas[10]. Esta norma, que nace con el objetivo de garantizar y promover el derecho a la igualdad de trato y no discriminación, recoge medidas destinadas a prevenir, eliminar, y corregir toda forma de discriminación, directa o indirecta, en los sectores público y privado (art.1.1). Concretamente en lo que a la IA se refiere, su artículo 23 dispone que "en el marco de la Estrategia Nacional de Inteligencia Artificial, de la Carta de Derechos Digitales y de las iniciativas europeas en torno a la Inteligencia Artificial, las administraciones públicas favorecerán la puesta en marcha de mecanismos para que los algoritmos involucrados en la toma de decisiones que se utilicen en las administraciones públicas tengan en cuenta criterios de minimización de sesgos, transparencia y rendición de cuentas, siempre que sea factible técnicamente. En estos mecanismos se incluirán su diseño y datos de entrenamiento, y abordarán su potencial impacto discriminatorio. Para lograr este fin, se promoverá la realización de evaluaciones de impacto que determinen el posible sesgo discriminatorio".

Hasta el momento la regulación de la IA, tanto nacional como europea, ha sido de *soft law*, es decir, se ha limitado a Comunicaciones, Informes y Cartas u otros documentos. Destáquese, en nuestro país, la Carta de Derechos digitales adoptada el 14 de julio de 2021, que contempla el derecho a la igualdad y a la no discriminación en el entorno digital. En particular, fomenta que los procesos de transformación digital apliquen la perspectiva de género y adopten, en su caso, medidas específicas para garantizar la ausencia de sesgos de género en los datos y algoritmos usados (VIII)[11].

2020). Por su parte, la Estrategia de la Unión Europea para la igualdad de género 2020-2024 también hace referencia al vínculo entre la IA y la igualdad de género (Comunicación de la comisión al Parlamento Europeo, al Consejo, al Comité Económico y social europeo y al Comité de las Regiones. Una Unión de la igualdad: Estrategia para la Igualdad de Género 2020-2025, Bruselas, 5.3.2020, COM (2020) 152 final) y la Red europea de organismos para la igualdad (Equinet) ha publicado el informe "Regulating for European AI that Protects and Advances Equality. An Equinet Position Paper", 22/06/2022.

9 En sentido similar, pero con referencia al Derecho privado, se pronuncia Navas Navarro, S.: "La perspectiva de género en la inteligencia artificial", *Diario La Ley*, núm. 48, sección Ciberderecho, 8 de marzo de 2021, p. 1.

10 BOE núm. 167, de 13.07.2022.

11 Un estudio detallado de la misma puede verse en Catalán Chamorro, M.J.: "La carta de derechos digitales y su implicación en el derecho procesal español", en AA. VV.: *Digitalización de la justicia: prevención, investigación y enjuiciamiento* (dir. por M. Llorente Sánchez-Arjona y S. Calaza López), Aranzadi, Cizur Menor, 2022, pp. 179 - 208. Véase también de esta autora: L*a justicia digital en España. Retos y desafíos*, Tirant Lo Blanch, Valencia, 2023.

En Europa, tras diversas normas de *soft law* (Carta ética europea sobre el uso de la inteligencia artificial en los sistemas judiciales y su entorno de 2018[12], Directrices éticas para una IA fiable de 2019[13] y Libro Blanco de la Inteligencia Artificial de la Comisión de 2020[14], entre las más destacadas), finalmente ha llegado el Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (ley de inteligencia artificial) y se modifican determinados actos legislativos de la Unión, cuyo objeto principal reside en impulsar la innovación a partir de normas que promuevan la confianza en las tecnologías[15]. En el mismo se clasifican los sistemas de IA en cuatro categorías atendiendo al riesgo potencial que implica su uso: prohibidos, alto riesgo, riesgo medio/bajo y resto de sistemas. En particular, a fin de evitar el riesgo de posibles sesgos, errores y opacidades, procede a considerar de alto riesgo aquellos sistemas de IA destinados a ser utilizados por una autoridad judicial o en su nombre para ayudar a las autoridades judiciales a investigar e interpretar los hechos y el Derecho y a aplicar la ley a unos hechos concretos (Considerando 61 y Anexo III punto 8.)[16]. A los sistemas de alto riesgo, a los que se dedica la mayor parte del articulado de la norma, se les exige el cumplimiento de toda una serie de requisitos y obligaciones específicas previstas en los capítulos 2 y 3.

Para finalizar la introducción de este trabajo, quisiera resaltar la labor llevada a cabo por la UNESCO en esta materia. Especialmente su Recomendación sobre la

12 Aprobada por la Comisión europea para la eficacia de la justicia (CEPEJ) el 4 de diciembre de 2018.

13 Elaboradas por un Grupo de expertos de alto nivel sobre IA, por encargo de la Comisión Europea, el 8 de abril de 2019. Entre los entre los siete requisitos que establece para una IA fiable, incluye la diversidad, la no discriminación y la equidad.

14 Libro Blanco sobre la IA -un enfoque europeo orientado a la excelencia y la confianza de 19 de febrero 2020 (COM (2020) 65 final).

15 Resolución legislativa del Parlamento Europeo, de 13 de marzo de 2024, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión (P9_TA(2024)0138). El Reglamento complementa el Derecho de la Unión vigente en materia de no discriminación al establecer requisitos específicos que tienen por objeto reducir al mínimo el riesgo de discriminación algorítmica, en particular en lo tocante al diseño y la calidad de los conjuntos de datos empleados para desarrollar sistemas de IA, los cuales van acompañados de obligaciones referentes a la realización de pruebas, la gestión de riesgos, la documentación y la vigilancia humana durante todo el ciclo de vida de tales sistemas (EM, 1.2)

16 No obstante, dicha clasificación no debe hacerse extensiva a los sistemas de IA destinados a actividades administrativas meramente accesorias que no afectan a la administración de justicia en casos concretos, como la anonimización o seudonimización de las resoluciones judiciales, documentos o datos; la comunicación entre los miembros del personal o las tareas administrativas. En tal sentido, el art. 6.3 manifiesta que, no obstante, un sistema de IA no se considerará de alto riesgo si no plantea un riesgo importante de causar un perjuicio a la salud, la seguridad o los derechos fundamentales de las personas físicas, en particular al no influir sustancialmente en el resultado de la toma de decisiones. Así será cuando se cumplan una o varias de las condiciones siguientes: a) que el sistema de IA tenga por objeto llevar a cabo una tarea de procedimiento limitada; b) que el sistema de IA tenga por objeto mejorar el resultado de una actividad humana previamente realizada; c) que el sistema de IA tenga por objeto detectar patrones de toma de decisiones o desviaciones con respecto a patrones de toma de decisiones anteriores y no esté destinado a sustituir la evaluación humana previamente realizada sin una revisión humana adecuada, ni a influir en ella; o d) que el sistema de IA tenga por objeto llevar a cabo una tarea preparatoria para una evaluación pertinente a efectos de los casos de uso enumerados en el anexo III. Los sistemas de IA siempre se considerarán de alto riesgo cuando lleven a cabo la elaboración de perfiles de personas físicas.

ética de la inteligencia artificial de 23 de noviembre de 2021[17], en cuyo ámbito de actuación número 6, que versa sobre género, insta a los Estados para que velen por que se optimice plenamente el potencial de las tecnologías digitales y la IA para contribuir a lograr la igualdad de género, así como por que los estereotipos de género y los sesgos discriminatorios no se trasladen a los sistemas de IA, sino que se detecten y corrijan de manera proactiva (puntos 89 y 90)[18].

Siendo este el estado de la cuestión, pasamos a analizar en el siguiente apartado algunas de las amenazas que acechan los sistemas de IA.

II. AMENAZAS: REFUERZO DE ESTEREOTIPOS Y NUEVAS FORMAS DE VIOLENCIA CONTRA LAS MUJERES.

Entre las diversas amenazadas asociadas al uso de IA en el ámbito de la Justicia, queremos destacar dos. En primer lugar, advertimos del riesgo de que las herramientas algorítmicas empleadas en los Juzgados puedan contener sesgos que reproduzcan estereotipos que perjudiquen a las mujeres. En segundo lugar, nos referimos a las nuevas formas de violencia que pueden ejercerse a través de la IA, particularmente a los "deepfakes" y a su posible incorporación en el acervo probatorio de un proceso judicial.

1. Los sesgos algorítmicos de género. Ejemplos en el marco de un proceso judicial.

Uno de los principales desafíos vinculados al uso de sistemas de IA en la Justicia reside en la posibilidad de que se generen situaciones discriminatorias que puedan comprometer el principio de igualdad.

Es ya un lugar común admitir que los sesgos algorítmicos reproducen los sesgos humanos[19]. En este sentido, requieren especial atención los sesgos algorítmicos de género que encontramos cuando un sistema informático propone o adopta

17 Disponible en: https://unesdoc.unesco.org/ark:/48223/pf0000380455_spa

18 Véase asimismo su informe "Artificial intelligence and gender equality" de 2020, en el que propone que la igualdad de género se constituya en un principio autónomo dentro del elenco de principios éticos de la IA (p. 16) y "I'd Blush if I Could: closing gender divides in digital skills through education" de 2019 ("Me sonrojaría si pudiera: cerrando brechas de género en la esfera digital a través de la educación"; título que proviene de la respuesta proporcionada por Siri al insulto "eres una puta"), en el que aborda el potencial de los sesgos algorítmicos de propagar y reforzar estereotipos de género. Ambos informes se encuentran disponibles en https://unesdoc.unesco.org/ark:/48223/pf0000374174 y https://unesdo c.unesco.org/ark:/48223/pf0000367416.page=1. Otra iniciativa a destacar, en este caso privada, ha sido la llevada a cabo por Amnistía Internacional, Access Now y otras organizaciones en 2018 reflejada en la Declaración de Toronto sobre la protección del derecho a la igualdad y la no discriminación en los sistemas de aprendizaje automático.

19 Un refrán muy conocido entre los informáticos "Garbage in, garbage out" (si entra basura, sale basura), transmite la idea de que cualquier resultado algorítmico discriminatorio procede de prejuicios inyectados en los algoritmos por seres humanos. En otras palabras, y tal y como lo replantea Mayson, "Bias in, bias out". Mayson, S. G.: "Bias In, Bias Out", *Yale Law Journal*, 2018, núm. 128, pp. 2218- 2300.

decisiones erradas que reproducen estereotipos de género[20]. Se entrelazan así, los algoritmos por un lado y, por otro, los estereotipos de género[21]. Estos últimos se definen como percepciones generalizadas o prejuicios acerca de los atributos o características que se supone que hombres y mujeres poseen, o deberían poseer, así como las funciones sociales que se espera que desempeñen[22].

Son tres, principalmente, las etapas clave en las que se pueden introducir los sesgos en los sistemas de IA: (i) cuando se decide el objetivo a alcanzar por el sistema; (ii) cuando se recopilan los datos (que son poco representativos[23] o reflejan prejuicios existentes en la realidad social) y (iii) cuando se seleccionan los atributos que se quiere que tenga en cuenta el algoritmo[24]. Aunque en ciertas situaciones los sesgos algorítmicos responden a un objetivo claramente discriminatorio (discriminación directa), en la mayoría de casos simplemente son provocados por el desinterés hacia su impacto colateral[25].

Si los sistemas de IA no se diseñan y desarrollan desde una perspectiva de género que sea capaz de detectar, analizar y corregir los sesgos, estos no solo serán susceptibles de ser replicados sino incluso acrecentados y reforzados. Sus efectos podrán ser infinitamente más rápidos y devastadores[26], lo que resulta especialmente preocupante si se augura que en un futuro cercano los jueces van a auxiliarse cada vez más de este tipo de herramientas.

Existen numerosos ejemplos de discriminación algorítmica hacia las mujeres, como el caso del chatbot "Tay.AI" de Microsoft, los créditos bancarios de Apple

20 Danesi, C.: "Sesgos algorítmicos de género con identidad iberoamericana: las técnicas de reconocimiento facial en la mira", *Revista Derecho de Familia*, 2021, núm.100, p. 161.

21 El Índice de Normas Sociales de Género (GSNI, por sus siglas en inglés) revela la falta de avances en la superación de los prejuicios contra las mujeres en la última década, ya que aproximadamente 9 de cada 10 hombres y mujeres en el mundo siguen manteniendo en la actualidad un sesgo contra las mujeres. "Una década de estancamiento: el PNUD presenta nuevos datos que muestran la persistencia de los sesgos de género", Comunicado de prensa, Programa de las naciones unidas para el desarrollo, Nueva York, 12 de mayo de 2023, disponible en file:///C:/Users/Admin/Documents/gsni_2023_pr_sp.pdf

22 Belloso Martin, N.: "La problemática de los sesgos algorítmicos (con especial referencia a los de género) ¿Hacia un derecho a la protección contra los sesgos?", en AA.VV.: *Inteligencia artificial y filosofía del derecho* (dir. por F. llano Alonso), Laborum, Murcia, 2022, p. 55.

23 Los algoritmos necesitan entrenarse con una gran cantidad de datos y, además, deben ser de calidad, esto es, representativos de toda la población. De lo contrario, se pueden producir situaciones en las que el sesgo de la muestra de entrenamiento se incorpora como un criterio que se ha de cumplir, lo que dificulta que se avance en la igualdad de oportunidades. Fernández, A., "Inteligencia artificial en los servicios financieros", *Boletín económico - Banco de España*, 2019, núm. 2, p. 5.

24 Ei, D., y Moser, G.: "Human arbitrators (the undisputed champion) v (the robots challenger)", *Hong Kong L.J*, 2020, vol. 50, p. 239. Hao, K., "This Is How AI Bias Really Happens - and Why It's So Hard to Fix", MIT *Technology* Review, 4 febrero 2019, disponible en: https://www.technologyreview.com/s/612876/this-ishow-ai-bias-really-happensand-why-its-so-hard-to-fix/

25 Rivas Vallejo, P.: "Sesgos de género en el uso de inteligencia artificial para la gestión de las relaciones laborales: análisis desde el derecho antidiscriminatorio", *e-Revista Internacional de la Protección Social(e-RIPS)*, 2022, vol. VII, núm. 1, p. 54.

26 O'Neil manifiesta que es crucial entender que, bajo la apariencia de neutralidad de los algoritmos, hay decisiones morales que perpetúan y aumentan las desigualdades sociales. Por eso los denomina "armas de destrucción matemática". *Armas de destrucción matemática*, Capitán Swing, Madrid, 2017.

Card, el reclutador inteligente de Amazon o los motores de búsqueda de Google, entre otros[27]. Excede de nuestro trabajo profundizar en ellos. No obstante, si vamos a mostrar, a modo de hipótesis, algunos ejemplos que ilustran las nocivas consecuencias del empleo de herramientas algorítmicas sesgadas en el marco de un proceso judicial. Para ello, partiremos de la clasificación, previamente mencionada, de las tres etapas clave en las que se pueden introducir los sesgos.

En primer lugar, los sesgos pueden incorporarse en un sistema de IA desde el momento en el que se establece el objetivo a alcanzar. Trasladado al marco de un proceso penal, imaginemos una herramienta que se diseña con el único fin de detectar y, consiguientemente, perseguir denuncias falsas presentadas por víctimas de violencia de género. La decisión de crear un instrumento específico para este propósito, asumiendo que estas denuncias son tan frecuentes como las denuncias falsas por robo (para las cuales ya se ha desarrollado una herramienta[28]), revela una percepción errónea de que las denuncias por violencia de genero son más propensas a ser falsas. Este prejuicio podría acarrear repercusiones devastadoras para las víctimas de tales delitos, perpetuar la desconfianza hacia ellas y contribuir a un entorno que desaliente la presentación de denuncias legítimas.

En segundo lugar, las herramientas de IA pueden introducir sesgos que estén presentes en las bases de datos de las que se nutren, bien porque se recopilan datos que son poco representativos bien porque reflejan prejuicios existentes en la realidad o tejido social. Probablemente este sea el supuesto más común en la práctica.

Los softwares de reconocimiento facial son un buen ejemplo de cómo este tipo de herramientas pueden tener consecuencias perjudiciales en la justicia penal. De hecho, se alerta constantemente acerca de su potencial discriminatorio, dado que muchos de estos sistemas se entrenan con conjuntos de datos que están sesgados en términos de representación. Fundamentalmente porque sobrerepresentan a hombres caucásicos e infrarrepresentan a mujeres. El resultado que ofrecen, por consiguiente, puede ser un reconocimiento facial menos preciso y más propenso a cometer errores cuando se aplica a mujeres de piel oscura. Este sesgo en los datos de entrenamiento puede llevar a disparidades en el trato, ya que las personas

27 Nos remitimos a los brillantes trabajos de Soriano Arnanz, A.: "Discriminación algorítmica: garantías y protección jurídica", en AA.VV.: *Derechos y garantías ante la inteligencia artificial y las decisiones automatizadas* (dir. por L. Cotino Hueso), Aranzadi, 2022, pp. 139-169 y "Creating non-discriminatory Artificial Intelligence systems: balancing the tensions between code granularity and the general nature of legal rules", *Revista de Internet, Derecho y Política*, 2023, núm. 38.

28 Nos referimos a Veripol, herramienta utilizada por la policía en nuestro país que estima la probabilidad de que una denuncia por robo con violencia e intimidación sea falsa. El sistema identifica el delito basándose en el texto de la denuncia. Utiliza el procesamiento del lenguaje natural y la IA para analizar y calcular las combinaciones de palabras más comunes cuando se miente ante un policía.

pertenecientes a los grupos infrarrepresentados pueden enfrentarse a tasas más altas de falsas identificaciones[29].

Por otro lado, los datos contenidos en las bases que alimentan el sistema de IA también pueden reflejar prejuicios existentes en nuestra sociedad. Pensemos, de nuevo, un ejemplo que podría darse en un proceso judicial. El juez se auxilia de una herramienta de IA para resolver el caso que le proporciona argumentos a favor y en contra. La herramienta, que se nutre de un repertorio de sentencias previas que han resuelto casos de agresiones sexuales, podría aprender y replicar los prejuicios y estereotipos contenidos en las mismas sobre el comportamiento que se espera de una víctima (resistirse de determinada manera, denunciar inmediatamente o mantenerse alejada de la vida social). Esto podría llevar al dictado de una resolución que resuelva que la violencia no ha existido, además de reflejar juicios sesgados y discriminatorios que contribuyen a la perpetuación de desigualdades en el sistema judicial[30]. Ello inevitablemente podría comportar consecuencias perjudiciales para las mujeres que intervienen en los procesos judiciales, así como favorecer automáticamente la desconfianza hacia sus declaraciones.

En tercer y último lugar, los sesgos también pueden provenir del modo en que se entrena al algoritmo, a la hora de seleccionar los atributos que deben tenerse en cuenta.

Veamos el ejemplo ficticio planteado por MARTÍNEZ, BORGES y SIMÓ. Se crea un software para ayudar al juez a valorar la declaración de la víctima y ese algoritmo ha sido entrenado bajo el criterio de que la tardanza en denunciar es relevante para valorar su credibilidad, fruto de un estereotipo humano vigente en los tribunales. Ante un supuesto en el que la víctima denunciara los hechos inmediatamente después de que ocurrieran, su nivel de credibilidad sería alto. Sin embargo, si la víctima tardara meses en denunciar, el algoritmo le reportaría al juez un grado de credibilidad mínimo. Estaríamos rotundamente ante un supuesto

29 Vid. European Union Agency for fundamental rights, *Facial recognition technology: fundamental rights considerations in the context of law enforcement,* 2020 y European Parliamentary Research Service, *Regulating facial recognition in the EU*, septiembre 2021, Bruselas.

30 Como señala GIL, existe el pensamiento generalizado de que una víctima que no cuenta desde el principio que sufrió abuso o agresión sexual, y lo cuenta después, no está diciendo la verdad; o que la víctima se pierda o desordene fechas o momentos en que suceden los hechos denota que tampoco dice la verdad: o que recuerde con mayor nitidez unos u otros momentos implica un testimonio poco fiable; o que no haya precisado atención psiquiátrica indica que quizá lo que relata no ocurrió; o que una víctima que efectúa su relato con entereza y sin llorar o con buena apariencia física, ya parece que no es víctima. Estos prejuicios son los que planea sobre los testimonios de las víctimas. Son una muestra de los estereotipos que existen y persisten en nuestra sociedad, y en el ámbito concreto de la justicia; además denota las enormes carencias que hay en la formación de los operadores jurídicos. Es no entender como un acto violento de estas características produce bloqueo en las víctimas, sentimientos de vergüenza o de culpabilidad. "La perspectiva de la mujer víctima del sistema judicial ajeno al género", en AA.VV.: *Análisis de la Justicia desde la perspectiva de género*, Tirant Lo Blanch, Valencia, 2018, pp. 238 y 239.

de discriminación algorítmica[31]. Lo mismo ocurría si se entrena al algoritmo pautándole que si la víctima no recuerda los detalles, no quiere declarar o quiere retirar la denuncia contra su pareja, entonces debe entenderse que es falsa[32].

Un último ejemplo podríamos hallarlo en las herramientas algorítmicas de evaluación de riesgos que, al entrenarse con datos históricos, reflejan y perpetúan estereotipos de género existentes en los casos anteriores de los que se nutre. Supongamos que, en el pasado, las denuncias de ciertos tipos de violencia contra las mujeres fueron consideradas de menor gravedad. Si el algoritmo se entrena con esos datos, podría aprender patrones sesgados y asignar automáticamente menores niveles de riesgo a casos similares en el futuro, lo que podría afectar negativamente a la atención y recursos asignados a las víctimas.

Vistos estos ejemplos, no podemos sino concluir que hay que esforzarse por procurar que no se reproduzcan sesgos históricos de género con herramientas algorítmicas empleadas en el marco de la Justicia. La tecnología no puede convertirse en un vehículo que facilite la vulneración de los derechos que principian el proceso, concretamente, el de igualdad. El riesgo de que estos instrumentos puedan discriminar resulta inaceptable. No olvidemos que estamos ante sistemas de alto riesgo dado que se destinan a auxiliar a los jueces, por lo que pueden tener efectos importantes sobre los derechos fundamentales, entre otros, el derecho a la tutela judicial efectiva y a un juez imparcial. De manera que resulta crucial trabajar para mejorar la detección de los sesgos algorítmicos y poner en marcha las medidas necesarias para neutralizarlos. Esto implica la adopción de medidas tanto de índole política como jurídica y tecnológica[33].

En este contexto, resulta imprescindible que los algoritmos sean auditados y controlados tanto de manera previa a su puesta en marcha como de forma periódica. Para ello, los programas, en la medida de lo posible, tendrán que ser

31 Martínez García, E.; Borges Blázquez, R., y Simó Soler, E.: "Inteligencia artificial y perspectiva de género en la justicia penal", *Diario* La *Ley*, Sección Ciberderecho, 20 de enero de 2021, núm. 47, p. 6. No olvidemos que el propio Tribunal Supremo ha declarado en su sentencia 184/2019, de 2 de abril (ES:TS:2019:1071) que la credibilidad de la víctima no debe ser menoscabada por el hecho de retrasar la denuncia.

32 En lugar de pensar en las dudas que puedan tener las mujeres por las posibles consecuencias que afectarían al "padre de sus hijos", o los miedos por las presiones y amenazas de los entornos. Lorente Acosta, M.: "Justicia, género y estereotipos", en AA.VV.: *Análisis de la Justicia desde la perspectiva de género*, Tirant Lo Blanch, Valencia, 2018, p.154.

33 Belloso Martin, N.: "La problemática", cit., p. 69.
Se propone la incorporación de una mayor presencia femenina en los equipos que diseñan estas herramientas. Además, que se trate de equipos formados capaces de introducir la perspectiva de género desde el diseño (*gender-by-design*) del propio sistema de IA. "La perspectiva de género en la inteligencia artificial", cit., p. 10. Como señalan, Ortiz De Zárate y Guevara, la diversidad en los equipos puede ofrecer nuevas perspectivas y traer a colación experiencias que permitan reconocer los sesgos y trabajar para corregirlos. *Inteligencia artificial e igualdad de género. Un análisis comparado entre la UE, Suecia y España*, Fundación alternativas, 2021, núm. 101, p. 24. En esta línea, la nueva Agenda España Digital 2026 en su noveno eje, referido a las competencias digitales, prevé que el reto para 2026 sea reforzar las competencias digitales de la ciudadanía, reduciendo las brechas digitales, consiguiendo una paridad de género en los especialistas digitales.

trasparentes y explicables. Solo así se podrá mitigar el problema de los sesgos, en tanto en cuanto se permitirá, a *priori*, su corrección y perfeccionamiento[34].

2. *Deepfakes:* violencia basada en el género con empleo de IA.

La manipulación de imágenes, audios o vídeos no es un fenómeno novedoso. Sí lo es su ejecución mediante técnicas de IA que implican un mayor grado de sofisticación y producen resultados que se asemejan mucho más a la realidad, hasta el punto de dificultar considerablemente el discernimiento entre la autenticidad y la falsedad de los contenidos generados.

A través de redes generativas adversariales (*generative adversarial networks* o GAN por sus siglas en inglés) pueden crearse falsos contenidos audiovisuales hiperrealistas que dan lugar a los denominados *deepfakes*. Este término, en inglés, deriva de la combinación de las palabras "fake" (falsificación) y "deep learning" (aprendizaje profundo)[35]. Los *deepfakes* ganaron notoriedad a finales de 2017, cuando un usuario anónimo de la plataforma Reddit (conocido con el alias "deepfake") compartió videos pornográficos falsos que superponían los rostros de celebridades como Taylor Swift o Scarlett Johansson, en cuerpos de mujeres desnudas. A pesar de la pronta eliminación de estos videos, esta técnica de manipulación se ha propagado rápidamente por Internet, lo que se ha debido en gran medida a que la creación de este tipo de material falso está al alcance de cualquiera, dado que existen aplicaciones gratuitas cada vez más populares que facilitan la edición de contenidos de manera relativamente sencilla.

Los *deepfakes* tienen múltiples usos. Algunos son legítimos. Por ejemplo, en el ámbito de la publicidad se pueden crear campañas más impactantes y personalizadas; en el de la educación se puede generar material didáctico interactivo; en el cine se pueden realizar efectos especiales más realistas y en medicina se pueden simular escenarios clínicos para propósitos de formación. Sin embargo, al mismo tiempo los *deepfakes* ostentan un enorme potencial para ejercer una variedad de fines maliciosos e incluso delictivos, que incluyen, entre otros, difusión de noticias falsas, atribución a políticos (caso de Obama) o empresarios (caso de Zuckerberg) de

34 Macchiavelli, N.: "La violencia de género y el uso de algoritmos como herramienta efectiva para la protección de los derechos fundamentales", *AFD*, 2022 (XXXVIII), p. 64.

35 La tecnología utilizada para generar estos contenidos depende de distintos tipos de falsificaciones digitales que, en términos generales, pueden clasificarse de la siguiente manera: a) Sustitución de caras: intercambio de la cara de una persona, fusionándola con la de otra; b) Reinterpretación facial: manipulación de los rasgos faciales de un sujeto para parecer que está diciendo algo que en realidad no es así; d) Generación de rostros: creación de imágenes sintéticas convincentes y ficticias de personas; e) Síntesis de voz: generación de contenido de audio mediante el uso y entrenamiento de algoritmos para crear una voz falsa o un archivo de audio sintético y, f) Shallowfakes: falsificaciones audiovisuales menos sofisticadas creadas mediante técnicas de edición rudimentarias. T Trend Micro Research, United Nations Interregional Crime and Justice Research Institute (UNICRI) Europol's European Cybercrime Centre (EC3), "Malicious Uses and Abuses of Artificial Intelligence", 2020, pp. 53 y 54. Disponible en: file:///C:/Users/Admin/OneDrive%20-%20Universitat%20de%20Valencia/vid.%20pp.%2053%20y%2054.pdf.

declaraciones que nunca realizaron, destrucción de la imagen y credibilidad de una persona, acoso o humillación en línea, perpetración de extorsiones y fraudes, distribución de desinformación y manipulación de la opinión pública, chantajes, desbloqueo de dispositivos, suplantaciones de identidad para estafas, falsificación o manipulación de pruebas en procesos judiciales, etc[36]. De entre todos ellos, la producción de pornografía, especialmente en los casos de "pornovenganza" (*revenge porn*), se erige como su principal manifestación[37]. Recuérdese en este sentido, lo sucedido en Almendralejo (Badajoz), donde decenas de chicas adolescentes han sido víctimas de estos 'desnudos', que han circulado rápidamente entre los móviles de sus compañeros[38].

Consciente de estos peligros, el Reglamento de IA ha tomado – aunque muy prudentemente- cartas en el asunto. A pesar de no prohibir esta tecnología, sí que impone ciertos requisitos mínimos, especialmente en lo que se refiere a obligaciones de transparencia. De este modo, los creadores de *deepfakes* deben hacer público que el contenido se ha generado de forma artificial o ha sido manipulado. Esta obligación no se aplicará cuando su uso esté autorizado por la ley para detectar, prevenir, investigar o enjuiciar infracciones penales (art. 50.2)[39].

Dicho esto, queremos hacer hincapié en que el empleo de las tecnologías se está convirtiendo en un componente cada vez más habitual en la violencia contra las mujeres[40]. En este sentido, el surgimiento de la IA ha dado lugar a nuevos modos de violencia con el mismo propósito de control y dominación[41]. Como ocurre

36 Trend Micro Research, "Malicious Uses", cit., p. 52.

37 Excede del objeto de este trabajo analizar la calificación jurídico-penal que merecen estas conductas. Nos remitimos a las reflexiones de Bello San Juan, P.: "La inteligencia artificial al servicio del crimen: La revolución del deepfake desde una perspectiva criminológica", en AAV.: *La justicia en la sociedad 4.0: nuevos retos para el siglo XXI* (dir. por L. Fontestad Portalés), Colex, 2023, p. 239. Si queremos mencionar que la recientemente aprobada Directiva sobre la lucha contra la violencia contra las mujeres y la violencia doméstica de 14 de mayo de 2024 (DOUE: 2024/1385), expresamente se refiere a los *deepfakes* que representan actividades sexuales e insta a los Estados a penalizar la producción, manipulación o divulgación no consentida del material manipulado.

38 Borraz, M. y Pastor, A.: "'Deepfakes sexuales: el caso de las menores de Almendralejo consolida una nueva forma de violencia machista", *el Diario.*es, 19 de septiembre de 2023.

39 Véase el Informe que con carácter previo emitió el Parlamento Europeo titulado "Tackling deepfakes in European Policy" de julio 2021. Véase asimismo en nuestro país la Proposición de Ley Orgánica de regulación de las simulaciones de imágenes y voces de personas generadas por medio de la inteligencia artificial, presentada por el Grupo parlamentario Plurinacional SUMAR. BOE núm. 23-1 de 13 de octubre de 2023.

40 Entre los comportamientos específicos que utilizan tecnología como medio para ejercer violencia contras las mujeres (ciber violencia), se incluye el ciberacoso, ciberhostigamiento, el sexting, el stalking, la publicación de contenido sexual en línea sin consentimiento, etc. Estas prácticas, sin lugar a dudas, afectan principalmente a las mujeres. Vid. Lloria García, P.: *Violencia sobre la mujer en el siglo XXI. Violencia de control y nuevas tecnologías: habitualidad, sexting y stalking*, Iustel, Madrid, 2020.

41 La tecnología incrementa el riesgo de violencia, especialmente de la violencia psicológica porque permite a los agresores crear "una sensación de omnipresencia" que erosiona la sensación de seguridad. La mayoría de estudios sobre violencia de género facilitada por la tecnología se centra en ciberriesgos "convencionales", como el abuso a través de redes sociales. Pero hay un área más nueva de la tecnología que merece también atención: el "Internet de las Cosas" o el "IoT", término que describe la red de dispositivos autónomos conectados a Internet que las personas pueden supervisar o controlar desde una ubicación remota. Estos dispositivos abarcan toda una serie de tecnologías como electrodomésticos

con los deepfakes, "el fenómeno de la violencia contra las mujeres no es nuevo, lo es el procedimiento a través del cual se procura su ejercicio'"[42]. Precisamente su propagación está estrechamente ligada a la elaboración y distribución de contenido pornográfico falso protagonizado por mujeres. La generación de este tipo de imágenes no deja de ser una herramienta y un atentado más que afecta directamente contra su imagen, dignidad e integridad. Además, tengamos presente que no solo se han visto afectadas celebridades, sino también mujeres anónimas cuyos exnovios o amantes han utilizado esta tecnología para vengarse de ellas y humillarlas en línea. Es, por tanto, un arma que puede ser muy peligrosa contra ellas para acosarlas, intimidarlas y degradarlas[43].

En este sentido, como señala Bello San Juan, resulta insoslayable el componente de género subyacente tras estas conductas, al ser principalmente mujeres las perjudicadas por este tipo de acciones con independencia de su condición social, económica o la posición que represente en la sociedad[44]. La abrumadora mayoría de víctimas de estos vídeos son mujeres[45]. Como muestra, la aplicación DeepNude permite desnudar artificialmente incorporando una foto de un rostro a un cuerpo

inteligentes (altavoces, frigoríficos, televisores), dispositivos personales (relojes, dispositivos médicos, coches), sistemas domésticos (termostatos, cámaras de seguridad, iluminación), asistentes domésticos (Alexa), etc. La creciente prevalencia de estos dispositivos "inteligentes" proporciona a los agresores una nueva y poderosa herramienta para ampliar y magnificar los daños tradicionales de la violencia doméstica. Permiten superar los límites geográficos y espaciales que de otro modo les impediría vigilar, controlar, acosar, aislar y amenazar a las víctimas. Nos podemos hacer una idea de la gravedad que puede alcanzar este asunto con los ejemplos expuestos por MADISON LO, de conductas que un maltratador podría llevar a cabo. Entre otras, el apagado a distancia de los aparatos de aire acondicionado, el cambio diario de las contraseñas digitales de la puerta principal, el timbre de la puerta sonando incesantemente, cambiar la temperatura de una vivienda a kilómetros de distancia, hervir un hervidor de agua para recordar que el maltratador está mirando, utilización de sensores que controlan las cerraduras inteligentes para restringir la capacidad para salir de casa, control del historial de búsqueda de los asistentes virtuales por voz para asegurarse de que no se busca ayuda, etc. LO, M.: "A Domestic Violence Dystopia: Abuse via the Internet of Things and Remedies Under Current Law", *California Law Review*, 2021, vol. 109, pp. 277- 315.

42 Simó Soler, E.: "Retos jurídicos derivados de la Inteligencia Artificial Generativa Deepfakes y violencia contra las mujeres como supuesto de hecho", *InDret*, febrero 2023, núm.2, p. 498.

43 Soto Santana, M.: "Justice for Women: Deep fakes and Revenge Porn", 3rd Global Conference on woman´s studies, 25-27 septiembre 2022, p. 113. Disponible en file:///C:/Users/Admin/OneDrive%20-%20Universitat%20de%20Valencia/Inteligencia%20artificial/Deepfakes/Justice%20for%20woman.pdf

44 Bello San Juan, P.: "La inteligencia artificial", cit., p. 244. Son una manifestación más de la cosificación de la mujer. Ellas protagonizan falsas escenas eróticas y pornográficas; ellos, discursos y circunstancias relacionados con el humor o con la política, apareciendo normalmente vestidos. Ellas asoman en espacios privados; ellos, en espacios públicos ostentando el poder o un protagonismo sano. Ellas son cosificadas y sus rostros se pegan al cuerpo de una actriz despersonificada. Ellos tienen otro cuerpo, pero no pierden su esencia personal ni son tratados como objetos porque lo llamativo es lo que dicen o hacen. Ellas son sujetos pasivos; ellos protagonistas activos. Cerdán Martínez, V. y Padilla Castillo, G.: "Historia del fake audiovisual: deepfake y la mujer en un imaginario falsificado y perverso", *Historia y comunicación social*, 2019, núm. 24 (2), pp. 505-520.

45 En un informe elaborado en el 2023 por Home Security Heroes, empresa especializada en ciberseguridad, se alcanzaron las siguientes conclusiones: el número total de vídeos deepfake en línea en 2023 fue de 95.820, lo que representa un aumento del 550% con respecto a 2019; La pornografía deepfake representa el 98 % de todos los deepfake en línea; El 99% de las personas a las que se dirige esta pornografía son mujeres; Una de cada tres herramientas de deepfake permite a los usuarios crear pornografía; Se tarda menos de 25 minutos y cuesta 0 dólares crear un vídeo pornográfico de 60 segundos con tan solo utilizar una imagen de la cara. "2023 State of Deepfakes. Realities, threats, and impact", disponible en: https://www.homesecurityheroes.com/state-of-deepfakes/#appendix

desnudo obtenido de una base de datos que únicamente contiene imágenes de mujeres.

En definitiva, los *deepfakes* sexuales no consentidos plantean un riesgo significativo porque los agresores pueden utilizarlos para amenazar, controlar, intimidar, aislar, avergonzar, chantajear y abusar de las víctimas que son, en su mayoría, mujeres[46]. Esto, trasladado al marco de un proceso judicial podría tener unos efectos claramente perniciosos. Como afirma Simó Soler, no sería descabellado pensar que los maltratadores puedan generar *deepfakes* para poner en duda la versión de las futuras denunciantes («Tengo la prueba de que hubo consentimiento»), destruir su imagen y credibilidad y forzar el desistimiento («¿Quién te va a creer si eres una buscona?»)[47].

Hasta el momento la doctrina se ha centrado en analizar cómo prevenir, mitigar y sancionar el uso malicioso de esta tecnología. Pero hay otro aspecto que no debe olvidarse: los *deepfakes* también van a llegar, de manera inevitable, a los juzgados. En tal caso, los contenidos audiovisuales falsos creados mediante GAN podrían socavar seriamente la integridad de los procesos judiciales de varias maneras. Entre otras, podrían ser presentados como pruebas, bien con la intención de engañar al juzgador, bien sin ser la parte que los aporta consciente de su falsedad. Podrían también viciar las declaraciones de los testigos en la medida en que se hayan visualizado o escuchado grabaciones manipuladas por estos sistemas, creyéndolas reales[48]. Es más, incluso en situaciones donde los contenidos no fueran falsos, la mera existencia de los *deepfakes* podría complicar seriamente la tarea de demostrar la veracidad de las pruebas. Es decir, la parte contraria podría argumentar que se trata de un video falso e impugnar la prueba con el fin de descartarla como evidencia o, al menos, sembrar la duda acerca de su autenticidad[49]. Todo ello va a conllevar cargas adicionales para los diferentes operadores jurídicos (abogados, jueces, fiscales, peritos, etc.), al tener que dedicar tiempo, dinero y esfuerzo en la detección y comprobación de falsificaciones cada vez más sofisticadas.

Dada la complejidad técnica inherente, son precisos conocimientos específicos que el juez no dispone, por lo que la respuesta más directa e inmediata a los *deepfakes* pasaría por la prueba pericial. Se plantea así, como vía para despejar

46 Kweilin, L.T.: "Deepfakes and domestic violence: perpetrating intimate partner abuse using video technology", *Victims & Offenders*, 2022, vol. 17, núm. 5, p. 648.

47 Simó Soler, E.: "Retos jurídicos", cit., p. 501.

48 Bello San Juan, P.: "La inteligencia artificial", cit., p. 238.

49 Este problema podría alcanzar proporciones especialmente graves cuando el sujeto afectado por el *deepfake* fuera una persona particularmente indefensa, o incapaz por sí mismo de reclamar justicia ante una prueba que no se corresponde con la realidad. Miguel Freita, P.: "Deepfakes, conteúdo gerado por inteligência artificial e verdade processual", en AA.VV.: *El proceso penal ante una nueva realidad tecnológica europea* (dir. por C. Arangüena Fanego, m. De Hoyos Sancho y E. Pillado González), Thomson Reuters Aranzadi, 2023, p. 204.

las dudas sobre la veracidad o falsedad de las pruebas que contienen imágenes, videos o audios, que se adjunte un informe pericial que acredite que, a la luz de los conocimientos tecnológicos actuales, no ha sido posible detectar indicios de que ese contenido sea parcial o totalmente artificial. Y ante la duda acerca de la parcialidad de dicho informe técnico, podría encomendarse dicha tarea a los peritos forenses oficiales designados por el juez, como ocurre con el resto de pruebas periciales[50].

En este sentido, se advierte acerca de "la necesidad de un peritaje judicial avanzado, sofisticado e hiperexperto, requiriendo incluso de la propia IA para detectar los vídeos falsos"[51]. Ahora bien, no consideramos que vaya a resultar imprescindible acudir siempre y en todo lugar a sofisticadas herramientas forenses para detectar las manipulaciones. Cuando los vídeos falsificados sean de mala calidad, la tarea no será tan difícil. Por otro lado, si demostrar la falsedad resulta demasiado complejo, será más fácil demostrar que el vídeo no ha sido manipulado, por ejemplo, adjuntando metadatos adicionales en el momento de grabar el vídeo, con el objetivo de dar fe de la autenticidad de la grabación del vídeo[52]. Además, no olvidemos que también podrá acudirse a otras pruebas, como, por ejemplo, a la testifical (llamar a quien tomó el video, a quien sale en él, a quien presenció la grabación, etc.) o al interrogatorio de la parte que ha presentado el video como prueba.

Teniendo en cuenta este escenario, y sin soslayar sus riesgos, no es, sin embargo, nuestra intención incurrir en un alarmismo desproporcionado. Es probable que nos enfrentemos a algunos de estos casos, pero no por ello vislumbramos la inminencia de una avalancha de falsificaciones profundas en los procesos judiciales (¡al menos no por el momento ¡). Y en el caso de que así fuera, aunque pudieran implicar un costo adicional, confiamos en que los tribunales afronten los desafíos que plantean, tal y como han hecho en el pasado con generaciones anteriores de falsificaciones, sin necesidad de modificar las reglas probatorias ni de imponer, con carácter general, normas más restrictivas para verificar la autenticidad de las pruebas[53].

50 Miguel Freita, P.: "Deepfakes, conteúdo", cit., p. 203

51 Simó Soler, E.: "Retos jurídicos", cit., p. 505.
Parece haber consenso en que el enfoque más eficaz para identificar estas representaciones sintéticas es emplear la misma tecnología utilizada para generar *deepfakes*, esto es, redes generativas adversarias.

52 Pfefferkorn, R.: "Deepfakes" in the Courtroom", *BU Pub. Int. LJ*, 2020, vol. 29, p. 268.

53 Pfefferkorn, R.: "Deepfakes" in the Courtroom", cit., p. 246. En sentido contrario se pronuncia Delfino, que considera que debe exigirse a los tribunales que adopten medidas adicionales para determinar la autenticidad de las imágenes antes de admitirlas como prueba. "Deepfakes on trial: a call to expand the trial judge's. Gatekeeping role to protect legal proceedings from technological fakery", *Hastings Law Journal*, 2023, vol. 74, núm. 2, p. 297.

III. IA AL SERVICIO DE LA LUCHA CONTRA LA VIOLENCIA HACIA LAS MUJERES.

A pesar de haber expuesto los riesgos de que se refuercen y perpetúen los sesgos, debe al mismo tiempo reconocerse que los sistemas de IA bien diseñados pueden ayudar a identificarlos y, por ende, a corregirlos[54]. En este sentido, la Carta ética europea sobre el uso de la IA en los sistemas judiciales y su entorno, hace referencia a su capacidad para revelar la discriminación existente. Por ello, no podemos desatender las virtudes y ventajas que la IA puede ofrecernos[55].

Como señalan XENIDIS y SENDEN, si bien los algoritmos aumentan los problemas de discriminación en algunos casos, también ofrecen la oportunidad de reducir la arbitrariedad mediante una mayor explicabilidad de los procedimientos de toma de decisiones. Mientras que las decisiones humanas podrían asimismo calificarse de "caja negra" por su naturaleza opaca y no reproducible, los algoritmos de aprendizaje automático ofrecen la posibilidad de una toma de decisiones más responsable, siempre que se cumplan ciertos requisitos de transparencia. Las decisiones humanas, a diferencia de las decisiones algorítmicas, no pueden reproducirse cambiando un factor para comprobar de dónde procede la discriminación. Por lo tanto, ciertos principios como la transparencia, la explicabilidad y la rendición de cuentas son fundamentales para desarrollar aplicaciones de IA si el objetivo es convertir los riesgos existentes de discriminación en una oportunidad para aumentar la igualdad[56].

Del mismo modo, aunque hemos visto que la IA ha facilitado el surgimiento de nuevos modos de violencia contra las mujeres, no podemos obviar la otra cara de la moneda. La IA también puede emplearse en la lucha contra el mayor exponente de la desigualdad, como es la violencia de género. Entre otras, con herramientas que ayuden a proteger a las víctimas, a investigar determinados delitos, así como a prevenir su ejecución mediante técnicas predictivas que estimen la probabilidad de reincidencia. Así las cosas, se entiende que la IA tiene un enorme valor para

54 Sunstein, C. R., "Algorithms, Correcting Biases", *Forthcoming, Social Research*, 12 diciembre 2018, disponible en SSRN: https://ssrn.com/abstract=3300171

55 Interesantes resultan al respecto las reflexiones vertidas por Simó Soler, que propone el uso de modelos de *machine learning* para la detección de estereotipos de género en las sentencias. *Estereotipos de género en procesos por violencia sexual,* Tirant lo Blanch, Valencia, 2023.

56 Senden Xenidis, R. y Senden, L.: "EU non-discrimination law in the era of artificial intelligence: Mapping the challenges of algorithmic discrimination", en AA.VV.: *General Principles of EU law and the EU Digital Order* (ed. por U. Bernitz *et al.*), Kluwer Law International, Países Bajos, 2020, p. 30. Señala al respecto Sanchis Crespo, La diferencia con los sesgos robóticos es que éstos se exteriorizan claramente —en tanto en cuanto el algoritmo sea transparente y esté bien evaluado— y desde esa perspectiva es más fácil mitigarlos. Los sesgos humanos pueden, sin embargo, pasar desapercibidos a menos que se muestren a las claras. "Inteligencia artificial y decisiones judiciales: crónica de una transformación anunciada", Scire: Representación y organización del conocimiento, 2023, vol. 29, núm. 2, p. 80.

mitigar ciertos aspectos de este tipo de violencia[57]. Veamos a continuación algunas de las bondades que puede brindarnos.

1. Tecnologías para atender a las víctimas. De la teleasistencia a la IA.

En los últimos años se han creado diversas herramientas "inteligentes" que pueden ser utilizadas para atender o auxiliar a las mujeres víctimas de violencia.

Ya en el año 2004 se puso en marcha Atenpro (Servicio Telefónico de Atención y Protección para víctimas de violencia contra las mujeres), un servicio de teleasistencia complementario al 016. Mediante el mismo se ofrece a las víctimas un dispositivo móvil a través del cual pueden recibir asistencia inmediata durante las 24 horas del día los 365 días del año. Atenpro, que se basa en la utilización de tecnologías de comunicación telefónica móvil, permite que las mujeres puedan entrar en contacto en cualquier momento con un Centro atendido por personal específicamente preparado para responder a sus necesidades, incluso en situaciones de riesgo con carácter de urgencia[58]. Durante muchos años este servicio apenas se ha modernizado. Sin embargo, recientemente se ha informado que va a incorporar IA para mejorar la protección de las usuarias y crear un sistema integral de seguimiento. Por un lado, los nuevos dispositivos se compondrán no solo de dispositivos móviles, sino también de relojes inteligentes y pulsadores que permiten a la policía la geolocalización de la víctima por GPS en caso de emergencia. Por otro lado, para mejorar su potencialidad, se pretende crear una aplicación informática dotada con IA que mejore la prevención y atención. Entre otras, la aplicación permitirá clasificar a las víctimas en función del nivel de riesgo, de forma que el personal de Atenpro contacte más con aquellas mujeres con mayor riesgo de ser agredidas[59]. Además de la protección a las víctimas de violencia de género, la actualización y modernización de este servicio, permitirá la atención a las víctimas de agresión sexual, acoso sexual y violencia sexual cometida en el ámbito digital, así como otras formas de violencia ejercida contra la mujer reconocidas en el Convenio de Estambul.

57 Macchiavelli, N.: Perspectiva de género en las nuevas tecnologías. El problema de los sesgos, *Diario Suplemento Derecho y Tecnología*, 2021, núm. 84, p. 9. Vid. asimismo Llorente Sánchez-Arjona, M.: "La inteligencia artificial como nueva estrategia de prevención en los delitos de violencia sexual", en AA.VV.: *Uso de la información y de los datos personales en los procesos: los cambios en la era digital* (dir. por I. Colomer Hernández), Aranzadi, 2022. La autora analiza el empleo de la IA en la lucha contra otras formas de violencia como la trata, pornografía infantil, agresores sexuales en serie, etc.

58 https://violenciagenero.igualdad.gob.es/informacionUtil/recursos/servicioTecnico/home.htm

59 El Gobierno ha ampliado el presupuesto estatal destinado al programa. En concreto, los fondos europeos Next Generation han consignado 32 millones para la modernización de Atenpro. En la puesta en marcha de la aplicación creada con IA está colaborando la Cátedra en Inteligencia Artificial de la Universidad de Alcalá. Martin, P., "España usará la IA y el 'big data' para proteger mejor a las víctimas del machismo", *Diario el Periódico*, 23 de septiembre de 2023, disponible en: https://www.elperiodico.com/es/sociedad/20230923/violencia-genero-machista-inteligencia-artificial-proteccion-big-data-victimas-92338576.

Aunque no se trata propiamente de un servicio de asistencia a las víctimas, queremos hacer mención a un interesante proyecto que, hasta donde alcanza nuestro conocimiento, todavía no se ha implantado. Nos referimos al Proyecto de investigación que recibe el nombre de "Certeza de Voz" del Instituto Andaluz de la Mujer (IAM), en colaboración con la Empresa Pública de Emergencias Sanitarias "EPES 061", dependiente de la Consejería de Salud y Familias. Se trata de un *software* inteligente creado para la detección precoz de supuestas víctimas de violencia de género mediante la voz de la mujer que llama a los Centros de Coordinación de Urgencias y Emergencias Sanitarias de Andalucía[60]. A través del mismo, se permitirá saber si la entonación, expresiones, uso de palabras, pausas o suspiros de la mujer que llama, muestra un patrón en las personas que sufren esta violencia. En tal caso, se generará una alerta de sospecha de un caso de violencia de género[61].

Fuera de España, destacamos PROTOBADI, creada en Bangladesh con el objetivo de proporcionar seguridad a las mujeres. Se trata de una aplicación para teléfonos inteligentes que crea mapas "calientes" que determinan las zonas con mayor probabilidad de producirse acoso sexual hacia las mujeres. Cuenta con un botón en la pantalla, que al ser presionado enciende una alarma muy ruidosa y a continuación, envía mensajes de texto a los contactos de la mujer indicando su ubicación y solicitando ayuda. Además, como hemos mencionado, permite recopilar los datos para configurar un mapa que señale las áreas más peligrosas, así como una especie de blog donde las usuarias pueden compartir sus experiencias[62]. Al igual que PROTOBADI, existen otras muchas aplicaciones destinadas a proteger a las mujeres en diversas partes del mundo, tales como: Eyewatch SOS for Women, SpotnSave Feel secure, iGoSafely, bSafe, Chilla, etc.[63]

Otras tecnologías que están utilizando IA para atender y ayudar a las víctimas de violencia de género son los chatbots. Entre otros, My*Sis Bot*, desarrollado en Tailandia, proporciona información, ayuda de emergencia, asistencia jurídica y acceso a diversos servicios (centros de llamadas sin ánimo de lucro, policía o juzgados de familia) a las mujeres que han sufrido violencia. La aplicación se descarga en el propio teléfono y permite a las usuarias mantener una conversación

60 Proyecto de investigación financiado con Fondos Feder, dentro del Pacto de Estado contra la Violencia de Género.

61 Constanza Gamboa, N., "La inteligencia artificial como herramienta al servicio de la erradicación de la Violencia de Género", Observatorio violencia, septiembre 2020, disponible en: https://observatorioviolencia.org/la-inteligencia-artificial-como-herramienta-al-servicio-de-la-erradicacion-de-la-violencia-de-genero/

62 El término Protobadi significa "alguien que protesta" en bengalí. Marks, P., "Bangladesh: Sex harassment app helps women map abuse", *NewScientist,* mayo 2014.

63 Vid. Gopika, B., "10 Safety Apps For Women", 12 junio 2018, BW Business World, disponible en https://www.businessworld.in/article/10-Safety-Apps-For-Women/12-06-2018-151793/

en tiempo real durante la cual reciben la asistencia que necesitan[64]. O el chatbot holandés elaborado por la Universidad de Maastricht que, con el fin de atender a las víctimas de acoso y agresión sexual, les permite contar su historia con libertad y ofrece a continuación consejos del lugar al que se debe acudir en función de cada caso (comisaría, hospital, psicólogo o refugio)[65]. Por su parte, en América Central se ha desarrollado el chatbot o asistente virtual inteligente Sara[66], diseñado con IA, que orienta a las mujeres sobre el riesgo de sufrir o haber sufrido violencia y proporciona información acerca de donde denunciar, los derechos que le asisten, etc[67].

En lo que a nuestro país respecta, se están desarrollando algunos proyectos, como el programa Improve (*Improving Access to Services for Victims of Domestic Violence by Accelerating Change in Frontline Responder Organisations*), financiado por la Unión Europea (*Horizon Europe*). Este robot conversacional multilingüe con IA, ofrecerá a las víctimas, si prefieren no acudir a una comisaría o llamar a la policía, asesoramiento inmediato, evaluación de riesgos además de orientarles sobre los servicios y recursos disponibles.

Son otras muchas las tecnologías que pueden proporcionar ayuda a las víctimas de violencia de género y que se están desarrollando en todo el mundo. Desde herramientas que analizan imágenes de vídeo para detectar comportamientos agresivos o violentos hacia las mujeres hasta análisis de llamadas de emergencia realizadas por mujeres con base en el tono de su voz y el lenguaje utilizado o identificación de publicaciones en redes sociales que contengan contenido de acoso[68].

2. Sistemas de IA en el marco de la investigación.

La IA puede resultar extremadamente útil en la investigación criminal, especialmente por lo que respecta a la mejora de los métodos de trabajo de las autoridades policiales. Como bien sabemos, aunque la instrucción sea dirigida por los jueces, son ellas quienes se encargan en realidad de llevarla a cabo.

64 "Using AI in accessing justice for survivors of violence", 30 mayo 2019, disponible en: https://www.unwomen.org/en/news/stories/2019/5/feature-using-ai-in-accessing-justice-for-survivors-of-violence.

65 https://eldiariofeminista.info/2019/10/11/chatbot-para-victimas-de-acoso-sexual/

66 https://chatbotsara.org/

67 Desarrollado por el Proyecto Regional Infosegura, iniciativa del Programa de las Naciones Unidas para el Desarrollo en colaboración con la Agencia de los EEUU para el Desarrollo Internacional.

68 Ejemplo paradigmático es el de Suecia, que ostenta el índice de igualdad de género más alto de la Unión Europea, que ha adoptado diversas iniciativas para usar tecnologías disruptivas de una forma proactiva a favor de la igualdad de género. Véase el informe presentado por Ortiz De Zárate Alcarazo, l. y Guevara Gómez. A.: "Inteligencia artificial", cit., p. 49.

Es evidente que la investigación penal está experimentando una transformación[69]. Las diligencias de investigación tecnológicas, recogidas en nuestra LECrim desde la reforma operada por la Ley 13/2015, han incorporado, en mayor o menor medida, sistemas de IA para el esclarecimiento y descubrimiento de los delitos[70]. Así, la policía empieza a emplear tecnologías de reconocimiento facial[71] (por ejemplo, para buscar en bases de datos de sospechosos e identificar a víctimas de trata de seres humanos o abuso y explotación sexual infantil), de identificación por voz, reconocimiento del habla, análisis autónomos de bases de datos identificadas, técnicas predictivas (actuación policial predictiva y análisis de puntos críticos de delincuencia), herramientas avanzadas de autopsia virtual para ayudar a determinar la causa de la muerte, vigilancia de las redes sociales (rastreo [scraping] y recopilación de datos para detectar conexiones), etc[72].

La implementación de sistemas de IA puede optimizar considerablemente algunas diligencias de investigación ya preexistentes. Pensemos, entre otras, en la práctica del agente encubierto informático (282 bis 6 de la LEcrim). Podríamos recurrir a la IA generativa, es decir, a sistemas que generan imagen, audio y vídeo para simular la identidad del agente e incluso para crear el material necesario para intercambiar el archivo ilícito[73]. De este modo, podría ponerse la técnica de los *deepfak*es al servicio de la investigación de determinados delitos y, por ejemplo, crear material "ultrafalso" pornográfico con la intención de desarticular una red

69 Como señala Barona Vilar, las ciencias forenses, la criminalística, han mutado; los métodos empleados se sostienen sobre algoritmos, software, que han introducido técnicas idóneas para ubicar, analizar, e introducir evidencias y pruebas en el proceso penal. *Algoritmización del Derecho y de la Justicia. De la inteligencia artificial a la Smart e Justice*, Tirant Lo Blanch, Valencia, 2021, p. 502.

70 Recordemos que la Ley 13/2015, de 5 de octubre, de modificación de la LECrim para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológicas, introdujo numerosos preceptos (arts. 588 bis a hasta 588 octies) para regular nuevos medios de investigación tecnológicos. Entre otros, la interceptación de las comunicaciones telefónicas y telemáticas (arts.588 ter a) y ss.); grabación de las comunicaciones orales directas (art. 588 quater a); captación de imágenes en lugares o espacios públicos (art. 588 quinquies a); utilización de dispositivos de geolocalización (art. 588 quinquies b); registro de dispositivos de almacenamiento masivo (art. 588 sexies b); registro remoto sobre equipos informáticos (art. 588 septies y ss.), etc.

71 Téngase en cuenta que el Reglamento de IA, en su art. 5, cataloga como "Prácticas de IA prohibidas", el uso de sistemas de identificación biométrica a distancia «en tiempo real» en espacios de acceso público con fines e aplicación de la ley, salvo y en la medida en que dicho uso sea estrictamente necesario para alcanzar determinados objetivos, entre los que se encuentra: la búsqueda selectiva de víctimas concretas de secuestro, trata de seres humanos o explotación sexual de seres humanos, así como la búsqueda de personas desaparecidas; la prevención de una amenaza específica, importante e inminente para la vida o la seguridad física de las personas físicas o de una amenaza real y actual o real y previsible de un atentado terrorista; o la localización o identificación de una persona sospechosa de haber cometido una infracción penal a fin de llevar a cabo una investigación o un enjuiciamiento penales o de ejecutar una sanción penal por alguno de los delitos mencionados en el anexo II que en el Estado miembro de que se trate se castigue con una pena o una medida de seguridad privativas de libertad cuya duración máxima sea de al menos cuatro años..

72 Vid. en este sentido, el Considerando M. de la Resolución del Parlamento Europeo, de 6 de octubre de 2021, sobre la inteligencia artificial en el Derecho penal y su utilización por las autoridades policiales y judiciales en asuntos penales (2020/2016(INI)).

73 González Pulido, I.: "El uso de la inteligencia artificial generativa en la investigación de la ciberdelincuencia de género: ante el auge de los deepfakes", *Ius et Scientia*, 2023, vol. 9, núm. 2, p. 176.

criminal, ganándose la confianza de sus miembros[74]. Algo similar es lo que ha hecho la holandesa *Sweetie*, de la ONG *Terre des Hommes*, que a través de un bot que se hace pasar por una niña, persigue la pornografía infantil en la red y ha conseguido localizar a miles de pederastas. A pesar de sus logros, la polémica está servida. Se plantean numerosas dudas acerca de su legalidad: presupuestos de legitimidad en la utilización de un agente encubierto robótico, los efectos jurídicos asociados a la provocación del delito, así como las dificultades para reconocer el derecho a la indemnidad sexual en un robot[75].

Como señala Llorente Sánchez-Arjona, el escenario en el que se desarrollan determinados delitos (abuso y explotación sexual infantil) resulta propicio a los sistemas de IA que pueden convertirse en una tecnología clave para hacer frente a los mismos. La autora cita algunos ejemplos, como el software denominado iCOP que permite identificar pederastia en la red; las herramientas creadas por Google y Apple (Neural Match) con el objetivo de luchar contra este tipo de delitos; C-SEX que analiza el comportamiento de los usuarios en el entorno de la pornografía infantil, etc.[76]. En nuestro país, la Secretaría de Estado de seguridad ha impulsado un proyecto para implementar una versión española de la herramienta *Chat Analysis Triage Tool* (CATT) para casos de *online child grooming*. Su objetivo es identificar, mediante el análisis del discurso y las tácticas utilizadas por los groomers en los chats, a aquellos abusadores que pretenden tener un encuentro físico con el menor, y diferenciarlos de aquellos que solo buscan satisfacer sus fantasías sin buscar un contacto real. De manera que se prioricen los recursos policiales en los primeros supuestos[77].

Sin duda alguna, la IA va a repercutir en el aumento de la eficacia de la lucha contra determinados delitos, entre los que destacamos, la explotación sexual en línea. Pero también debemos ser conscientes de los riesgos que implica. De ahí que nos cuestionemos, junto a Marchena Gómez, los límites que hay que imponer para que la investigación de esos delitos por el Estado no desborde los presupuestos que legitiman el ejercicio del *ius puniendi*. Como señala el magistrado, la necesidad de actualizar la metodología de la investigación penal no puede ser cuestionada.

74 Blázquez Moreno, R.: "Deepfakes en el procedimiento probatorio", *Revista vasca de derecho procesal y arbitraje*, 2023, vol. 35, núm. 3, p. 231.

75 Sea como fuere, la utilización de Sweetie ha sido asociada a la ventaja que proporciona, no ya como herramienta de investigación, sino para paliar los negativos efectos que los delitos de pornografía infantil producen en los agentes que los investigan. Los agentes infiltrados que operan en chats con el objetivo de localizar pedófilos tienen que soportar una fuerte carga psicológica por la exposición continuada a contenidos de esta pornografía, por lo que han de ser sustituidos cada cierto tiempo y pueden tener secuelas psicológicas, problema que se eliminaría si fuera un robot el que tratara con esos contenidos. Marchena Gómez, M.: "Inteligencia artificial y jurisdicción penal", Discurso con motivo de su ingreso como Académico de Número de la Real Academia de Doctores de España el 26 de octubre de 2022, separata de la Real Academia de Doctores de España, Madrid, p. 14.

76 Llorente Sánchez-Arjona, M.: "La inteligencia", cit., pp. 274 y 275.

77 En idéntico sentido, González-Álvarez, J.L., Santos-Hermoso, J. y Camacho-Collados, M.: "Policía predictiva en España. Aplicación y retos futuros", *Behavior & Law Journal*, 2020, núm. 6(1), p. 30.

Sin embargo, la constatación de ese hecho no debe llevarnos a legitimar, al amparo de las ventajas técnicas de la IA, una investigación en la que todo vale, sin reparar en la intensa injerencia estatal y consiguiente sacrificio del espacio de intimidad que cada ciudadano dibuja frente a los poderes públicos y a terceros. Por eso la importancia de que la regulación de estas diligencias ligadas a las nuevas tecnologías sea encabezada por una referencia a los principios rectores a los que se refiere el artículo 588 bis a) de la LECrim, es decir, a los principios de especialidad, idoneidad, necesidad y proporcionalidad[78].

En definitiva, no podemos olvidar que el empleo de sistemas de IA en el seno de una investigación judicial entraña numerosos riesgos que pueden afectar seriamente a los derechos y garantías constitucionales que deben presidir el proceso. La eficiencia no puede en modo alguno anteponerse o ir en detrimento de los mismos[79]. Deben, por tanto, necesariamente salvaguardarse los derechos de las personas investigadas. En este sentido, si bien no se prohíben en el Reglamento europeo de IA, se supedita su utilización al cumplimiento de determinados requisitos (previstos en los artículos 8 y ss) dado que, como ya hemos adelantado, se califican de alto riesgo. Entre otros, se exige garantizar un nivel de transparencia suficiente, permitir una efectiva supervisión humana y contar con un nivel adecuado de precisión, solidez y ciberseguridad.

3. Instrumentos de valoración del riesgo de reincidencia.

Tanto en el seno del proceso penal como en el ámbito penitenciario, asistimos al empleo de instrumentos de valoración del riesgo de reincidencia (*risk assessment instruments*, conocidos por sus siglas, RAIs)[80]. Estas herramientas estructuradas de valoración del riesgo han ido evolucionando hasta alcanzar su automatización y

78 Marchena Gómez, M.: "Inteligencia artificial", cit., p. 15. Como señala este autor, una puntualización es obligada. Los principios a los que hacemos referencia representan límites axiológicos que la LECrim contempla como presupuestos de legitimidad para validar diligencias intrusivas en el círculo de derechos definidos por el art. 18 de la CE. Sin embargo, son otros muchos los derechos afectados cuando el ciudadano se expone a las técnicas de investigación de IA que aspiran al esclarecimiento del hecho investigado. Algunos de estos derechos y los principios que han de condicionar su limitación por el Estado tienen hoy nombre propio en nuestro sistema constitucional -principio de contradicción, igualdad, derecho de defensa, imparcialidad del órgano judicial, protección de datos *ex* art. 24 de la CE. Otros son principios y derechos de nueva generación que discurren, hoy por hoy, en el terreno dogmático -principio de transparencia algorítmica, principio de trazabilidad, principio de imparcialidad del validador o derechos a la dignidad algorítmica y a la identidad algorítmica-, que, a buen seguro, adquirirán, antes o después, tratamiento normativo.

79 Alerta BARONA VILAR, además, sobre el peligro de emplear las medidas de investigación tecnológicas de alta fiabilidad investigadora para reducir o eliminar riesgos, empero no para investigar hechos cometidos. Obviamente, la confusión de funciones no es neutra, ni las consecuencias que se van a producir en el respeto a los derechos humanos tampoco lo es. Abandonamos el derecho penal *ex post*, para construir el derecho penal *ex ante*, que reacciona ante riesgos y amenazas, y lo hace con toda la carga en profundidad sobre las garantías y los derechos. *Algoritmización del,* cit., p. 503.

80 Aunque vamos a analizarlos únicamente en el marco de un proceso penal, estas herramientas también se emplean en el ámbito penitenciario. Así ocurre en nuestro país, en concreto en las prisiones catalanas, que utilizan la herramienta RISCANVI para evaluar la conducta de los internos, y en función de ello, asistir en la decisión acerca de la situación del privado de libertad, ya sea para concederle un permiso de salida, clasificarle en un grado o incluso, otorgarle la libertad condicional.

digitalización con un elevado grado de sofisticación. De hecho, las más novedosas se asisten de algoritmos para emitir el pronóstico, incluso recurriendo a sistemas inteligentes computarizados para su tratamiento[81], con el fin de conjurar el riesgo de reiteración delictiva basándose en la información que obra en los expedientes y en las informaciones estadísticas de casos previos[82].

Los instrumentos de valoración del riesgo pueden ser útiles en el asesoramiento al juez acerca del riesgo de reincidencia del presunto maltratador. Este riesgo, recordamos, es determinante en la adopción de las órdenes de protección del artículo 544 ter LEcrim u otras medidas cautelares para proteger a las víctimas de violencia de género (medidas de alejamiento, prohibición de comunicación, etc.) así como a sus hijos/as menores (suspensión cautelar del régimen de visitas del art. 544 ter.7 LEcrim)[83]. En este sentido, estas herramientas pueden auxiliar al juez a la hora de adoptar su decisión. Eso sí, solo como un elemento más, que deberá en todo caso ser corroborado por otros datos o circunstancias.

El carácter crónico y repetitivo de la violencia contra la pareja, así como la relación de afectividad existente entre la víctima y el agresor, conlleva un riesgo adicional para las víctimas de violencia de género que difiere del de otros delitos, y muestra una urgente necesidad de protección frente a una posible reincidencia. De ahí que, en los últimos tiempos, los instrumentos de valoración del riesgo de violencia contra la pareja se hayan multiplicado. Entre otros, destacan: SARA (*Spousal Assault Risk Assessment*), DASH (*Domestic abuse, stalking y harassment and honour-based violence*) y SVR-20 (*Sexual Violence Risk Assessment*[84]).

En España contamos desde el año 2007 con el sistema VioGén (Sistema de Seguimiento Integral en los casos de Violencia de Género). Esta herramienta informática permite el seguimiento y protección de las víctimas de violencia de género y de sus hijos/as. Entre sus objetivos, destaca la realización de valoraciones policiales del riesgo de las víctimas denunciantes de sufrir una nueva agresión, y en función del resultado, poder protegerlas. Para dicha tarea se sigue un Protocolo en el que se emplean dos instrumentos complementarios: la Valoración Policial del Riesgo (VPR4.0) para realizar una estimación inicial y la Valoración Policial de

81 Romeo Casabona, C. M.: "Riesgo, procedimientos actuariales basados en inteligencia artificial y medidas de seguridad", *Revista de Derecho, Empresa y Sociedad (REDS)*, julio-diciembre 2018, núm. 13, p. 43

82 Simón Castellano, P.: *Justicia Cautelar e inteligencia artificial. La alternativa a los atávicos heurísticos judiciales*, Bosch, Barcelona, 2021, p. 25.

83 Como refiere Magro Servet, nos encontramos ante un fenómeno claramente repetitivo y con un aspecto conductual que se reproduce en el tiempo, que tiene unos parámetros de actuación homogéneos en la mayoría de los casos y con un carácter predecible en cuanto a los hechos que han ocurrido y a la protección a las víctimas de lo que pueda ocurrir. Pocas materias existen en la actualidad en donde el mimetismo conductual se reproduce con tanta repetición como en la violencia de género. "La inteligencia artificial para mejorar la lucha contra la violencia de género", en AA.VV.: *Inteligencia artificial legal y Administración de Justicia* (dir. por S. Calaza López y M. Llorente Sánchez-Arjona), Cizur Menor: Aranzadi, 2022, pp. 398 y 405.

84 Esta herramienta valora el riesgo de violencia sexual.

la Evolución del Riesgo (VPER4.0) para el seguimiento del caso. Si bien VioGén se diseñó inicialmente para evaluar el riesgo de reincidencia de una agresión, posteriormente se creó otro algoritmo para valorar la posibilidad de sufrir violencia letal (formulario VPR5.0).

De manera que, cuando una víctima de violencia de género interpone una denuncia, deviene preceptiva la realización por parte de la policía de un análisis de la valoración del riesgo al que se encuentra sometida. Para ello, se le formulan una serie de preguntas y se cumplimenta por los agentes policiales el formulario VPR. Los datos introducidos se someten a un algoritmo que, tras valorar automáticamente cada ítem, establece uno de los cinco niveles de riesgo que presenta la víctima de sufrir una nueva agresión a corto plazo: "extremo", "alto", "medio", "bajo" y "no apreciado". En función del resultado asignado, se llevan a cabo de forma inmediata las medidas provisionales de protección policial aparejadas a cada nivel de riesgo[85]. El informe obtenido se incluirá en el atestado (junto al resto de diligencias policiales) y servirá para informar al juez a la hora de decidir las medidas de protección de la víctima que deben adoptarse en cada caso. Efectuada la valoración inicial, la estimación del riesgo debe mantenerse actualizada. Para ello, la policía cumplimenta el segundo formulario (VPER) que, mediante valoraciones periódicas, permite la monitorización de las víctimas[86].

Sin negar la utilidad de esta herramienta, no podemos obviar que puede fallar. Muestra de ello, es la Sentencia de 30 de septiembre de 2020 de la Audiencia Nacional, que ha condenado al Estado español por la deficiente protección que la Guardia Civil proporcionó a una mujer que solicitó una orden de protección[87]. El sistema VioGén asignó el nivel de "no apreciado" y sin mayores indagaciones, a pesar de la existencia de indicios suficientes de maltrato, las autoridades policiales calificaron el caso en este sentido, lo que determinó que el juez denegara la orden

85 Adviértase que el agente puede modificar (al alza) el riesgo apreciado si estima que existen razones para ello.

86 Conviene dejar claro que el sistema VioGén, al igual que otras herramientas actuariales de valoración del riesgo, no puede considerarse IA en sentido estricto. Miró Llinares, F.: "Inteligencia artificial y justicia penal: más allá de los resultados lesivos causados por robots", *Revista de Derecho Penal y Criminología*, 2018, núm. 20, p. 103. Cierto es que la conexión con la IA es evidente, pero la IA va más allá. Como señala Simón Castellano, es una diferencia sutil, puesto que casi todas las herramientas actuariales tienen una parte automática y automatizable, o digital, como es el cálculo de la probabilidad, pero esto no en realidad motivo bastante para considerarlo por si solo IA. *Justicia Cautelar,* cit., p. 94

87 Recordamos la importancia de formar en perspectiva de género a quienes hacen uso de estas herramientas. Como señala Arruti Benito, este caso evidencia la ausencia de perspectiva de género en la implementación de los sistemas de IA. Por un lado, muestra la fe ciega a la objetividad de los sistemas de IA, olvidando su carácter complementario y asistencial –que no sustitutivo–depositando, en la valoración de un algoritmo, la toma de decisión que corresponde a la inteligencia humana y al sentido común humano. Por otro lado, pone de manifiesto la ausencia de conocimiento sobre el potencial discriminatorio que entrañan este tipo de sistemas debido a los sesgos de género que pueden incorporarse. "Justicia e inteligencia artificial en clave de género", en AA.VV.: *Investigación y género. Proyectos y resultados en estudios de las mujeres: VIII Congreso Universitario Internacional de Investigación y Género* (ed. por M. E. García y A. M. de la Torre Sierra), Universidad de Sevilla, 2022, p. 402.

solicitada y su consecuente trágico final por el que la mujer murió asesinada a manos de su marido[88].

Son muchas las voces que advierten acerca de las falencias de este sistema[89]. Entre otras, se critica que actualmente VioGén se rige por unos parámetros que han ha quedado arcaicos, no siempre se ajustan a la realidad, y en ocasiones arroja resultados poco adecuados[90]. Se ha evidenciado que el sistema necesita una mejora. De ahí que, tal y como se ha anunciado, el Área de Violencia de Género, Estudios y Formación de la Secretaría de Estado de Seguridad ha incorporado la plataforma analítica de la empresa de software SAS Iberia, que va a "facilitar actualizaciones mucho más rápidas y eficaces del Protocolo VPR del Sistema VioGén, ponderando mejor los actuales indicadores de riesgo de reincidencia e identificando nuevas variables que ayuden a afinar aún más esa valoración de riesgo mediante análisis automatizados y en tiempo real de grandes cantidades de datos"[91].

V. A MODO DE SÍNTESIS FINAL.

La transformación digital de la Justicia debe realizarse desde una perspectiva de género. Solo así podrá promoverse una justicia que garantice el respeto del derecho constitucional a la tutela judicial efectiva en condiciones de igualdad.

El empleo de herramientas y aplicaciones de IA puede tener un impacto negativo significativo en la justicia, si no se identifican, abordan y afrontan los posibles sesgos algorítmicos que refuerzan estereotipos de género. Al mismo tiempo, preocupa la posibilidad de que la IA pueda ser utilizada como un instrumento para ejercer nuevas formas de violencia de género. Entre otras, a través de los *deepfake*s, que, además, podrían ser incorporados en un juicio socavando la integridad de los

88 Adviértase, que no se condena por error judicial, sino por no recibir una adecuada información de la Guardia Civil acerca de cuál era la situación real del riesgo de la víctima, que fue determinante a la hora de orientar al juez en el (no) dictado de una orden de protección.

89 Como alerta el Informe de auditoría externa del Sistema VioGén llevado a cabo en el año 2022 por la Fundación Ana Bella (p. 26), el sistema se basa en el supuesto de que las mujeres entienden y responden con claridad a los 35 puntos del formulario VPR y los agentes de policía transforman objetivamente las declaraciones de las mujeres en respuestas binarias (presente/no presente). Pero en la realidad, el proceso rara vez funciona de este modo idealizado. Esto significa que la calidad de los datos introducidos podría verse comprometida durante la fase de generación de datos, lo que daría lugar a posibles fuentes de sesgo y tergiversación.

90 En este sentido, Llorente Sánchez-Arjona, M.: "La inteligencia artificial", cit., p. 268. De otro lado, las Fuerzas y Cuerpos de Seguridad del Estado son las que se ocupan de introducir todos los datos en el sistema, muchos de los cuales desconocen y deben contestar de forma intuitiva a partir de la toma de declaración de la víctima, cuando presenta la denuncia, y del agresor.

91 Con el *software* de SAS Iberia se incorpora tecnología de analítica avanzada e IA que automatizará el análisis de una mayor cantidad de datos de criminalidad, combinados incluso con datos de fuentes abiertas, lo que ayudará a ponderar mejor los algoritmos, identificando nuevos indicadores de riesgo, y en periodos de tiempo mucho más cortos. Además, son algoritmos más sensibles a la evolución de la criminalidad y mejoran con ello la predicción de aquellos casos en los que es previsible que se produzcan agresiones reincidentes. La Moncloa. Interior 15.12.2020, disponible en: https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/interior/Paginas/2020/151220-inteligencia.aspx

procesos judiciales. Debemos, por tanto, tener en cuenta estos peligros y tratar de establecer medidas de índole política, jurídica y tecnológica adecuadas para prevenirlos.

A pesar de los riesgos mencionados, no podemos dejar de reconocer las bondades que las nuevas herramientas algorítmicas pueden ofrecer a la justicia en términos de colaboración o auxilio. Especialmente y en lo que a este trabajo se refiere, cuando nos enfrentamos ante uno de los mayores exponentes de la desigualdad como es la violencia de género. Estas herramientas pueden utilizarse para apoyar a las víctimas, investigar delitos y prevenir la reincidencia mediante sistemas de evaluación del riesgo, siempre y cuando no se menoscaben los derechos y garantías que deben presidir un proceso.

En definitiva, si bien la IA tiene el potencial de mejorar la eficiencia, efectividad e incluso, la calidad de la justicia, deviene imprescindible abordar los riesgos asociados a las misma. Para ello, la integración de la perspectiva de género no solo en su diseño y desarrollo sino también en su aplicación por parte de nuestros Juzgados resulta fundamental en aras de garantizar su impacto positivo y su alineación con el principio de igualdad.

BIBLIOGRAFIA

Arruti Benito, S.: "Justicia e inteligencia artificial en clave de género", en AA.VV.: *Investigación y género. Proyectos y resultados en estudios de las mujeres: VIII Congreso Universitario Internacional de Investigación y Género* (ed. por M. E. García y A. M. de la Torre Sierra), Universidad de Sevilla, 2022, pp. 395-406.

Barona Vilar, S.: *Algoritmización del Derecho y de la Justicia. De la inteligencia artificial a la Smart Justice*, Tirant lo Blanch, Valencia, 2021.

Barona Vilar, S.: "La necesaria deconstrucción del modelo patriarcal de justicia", en AA.VV.: *Análisis de la Justicia desde la perspectiva de género*, Tirant Lo Blanch, Valencia, 2018.

Barona Vilar, S.: "Dataización de la justicia (Algoritmos, Inteligencia Artificial y Justicia, ¿el comienzo de una gran amistad?)", *Revista Boliviana de Derecho*, 2023, núm. 36, pp. 14-45.

Belloso Martin, N.: "La problemática de los sesgos algorítmicos (con especial referencia a los de género) ¿Hacia un derecho a la protección contra los sesgos?", en AA.VV.: *Inteligencia artificial y filosofía del derecho* (dir. por F. llano Alonso), Laborum, Murcia, 2022.

Bello San Juan, P.: "La inteligencia artificial al servicio del crimen: La revolución del deepfake desde una perspectiva criminológica", en AA.VV.: *La justicia en la sociedad 4.0: nuevos retos para el siglo XXI* (dir. por L. Fontestad Portalés), Colex, 2023.

Blanco García, A. I.: "Retos para una inteligencia artificial inclusiva de los colectivos vulnerables", *Revista Actualidad jurídico Iberoamericana*, 2024, núm. 21.

Blázquez Moreno, R.: "Deepfakes en el procedimiento probatorio", *Revista vasca de derecho procesal y arbitraje*, 2023, vol. 35, núm. 3.

Borraz, M. y Pastor, A.: "'Deepfakes' sexuales: el caso de las menores de Almendralejo consolida una nueva forma de violencia machista", e*l Diario*.es, 19 de septiembre de 2023.

Catalán Chamorro, M.J.: "La carta de derechos digitales y su implicación en el derecho procesal español", en AA. VV.: *Digitalización de la justicia: prevención, investigación y enjuiciamiento* (dir. por M. Llorente Sánchez-Arjona y S. Calaza López), Aranzadi, Cizuer Menor, 2022, pp. 179 - 208.

Catalán Chamorro, M.J.: L*a justicia digital en España. Retos y desafío*s, Tirant Lo Blanch, Valencia, 2023.

Cerdán Martínez, V. y Padilla Castillo, G.: "Historia del fake audiovisual: deepfake y la mujer en un imaginario falsificado y perverso", *Historia y comunicación social*, 2019, núm. 24 (2).

Constanza Gamboa, N.: "La inteligencia artificial como herramienta al servicio de la erradicación de la Violencia de Género", Observatorio violencia, septiembre 21, 2020.

Danesi, C.: "Sesgos algorítmicos de género con identidad iberoamericana: las técnicas de reconocimiento facial en la mira", *Revista Derecho de Familia*, 2021, núm.100.

Delfino, R. A., "Deepfakes on trial: a call to expand the trial judge's. Gatekeeping role to protect legal proceedings from technological fakery", *Hastings Law Journal,* 2023, vol. 74, núm. 2, pp. 293- 348.

De Luis García, E., "Justicia, inteligencia artificial y derecho de defensa", *IDP: revista de internet, derecho y política*, 2023, núm. 39.

Ei, D., y Moser, G.: "Human arbitrators (the undisputed champion) v (the robots challenger)", *Hong Kong L.J*, 2020, vol. 50.

Fernández, A.: "Inteligencia artificial en los servicios financieros", *Boletín económico - Banco de España*, 2019, núm. 2.

Gil, P.: "La perspectiva de la mujer víctima del sistema judicial ajeno al género", en AA.VV.: *Análisis de la Justicia desde la perspectiva de género*, Tirant Lo Blanch, Valencia, 2018.

González Pulido, I.: "El uso de la inteligencia artificial generativa en la investigación de la ciberdelincuencia de género: ante el auge de los deepfakes", *Ius et Scientia*, 2023, vol. 9, núm. 2.

González-Álvarez, J.L., Santos-Hermoso, J. y Camacho-Collados, M.: "Policía predictiva en España. Aplicación y retos futuros", *Behavior & Law Journal*, 2020, núm. 6(1).

Hao, K., "This Is How AI Bias Really Happens - and Why It's So Hard to Fix", *MIT Technology Review*, 4 febrero 2019.

Kweilin, L.T.: "Deepfakes and domestic violence: perpetrating intimate partner abuse using video technology", *Victims & Offenders*, 2022, vol. 17, núm. 5.

Llorente Sánchez-Arjona, M.: "La inteligencia artificial como nueva estrategia de prevención en los delitos de violencia sexual", en AA.VV.: *Uso de la información y de los datos personales en los procesos: los cambios en la era digital* (dir. por I. Colomer Hernández), Aranzadi, Cizur Menor, 2022.

Lloria García, P.: *Violencia sobre la mujer en el siglo XXI. Violencia de control y nuevas tecnologías: habitualidad, sexting y stalking*, Iustel, Madrid, 2020.

LO, M.: "A Domestic Violence Dystopia: Abuse via the Internet of Things and Remedies Under Current Law", *California Law Review*, 2021, vol. 109.

Lorente Acosta, M.: "Justicia, género y estereotipos", en AA.VV.: *Análisis de la Justicia desde la perspectiva de género*, Tirant Lo Blanch, Valencia, 2018.

Macchiavelli, N.: "La violencia de género y el uso de algoritmos como herramienta efectiva para la protección de los derechos fundamentales", 2022, *AFD*, (XXXVIII).

Macchiavelli, N.: "Perspectiva de género en las nuevas tecnologías. El problema de los sesgos", *Diario Suplemento Derecho y Tecnología*, 2021, núm. 84.

Magro Servet, v.: "La inteligencia artificial para mejorar la lucha contra la violencia de género", en AA.VV.: *Inteligencia artificial legal y Administración de Justicia* (dir. por S. Calaza López y M. Llorente Sánchez-Arjona), Cizur Menor: Aranzadi, 2022.

Marchena Gómez, M.: "Inteligencia artificial y jurisdicción penal", Discurso con motivo de su ingreso como Académico de Número de la Real Academia de Doctores de España el 26 de octubre de 2022, separata de la Real Academia de Doctores de España, Madrid.

Marcos Francisco, D.: "Sistema arbitral de consumo: algunas propuestas 'inteligentes' de lege ferenda", *InDret*, 2024, núm. 1, pp. 114-150.

Marks, P., "Bangladesh: Sex harassment app helps women map abuse", *NewScientist,* mayo 2014.

Martin, P., "España usará la IA y el 'big data' para proteger mejor a las víctimas del machismo", *Diario el Periódico*, 23 de septiembre de 2023.

Martínez García, E.; Borges Blázquez, R. y Simó Soler, E.: "Inteligencia artificial y perspectiva de género en la justicia penal", *Diario* La *Ley*, Sección Ciberderecho, 20 de enero de 2021, núm 47.

Mayson, S. G.: "Bias In, Bias Out", *Yale Law Journal*, 2018, núm. 128, pp. 2218-2300.

Miguel Freita, P.: "Deepfakes, conteúdo gerado por inteligência artificial e verdade processual", en AA.VV.: *El proceso penal ante una nueva realidad tecnológica europea* (dir. por C. Arangüena Fanego, M. De Hoyos Sancho y E. Pillado González), Thomson Reuters Aranzadi, 2023.

Miró Llinares, F.: "Inteligencia artificial y justicia penal: más allá de los resultados lesivos causados por robots", *Revista de Derecho Penal y Criminología*, 2018, núm. 20.

Navas Navarro, S.: "La perspectiva de género en la inteligencia artificial", *Diario La Ley*, sección Ciberderecho, 8 de marzo de 2021, núm. 48.

O'neil, C.: *Armas de destrucción matemática*, Capitán Swing, Madrid, 2017.

Ortiz De Zárate, L. y Guevara gómez, A.: Inteligencia artificial e igualdad de género. Un análisis comparado entre la UE, Suecia y España, Fundación alternativas, 2021, núm. 101.

Pfefferkorn, R.: «Deepfakes" in the Courtroom», *BU Pub. Int. LJ*, 2020, vol. 29.

Rivas Vallejo, P.: "Sesgos de género en el uso de inteligencia artificial para la gestión de las relaciones laborales: análisis desde el derecho antidiscriminatorio", *e-Revista Internacional de la Protección Social(e-RIPS)*, 2022, vol. VII, núm. 1.

Romeo Casabona, C. M.: "Riesgo, procedimientos actuariales basados en inteligencia artificial y medidas de seguridad", *Revista de Derecho, Empresa y Sociedad* (REDS), julio-diciembre 2018, núm. 13.

Sanchis Crespo, C., "Inteligencia artificial y decisiones judiciales: crónica de una transformación anunciada", *Scire: Representación y organización del conocimiento*, 2023, vol. 29, núm. 2, pp. 65-84.

Senden Xenidis, R. y Senden, L.: "EU non-discrimination law in the era of artificial intelligence: Mapping the challenges of algorithmic discrimination", en AA.VV.: *General Principles of EU law and the EU Digital Order* (ed. por U. Bernitz *et al.*), Kluwer Law International, Países Bajos, 2020.

Simó Soler, E.: "Retos jurídicos derivados de la Inteligencia Artificial Generativa Deepfakes y violencia contra las mujeres como supuesto de hecho", *InDret*, febrero 2023, núm. 2, pp. 493- 515.

Simó Soler, E., *Estereotipos de género en procesos por violencia sexual,* Tirant lo Blanch, Valencia, 2023.

Simón Castellano, P., *Justicia Cautelar e inteligencia artificial. La alternativa a los atávicos heurísticos judiciales*, Bosch, Barcelona, 2021.

Soriano Arnanz, A.: "Discriminación algorítmica: garantías y protección jurídica", en AA.VV.: *Derechos y garantías ante la inteligencia artificial y las decisiones automatizadas* (dir. por L. Cotino Hueso), Aranzadi, 2022, pp. 139-169.

Soriano Arnanz, A.: "Creating non-discriminatory Artificial Intelligence systems: balancing the tensions between code granularity and the general nature of legal rules", *Revista de Internet, Derecho y Política*, 2023, núm. 38.

Soto Santana, M.: "Justice for Women: Deep fakes and Revenge Porn", 3rd Global Conference on woman´s studies, 25-27 septiembre 2022.

T Trend Micro Research, United Nations Interregional Crime and Justice Research Institute (UNICRI) Europol's European Cybercrime Centre (EC3), "Malicious Uses and Abuses of Artificial Intelligence", 2020.

¿QUIÉN ES QUIÉN EN EL REGLAMENTO EUROPEO DE INTELIGENCIA ARTIFICIAL? LAS AUTORIDADES NOTIFICANTES Y LOS ORGANISMOS NOTIFICADOS

WHO IS WHO IN THE ARTIFICIAL INTELLIGENCE ACT? THE NOTIFYING AUTHORITIES AND NOTIFIED BODIES

Actualidad Jurídica Iberoamericana Nº 21, agosto 2024, ISSN: 2386-4567, pp. 598-617

Adrián PALMA ORTIGOSA

ARTÍCULO RECIBIDO: 29 de mayo de 2023
ARTÍCULO APROBADO: 1 de julio de 2024

RESUMEN: Todos y todas queremos que un producto que usamos no nos cause daños y funcione adecuadamente. Ya ha quedado más que patente que el uso de sistemas de inteligencia artificial puede generar importantes riesgos para las personas. A su vez, tampoco hay duda del valor que aporta su uso a las sociedades de hoy en día. El Reglamento de IA marca las reglas del juego a las organizaciones que pretendan desarrollar o utilizar sistemas de IA en sus fronteras. Entre esas reglas encontramos una serie de entidades que tiene como objetivo cerciorarse que los sistemas de IA cumplen con las exigencias del Reglamento de IA, sobre todo, en la fase previa a la puesta en el mercado de estos. Estas entidades son los organismos notificados y la autoridad notificante. En este trabajo estudiamos su régimen jurídico y su ámbito de aplicación en diferentes sectores como el policial, judicial, identificación biométrica, productos sanitarios, ascensores, juguetes, entre otros.

PALABRAS CLAVE: Biometric identification; new legislative framework; notified body; conformity assessment; high-risk ai systems.

ABSTRACT: *People want a product not to harm them when they use it. It is clear that the use of AI systems creates risks for citizens. At the same time, there is also no doubt about the value that their use brings to today's societies. The Artificial Intelligence Act establishes the rules of the game for organisations seeking to develop or use AI systems within their borders. Among these rules several entities play an essential role in the pre-marketing phase of these AI systems. These entities are the notified bodies and the notifying authority. In this paper we study their legal regime and their scope of application in different sectors such as police, judicial, biometric identification, medical devices, lifts, toys, among others.*

KEY WORDS: *Identificación biométrica; nuevo marco legislativo; organismo notificado; evaluación de la conformidad; sistemas de inteligencia artificial de alto riesgo.*

I. INTRODUCCIÓN.

El Reglamento Europeo de Inteligencia Artificial[1] (Reglamento de IA) establece todo un conjunto de reglas que tratan de asegurar que ciertos sistemas de IA generen el menor número de riesgos para los derechos fundamentales de las personas[2].

1. Aproximación general al Reglamento de IA.

Estas reglas se pueden clasificar de forma resumida en los siguientes puntos.

En primer lugar, se prohíbe el uso de determinados sistemas de IA al considerarse que los riesgos que estos pueden generar a las personas no son tolerables en el entorno de la Unión Europea. A su vez, existen determinados sistemas de IA, los considerados de alto riesgo, cuyo uso resulta muy útil para la ciudadanía pero los riesgos que estos pueden generar son tan altos que las organizaciones que diseñan y ponen en el mercado estos sistemas se les obliga a desplegar toda una serie de medidas para reducir en la medida de lo posible dichos riesgos. Es decir, la Unión Europa los considera necesarios pero bajo unas garantías mínimas, garantías que se convierten en el grueso esencial previsto en el Reglamento de IA. Además de los sistemas de alto riesgo, también se contemplan reglas específicas para los llamados modelos de IA de propósito general, los cuales, pueden utilizarse para todo tipo de finalidades[3]. Finalmente se contemplan una serie de obligaciones

1 La versión que se ha tomado como referencia del Reglamento de IA es del 13 de marzo de 2024. Resolución legislativa del Parlamento Europeo, de 13 de marzo de 2024, sobre la Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión.

2 Este trabajo se ha llevado a cabo en el marco de los siguientes proyectos de investigación: "Algorithmical Law" (PROMETEO/2021/009. Financiado por la Generalitat Valenciana. "La regulación de la economía digital: tutela publica de la igualdad y herramientas algorítmicas" (PID2019-108745GB-I00). Ministerio de Ciencia e Innovación. "Derechos y garantías públicas frente a las decisiones automatizadas y el sesgo y discriminación algorítmicas" 2023-2025 (PID2022-136439OB-I00) financiado por el Ministerio de Ciencia e Innovación. "Herramientas algorítmicas para ciudadanos y Administraciones Públicas" (Proyectos de Generación de Conocimiento, Ministerio de ciencia e Innovación, convocatoria 2021, PID2021-126881OB-I00).

3 Artículo 3.63. Modelo de IA de uso general: un modelo de IA, también uno entrenado con un gran volumen de datos utilizando la autosupervisión a gran escala, que presenta un grado considerable de generalidad

• Adrián Palma Ortigosa
Profesor. Ayudante Doctor de Derecho Administrativo, Universitat de València.
Correo electrónico: adrian.palma@uv.es

mínimas de transparencia para determinados sistemas de IA que en determinados contextos pueden causar también importantes perjuicios para la sociedad, nos estamos refiriendo a los chatbots o a los sistemas generadores de deepfakes entre otros.

En segundo lugar, se definen y se establecen las funciones y obligaciones principales exigibles a los diferentes agentes y operadores que pueden están presentes durante el ciclo de vida de los sistemas de IA. Cabe destacar dos sujetos, los proveedores, que son los que se encargan de desarrollar los sistemas de IA, y, los responsables del despliegue, que son aquellos que los utilizan. Entre esas funciones están la de integrar adecuadamente en los sistemas de IA los requisitos técnicos esenciales[4], evaluar la conformidad de estos[5], notificar en determinadas circunstancias sobre diferentes incidentes sufridos por los sistemas de IA, etc.

En tercer lugar, se contempla la figura de una serie de entidades públicas y privadas que tienen un papel muy relevante antes de que los sistemas de IA se pongan en el mercado. Por un lado encontramos a los organismos de normalización europeos[6], estas entidades privadas tienen como función principal desarrollar normas técnicas voluntarias que posteriormente pueden aplicar los proveedores de sistemas de IA para cumplir con los requisitos exigidos a los sistemas de IA, las llamadas normas armonizadas. Estas normas técnicas también las puede elaborar la Comisión Europea, su nombre en estos casos se conoce especificaciones comunes[7]. Por otro lado, encontramos otra serie de organizaciones públicas y privadas que tienen como objetivo certificar que un sistema de IA, antes de que se ponga en el mercado, cumpla con los requisitos exigidos por el Reglamento de IA, estos son los organismos notificados.

En cuarto lugar el Reglamento de IA desarrolla una estructura de gobernanza integrada por diferentes organismos y entidades europeas que tratan de asegurar el cumplimiento de esta norma y la homogenización de su aplicación en la Unión

y es capaz de realizar de manera competente una gran variedad de tareas distintas, independientemente de la manera en que el modelo se introduzca en el mercado, y que puede integrarse en diversos sistemas o aplicaciones posteriores, excepto los modelos de IA que se utilizan para actividades de investigación, desarrollo o creación de prototipos antes de su comercialización". Reglamento Europeo de IA.

4 Para los sistemas de IA de alto riesgo esos requisitos se encuentran en los artículos 8 a 15, entre otros, calidad de los datos, niveles adecuados de transparencia, métricas de precisión o solidez, etc. Para los modelos de IA de uso general esos requisitos se encuentran en los artículos 53 a 55.

5 La evaluación de la conformidad es el proceso por el que se demuestra que un producto cumple con los requisitos especificados en una norma o estándar. ISO/IEC 17000:2004. Conformity assessment — Vocabulary and general principles.

6 Estos organismos europeos de normalización son CEN, CENELEC y ETSI.

7 Reglamento de Ejecución (UE) 2022/2346 de la Comisión de 1 de diciembre de 2022 por el que se establecen especificaciones comunes para los grupos de productos sin finalidad médica prevista enumerados en el anexo XVI del Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo, sobre los productos sanitarios.

Europea. Destacamos por ejemplo al Consejo Europeo de IA o a la Oficina de la IA.

Finalmente, en quinto lugar, se obliga a los Estados Miembros a crear o en su caso otorgar toda una serie de competencias a diferentes autoridades públicas que velarán también en el plano nacional por el cumplimiento del Reglamento de IA. Estas autoridades son la autoridad de vigilancia del mercado y la autoridad notificante.

2. El Nuevo Marco Legislativo.

La estructura previamente descrita no es novedosa del Reglamento Europeo de IA. Esta norma sigue el esquema establecido por el llamado "nuevo marco legislativo", en adelante NML. El NML está integrado por varios textos legales europeos que establecen unas bases comunes sobre la comercialización, evaluación y vigilancia de productos en la Unión Europea[8]. De esta manera, la Unión Europea, cuando pretende regular la producción y puesta en el mercado de un producto puede tomar como referencia la estructura marcada por el NML[9], el cual tiene como objetivo asegurar una evaluación y puesta en el mercado fiable de tales productos y bienes cuyo uso pueden generar riesgos para las personas[10].

Entre los productos o componentes de seguridad de productos que siguen la estructura marcada por el NML encontramos: ascensores, máquinas, juguetes, equipos radioeléctricos, productos sanitarios, productos sanitarios para diagnóstico in vitro, equipos a presión, equipo de embarcaciones de recreo, instalaciones de transporte por cable, etc.

II. LOS ORGANISMOS NOTIFICADOS.

1. Concepto de organismo notificado.

Los organismos notificados son aquellas organizaciones que realizan la evaluación de la conformidad de los sistemas de IA de acuerdo a los requisitos establecidos en el Reglamento de IA y otras legislaciones aplicables a estos sistemas. La tarea fundamental por tanto de los organismos notificados es verificar

8 Las tres textos legales que conforman el Nuevo Marco Legislativo son: el Reglamento (CE) n.º 765/2008 del Parlamento Europeo y del Consejo por el que se establecen los requisitos de acreditación y vigilancia del mercado de los productos; la Decisión n.º 768/2008/CE del Parlamento Europeo y del Consejo sobre un marco común para la comercialización de los productos y; el Reglamento (UE) 2019/1020 del Parlamento Europeo y del Consejo relativo a la vigilancia del mercado y la conformidad de los productos.

9 Para una aproximación histórica del Nuevo Marco legislativo véase: Álvarez García, V.: *Industria,* Iustel, 2010, pp. 47 y ss. Véase también la *Guía azul sobre la aplicación de la normativa europea relativa a los productos* de 2022 de la Comisión Europea, pp.7 y ss. También: Bernárdez García, B.: "El papel de los organismos de control en el aseguramiento de la seguridad industrial", *Economía industrial,* 2015, núm. 396, p. 82.

10 Véase los considerandos 46, 64, 83, 84, 87, 124 del Reglamento Europeo de IA.

que un sistema de IA que pretende poner en el mercado un proveedor cumple con los requisitos exigidos por el Reglamento de IA. Esta tarea resulta esencial ya que supone un control ex ante del sistema de IA previo a su uso.

Para que un organismo notificado pueda realizar la evaluación de la conformidad de los sistemas de IA, éste deberá haber sido autorizado por una autoridad pública, esta es, la autoridad notificante. Esta última comprobará a través de un procedimiento específico si esa entidad puede realizar las verificaciones de conformidad[11].

Los organismos notificados pueden ser tanto personas físicas como jurídicas[12], así como entidades públicas y privadas. En todos los casos estas entidades deben contar con los requisitos exigidos en el Reglamento de IA, así como con las normas previstas en el derecho interno de los EEMM. Estos han de tener su sede en alguno de los Estados miembros de la UE o en un tercer país con el que la Unión Europea haya celebrado un acuerdo para realizar evaluaciones de la conformidad de sistemas de IA conforme al Reglamento de IA[13]. Si ese acuerdo no existe, los certificados que emita el organismo de evaluación de la conformidad de ese tercer estado no serán válidos a efectos de demostrar la conformidad del sistema de IA[14].

El listado de organismos notificados para la realización de evaluaciones de la conformidad de los diferentes productos de la legislación europea en los que se exige la intervención de estas entidades es público[15], éste es conocido como sistema de información NANDO[16].

2. Requisitos de los organismos notificados.

En primer lugar, los organismos notificados deberán contar con los medios técnicos, organizativos y humanos necesarios para poder realizar adecuadamente las tareas que se les encomiendan. Por lo que se refiere al personal, estos deben tener experiencia y conocimiento técnico, jurídico y científico respecto de los requisitos esenciales que se exigen a los sistemas de IA en el Reglamento de IA[17].

11 En el siguiente apartado de este trabajo se analiza ese proceso de notificación de los organismos notificados por parte de la autoridad notificante. Véase también los artículos 29 a 30 del Reglamento de IA.

12 Artículo 31.1. Reglamento de IA. Como ha aclarado la jurisprudencia, las personas físicas también pueden llegar a ser organismos notificados si cumplen con los requisitos exigidos por la normativa. STS 2 noviembre 2017. (RJ 2017,4806)

13 Artículo 39. Reglamento de IA.

14 STSJ Madrid 24 noviembre 2011. (Rec. 486, 1997) Fundamento Jurídico 6º.

15 Artículo 35.2. Reglamento de IA.

16 Algunos ejemplos de organismos notificados españoles son: AENOR, BUREAU VERITAS, CNCps, etc. Este listado de organismos notificados junto con los productos y actividades para las que pueden realizar la verificación de la conformidad de las diferentes legislaciones se puede encontrar en la siguiente web: https://webgate.ec.europa.eu/single-market-compliance-space/#/notified-bodies

17 Artículo 31.11. Reglamento de IA.

En segundo lugar, deberán contar con un seguro de responsabilidad adecuado al nivel de riesgo vinculado a las actividades de verificación que llevan a cabo. Como regla general, la responsabilidad de la conformidad de un sistema de IA será atribuible normalmente al fabricante o proveedor que en su caso lo haya puesto en el mercado, incluso cuando haya participado en el proceso de verificación de la conformidad un organismo notificado[18]. No obstante, tal y como ha indicado el TJUE, dado que la intervención del organismo notificado durante el proceso de evaluación de la conformidad tiene como objetivo proteger a los destinatarios finales de los productos que superan tal proceso de verificación, el incumplimiento de sus obligaciones como evaluador puede dar lugar a las correspondientes responsabilidades por los daños causados[19].

En tercer lugar, los organismos notificados deberán actuar con total independencia y objetividad en las actividades que lleven con relación a todas las partes con las que estos organismos se relacionan. Esa exigencia deberá estar especialmente presente respecto de aquellas entidades u organizaciones en las que pueden verse en mayor grado comprometidas las actividades que le ha atribuido el Reglamento de IA a los organismos notificados. Por ejemplo, los proveedores[20], los responsables del despliegue del sistema, la autoridad notificante, la autoridad de vigilancia del mercado, etc.

3. Principales actividades de los organismos notificados. La evaluación de la conformidad.

El Reglamento de IA asigna a los organismos notificados una serie de actividades.

A) Evaluación de la conformidad.

Como ya se ha adelantado previamente, la función principal de los organismos notificados es evaluar que los sistemas de IA se hayan desarrollado conforme a los requisitos exigidos por el Reglamento de IA. No todos los sistemas de IA que se regulan en el Reglamento de IA han de pasar por un proceso de evaluación de la conformidad con presencia de organismo notificado[21]. En este sentido, a una

18 *Guía azul sobre la aplicación de la normativa europea relativa a los productos* de 2022 de la Comisión Europea, pp.78 y ss.

19 STJUE 16 febrero 2017, asunto C219/15. Fundamentos 49 y ss.
Sobre la posibilidad de responsabilidad por parte de un organismo notificado también se han pronunciado nuestros tribunales internos. STS 9 junio 2021. (RJ 2021\3188)
Véase también: Álvarez Lata, N.: "¿Responden los organismos notificados por los daños producidos por los productos auditados por ellos frente a los consumidores? Comentario a la STS, de 18 de enero de 2021", *Cuadernos Civitas de jurisprudencia civil*, 2021, núm. 117, pp. 139-154.

20 Artículo 31.4. Reglamento de IA.

21 Un estudio sobre el proceso de evaluación de la conformidad regulado en el Reglamento de IA puede verse en: Palma Ortigosa, A.: "La evaluación de la conformidad en el diseño y producción de sistemas basados en IA en el contexto del Nuevo Marco Legislativo", en AA.VV.: *Tratado sobre el Reglamento Europeo de Inteligencia Artificial* (dir. por L. Cotino Hueso y P. Simón Castellano), Thomson-Aranzadi, 2024. En prensa.

gran parte de los sistemas de IA considerados de alto riesgo no les requiere la participación de los organismos notificados, sino que dicha evaluación la realiza el propio proveedor que ha desarrollado el sistema de IA[22].

Así, para las finalidades consideradas de alto riesgo a excepción de la identificación biométrica[23], el procedimiento de evaluación de la conformidad consistirá en la propia verificación de los requisitos por parte del proveedor del sistema de IA. Es decir, antes de poner en el mercado el sistema, la propia organización que lo ha desarrollado deberá evaluar su conformidad con el Reglamento de IA.

Por su parte, cuando el sistema de IA tenga como finalidad la identificación biométrica[24], el proveedor del sistema de IA podrá optar entre realizar el mismo la autoevaluación del sistema o solicitar la participación de un organismo notificado. Esta facultad solo se permite en los casos en los que el proveedor haya aplicado normas armonizadas o especificaciones comunes que cubran todos los requisitos del Reglamento de IA en el proceso de desarrollo de su sistema de IA. En caso contrario, el proveedor estará obligado a solicitar que la evaluación de la conformidad la realice un organismo notificado.

A su vez, cuando el sistema de IA sea un producto o un componente de seguridad de un producto sometido a legislación europea que sigue el NML[25], el proveedor deberá llevar a cabo la evaluación de la conformidad prevista en esa legislación europea. En este sentido, como norma general, para la evaluación de estos productos está contemplada la participación de organismos notificados.

Por tanto, en los casos en los que sí que se requiera la participación de organismo notificado, éste deberá llevar a cabo todas las actividades necesarias para verificar que dicho sistema de IA objeto de evaluación cumple con los requisitos del Reglamento de IA y por tanto, puede utilizarse y ponerse en el mercado. En la medida de lo posible, los procesos de evaluación de la conformidad y las tasas aplicadas a estos deberán tener en cuenta el tipo de proveedor del sistema de IA, sobre todo si es una Pyme[26].

22 Véase el artículo 43 del Reglamento de IA.

23 Se consideran finalidades de alto riesgo, entre otras, las siguientes: Infraestructuras críticas, justicia, usos policiales, empleo, gestión de trabajadores, scoring bancario, prestaciones públicas, etc. Véase apartados 2 a 8 del Anexo III. Reglamento de IA.

24 Apartado 1 del Anexo III.

25 Entre otros productos, entre otros: juguetes, ascensores, embarcaciones de recreo, máquinas, productos sanitarios, etc. Anexo I del Reglamento de IA.

26 Artículos 62.2 y 34.2. Reglamento de IA. Véase también el artículo 11.1 de esta misma norma con relación a la solicitud simplificada a la que pueden acogerse los proveedores que sean Pymes durante el proceso de evaluación de la conformidad con presencia de organismo notificado.

El proceso de evaluación de la conformidad con presencia de organismo notificado está regulado en el artículo 43 y en el Anexo VII del Reglamento de IA[27].

Corresponde a los proveedores de los sistemas de IA presentar la correspondiente solicitud de evaluación ante el organismo notificado que consideren oportuno. Éste último llevará a cabo todas las actividades necesarias para verificar el cumplimiento del sistema de IA con el Reglamento. Estas actividades comprenderán entre otras la calibración, ensayos, certificaciones, inspecciones, comprobación de documentación técnica, etc[28].

Superado el proceso de evaluación de la conformidad, los organismos notificados expedirán el correspondiente certificado que habilita a los proveedores a poner en el mercado su sistema de IA. En caso contrario, el organismo notificado emitirá una resolución motivada indicando las razones por las que considera que el sistema de IA no ha superado la evaluación. Esta denegación puede ser recurrida en virtud del procedimiento que se regule al efecto[29].

El certificado emitido por un organismo notificado tiene validez en toda la UE[30] durante un periodo no superior a cinco años para los sistemas de IA que sean considerados productos de alto riesgo y de cuatro años para los sistemas de IA que se utilicen con una finalidad considerada de alto riesgo[31].

B) Otras actividades.

Junto a la evaluación de la conformidad, corresponde al organismo notificado otras funciones y obligaciones.

En primer lugar, está obligado a colaborar con las autoridades públicas que le requieran información y documentos sobre los proveedores y sistemas de IA que han evaluado. Esta colaboración ha de ser tanto activa como reactiva. A modo de ejemplo, de forma pro activa los organismos notificados han de informar a la autoridad notificante de los certificados que hayan podido restringir, retirar o no aceptar[32]. De forma reactiva, siempre que una autoridad pública le solicite documentos o información, estos organismos han de colaborar con las Administraciones Públicas.

27 Este proceso queda integrado por dos grandes actividades de verificación. La evaluación del sistema de gestión de la calidad y la evaluación de la documentación técnica. Anexo VII.

28 *Guía azul sobre la aplicación de la normativa europea relativa a los productos* de 2022 de la Comisión Europea, p.75.

29 Artículo 44.3 del Reglamento de IA.

30 STJCE 30 abril 2009, asunto C-132/08. Fundamentos 26 y ss. También en: STSJ Madrid 21 julio 2009. (JUR 2009\455104). Fundamento Jurídico 4.

31 Artículo 44.2 del Reglamento de IA.

32 Artículo 45 del Reglamento de IA.

En segundo lugar, los organismos notificados participarán en las diferentes actividades de coordinación que fomenten las autoridades públicas con otros organismos notificados y organizaciones europeas de normalización[33]. En este sentido, suelen crearse distintos grupos de organismos notificados en función de la legislación que estos cubren[34]. En estos grupos suelen participar integrantes de los Estados Miembros, de la Comisión Europea y de organizaciones europeas de normalización.

En tercer lugar, los organismos notificados deben informar de diferentes cuestiones a los proveedores de los sistemas de IA que hayan evaluado. Entre otras, el cese voluntario de sus funciones como organismo notificado, la retirada o suspensión de la designación como organismo notificado emitida por una autoridad pública, etc[35].

En cuarto lugar, los organismos notificados también han de informar al resto de organismos notificados de diferentes cuestiones tanto de forma proactiva como a solicitud del resto de organismos notificados. Por un lado, los organismos notificados informarán por defecto de los certificados que hayan retirado, rechazado o suspendido sobre el sistema de gestión de la calidad o la documentación técnica. Ello tiene sentido, ya que esta información puede servir a modo de advertencia para el resto de los organismos notificados a los que se puede dirigir posteriormente un determinado proveedor de un sistema de IA cuyo sistema no ha superado la evaluación de la conformidad o ha visto suspendido o retirado su certificado previamente concedido. Por otro lado, a petición de otro organismo notificado, estos estarán obligados a informar también de los certificados que hayan expedido sobre las materias previamente mencionadas.

3. Los organismos notificados de los distintos tipos de sistemas de IA del Reglamento de IA.

Como se ha señalado anteriormente, la presencia del organismo notificado solo está contemplada cuando se pretenda llevar a cabo la evaluación de la conformidad de determinados sistemas de IA. Estos son, cuando el sistema de IA tenga como finalidad la identificación biométrica y cuando el sistema de IA sea un producto o componente de seguridad de un producto que esté sometido a la legislación que sigue la estructura del NML.

33 Artículo 31.12 y 38 del Reglamento de IA.

34 A modo de ejemplo, en materia de productos sanitarios existe el Grupo de Coordinación de Productos Sanitarios (MDCG).

35 Artículo 36.5 del Reglamento de IA.

A) Los organismos notificados de los productos o componentes de seguridad de productos que sean sistemas de IA.

El Reglamento de IA establece que los organismos notificados que han sido autorizados para realizar la evaluación de la conformidad de los productos sometidos a los actos legislativos que siguen el NML disponen de la facultad para verificar la conformidad de los requisitos del Reglamento de IA cuando dicho producto sea un sistema de IA[36]. A modo de ejemplo, un organismo que ha sido notificado para realizar evaluaciones de la conformidad de un juguete en virtud de la legislación de ese producto[37], tiene también la facultad de ser el que lleve a cabo las evaluaciones de conformidad de ese juguete cuando éste lleve integrado un sistema de IA.

En estos supuestos, el organismo notificado no sólo deberá disponer del personal y medios necesarios para poder llevar a cabo evaluaciones de conformidad de juguetes, sino también de sistemas de IA[38].

Resulta inicialmente lógico pensar que el organismo notificado que ya cuenta con la estructura y los medios adecuados para realizar evaluaciones de conformidad de un ascensor o un producto sanitario sea el más indicado para realizar evaluaciones de conformidad de esos mismos productos, agregando el elemento diferencial de que tales productos llevan integrados un sistema de IA. En este sentido, el proceso de evaluación de la conformidad de estos sistemas de IA deberá seguir la estructura marcada por la evaluación de la conformidad establecida en la legislación del producto o componente de seguridad del producto en el que se integra dicho sistema de IA[39].

El Reglamento de IA permite a los organismos notificados que subcontraten o creen filiales para realizar las labores de verificación de los requisitos del Reglamento de IA[40]. Esta posibilidad abre la puerta a que los organismos notificados de productos o componentes de seguridad de productos sometidos a legislación que siguen el NML expandan sus procesos de verificación a sistemas de IA.

Dicho lo cual, nada impide que otros organismos notificados distintos a los que vinieran realizando evaluaciones de conformidad de productos o componentes de seguridad de productos pueda evaluar la conformidad de sistemas de IA y productos siempre que cumplan los requisitos de ambas legislaciones.

36 Artículo 43.3 del Reglamento de IA.

37 Véase el Real Decreto 1205/2011, de 26 de agosto, sobre la seguridad de los juguetes y la Directiva 2009/48/CE del Parlamento Europeo y del Consejo, de 18 de junio de 2009, sobre la seguridad de los juguetes.

38 Apartados 4, 9 y 10 del artículo 31 del Reglamento de IA.

39 Artículo 43.3 del Reglamento de IA.

40 Artículo 33 del Reglamento de IA.

B) Los organismos notificados de los sistemas de identificación biométrica. El futuro papel de la AESIA.

De acuerdo con el artículo 43.1 del Reglamento de IA, la evaluación de la conformidad de los sistemas que tengan como finalidad la identificación biométrica, cuando no estén prohibidos, se deberá llevar a cabo con la presencia de un organismo notificado si no se han utilizado normas armonizadas o especificaciones comunes que cubran los requisitos esenciales del Reglamento de IA.

Como es lógico, actualmente no existen organismos notificados designados para llevar a cabo las evaluaciones de conformidad de estos sistemas de IA. Los futuros organismos notificados como ya hemos indicado podrán pertenecer al sector privado y al público.

Un modelo que puede resultar interesante replicar sobre el papel de los organismos notificados públicos es el que lleva ya años implantado por parte de la Agencia Española del Medicamento y Productos Sanitarios (AEMPS). En este sentido, el Centro Nacional de Certificación de Productos Sanitarios (CNCps) es el único organismo notificado designado para realizar evaluaciones de la conformidad de productos sanitarios[41]. Se trata de un órgano administrativo adscrito a la AEMPS[42].

Este modelo ha permitido focalizar todas las evaluaciones de conformidad que se realizan en nuestro país sobre productos sanitarios en este organismo notificado tanto de fabricantes nacionales como extranjeros[43], en parte atraídos supuestamente por las tarifas más reducidas que ofrece este organismo notificado respecto de otros del sector privado en otros Estados miembros.

Podría resultar interesante que uno de los organismos notificados que pueda ser competente para evaluar los sistemas de identificación biométrica sea público y en su caso se adscriba a la Agencia Española de Supervisión de Inteligencia Artificial (AESIA).

Ello permitiría que un organismo notificado público fuera el encargado de llevar a cabo las evaluaciones de conformidad de los sistemas de IA de finalidad biométrica, lo que habilitaría a un control previo por parte de un organismo público de la certificación de estos sistemas que se consideran de alto riesgo y cuyo uso ha despertado fuertes críticas por los riesgos que estos pueden generar.

41 Organismo Notificado 0318. Más información en: https://certificaps.gob.es/

42 Artículo 30.3. Real Decreto 1275/2011, de 16 de septiembre, por el que se crea la Agencia estatal "Agencia Española de Medicamentos y Productos Sanitarios" y se aprueba su Estatuto.

43 Para más información véase: *Memoria anual 2022* del Centro Nacional de Certificación de Productos Sanitarios: Organismo Notificado 0318 y entidad acreditada para la certificación norma en ISO 13485, p.24.

Sin lugar a duda, esta decisión política requeriría de fuertes inversiones para dotar a este organismo público del personal y los medios adecuados y competentes para llevar a cabo y de forma competitiva con el sector privado este tipo de evaluaciones[44].

Actualmente el estatuto de la AESIA no contempla la posibilidad de que alguno de sus órganos o departamentos puedan ejercer actividades como organismo notificado, de ahí que, si se pretende replicar el modelo que ha adoptado la AEMPS, será necesario modificar los estatutos actuales de la AESIA[45]. Por un lado, debería reconocerse la competencia de la AESIA para llevar a cabo evaluaciones de la conformidad y por otro lado asignar a un departamento u órgano específico la realización de éstas[46].

Dicho lo cual, es importante destacar que debe quedar clara la independencia entre la AESIA y el organismo encargado de realizar las evaluaciones de la conformidad. En este sentido, la AEMPS en su momento tuvo que alterar sus estatutos para asegurar cierta independencia entre ésta y el CNCps, ya que así se exige tanto en la normativa europea que regula los productos sanitarios como en las normas que configuran el NML[47]. En este sentido, el Consejo de Estado no consideró suficiente el cambio realizado, al entender que no existía la independencia requerida por la normativa europea[48], sin embargo, ni la autoridad notificante (Ministerio de Sanidad) ni la Comisión Europea y los Estados Miembros plantearon problemas a esta designación[49].

Tal independencia es necesaria debido a que ese hipotético organismo notificado evaluará sistemas diseñados tanto por el sector privado como por el sector público, cualquier injerencia podría afectar al proceso de evaluación de los sistemas de IA y, por ende, en casos de errores de tales sistemas por una incorrecta verificación ex ante, a los derechos de los ciudadanos ex post.

C) Los organismos notificados obligatorios para finalidades de identificación biométrica por parte de determinadas autoridades públicas.

44 Por ejemplo, el CNCps cuenta con un total de 31 trabajadores y trabajadores especializados en este ámbito. Más información en: https://certificaps.gob.es/quienes-somos/

45 Real Decreto 729/2023, de 22 de agosto, por el que se aprueba el Estatuto de la Agencia Española de Supervisión de Inteligencia Artificial.

46 Así se contempla en los Estatutos de la AEMPS en sus artículos 7.30 y 35.bis.1.a) del Real Decreto 1275/2011, de 16 de septiembre, por el que se crea la Agencia estatal "Agencia Española de Medicamentos y Productos Sanitarios" y se aprueba su Estatuto.

47 Véase el Anexo VII. 1.2.6 del Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, sobre los productos sanitarios, por el que se modifican la Directiva 2001/83/CE, el Reglamento (CE) n.º 178/2002 y el Reglamento (CE) n.º 1223/2009 y por el que se derogan las Directivas 90/385/CEE y 93/42/CEE del Consejo.

48 Dictamen de 24 de marzo de 2022. Consejo de Estado.

49 Como hemos señalado anteriormente, el CNCps fue notificado el 14 de julio de 2022. Más información, véase la web de la AEMPS.

En términos generales, los proveedores tienen libertad para elegir el organismo notificado que consideren oportuno a la hora de someter su sistema de IA a la evaluación de la conformidad, siempre claro está, que dicho organismo haya sido notificado para realizar evaluaciones de conformidad de los requisitos del Reglamento de IA.

Dicho lo cual, se establecen algunos supuestos donde los proveedores tienen limitada su capacidad de elección en función del sistema de IA que hayan desarrollado y la finalidad de este.

En primer lugar, para aquellos casos en los que se utilice un sistema de IA con la finalidad de identificación biométrica por parte de las autoridades en aplicación de la ley o las autoridades de inmigración se prevé un organismo notificado específico. De acuerdo con el Reglamento de IA, las autoridades en aplicación de la ley son aquellas que realizan actividades para la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales o la ejecución de sanciones penales, entre otras[50]. Entendemos que este concepto abarca entre otras a las fuerzas y cuerpos de seguridad, las administraciones penitenciarias, las autoridades judiciales del ámbito penal o el Ministerio Fiscal.

Para estos supuestos, el organismo notificado será o bien la autoridad de control en virtud de la normativa de protección de datos, o bien una autoridad pública suficientemente independiente[51].

Para las fuerzas y cuerpos de seguridad posiblemente el organismo notificado acabe siendo la AEPD, ya que es la autoridad de protección de datos competente para el tratamiento de datos en virtud de la Directiva de datos con fines policiales[52] y además goza de un grado de independencia respecto del Gobierno central muy relevante[53]. No tenemos claro que ocurrirá para el caso de las autoridades judiciales en el ámbito penal, ya que la AEPD no es la competente para el tratamiento de los datos en el ámbito judicial, sino el CGPJ[54], de ahí que es posible que sea un órgano administrativo del Ministerio de Justicia el que acabe siendo el organismo notificado en estos casos.

50 Artículo 3.46 del Reglamento de IA.

51 Véase los artículos 43.1 párrafo último y 74.8 del Reglamento de IA.

52 Artículo 74.8. Reglamento de IA.

53 La AEPD se ha configurado como una autoridad administrativa independiente. Se trata de un tipo de entidades del sector público instrumental que más grado de independencia tienen respecto de las Administraciones Públicas territoriales. Artículo 109 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

54 Concretamente a la Dirección de Supervisión y Control de Protección de Datos del Consejo General del Poder Judicial. Artículo 236. Nonies. Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

Ahora bien, tanto para el caso de las fuerzas y cuerpos de seguridad, como para el caso de las autoridades judiciales penales, no creemos que algún órgano integrante de la AESIA pueda llegar a considerarse organismo notificado de estos sistemas ya que la estructura y funciones asignadas a esta autoridad no alcanza el nivel de independencia que exige el Reglamento de IA para estas autoridades en este contexto específico, nivel de independencia que no sólo requeriría la modificación de sus estatutos actuales, sino también de la ley de creación de esta Agencia[55].

En segundo lugar, cuando un proveedor de un sistema de IA tenga como finalidad la identificación biométrica y tal sistema se prevea su puesta en servicio por parte de instituciones o agencias de la UE, el organismo notificado será el Supervisor Europeo de Protección de Datos[56].

III. AUTORIDAD NOTIFICANTE.

1. Concepto de autoridad notificante.

La autoridad notificante es la responsable de establecer y llevar a cabo los procedimientos necesarios para la evaluación, la designación y la notificación de los organismos de evaluación de la conformidad, así como de su supervisión[57].

La autoridad notificante es la autoridad pública ante la cual un organismo de evaluación de la conformidad es notificado (autorizado) [58], y por ende, pasa a considerarse organismo notificado de una legislación específica, en nuestro caso, el Reglamento de IA. Es decir, una vez que ese organismo es notificado, éste puede llevar a cabo evaluaciones de conformidad de sistemas de IA.

Corresponde a los Estados miembros decidir el número de autoridades notificantes, debiendo existir al menos una por país[59]. Como regla general, las autoridades notificantes que han sido designadas conforme otras legislaciones

55 Actualmente la AESIA es una Agencia Estatal que depende en gran medida del Gobierno Central, a diferencia de una autoridad independiente. D.A 130. Ley 22/2021, de 28 de diciembre, de Presupuestos Generales del Estado para el año 2022 y Real Decreto 729/2023, de 22 de agosto, por el que se aprueba el Estatuto de la Agencia Española de Supervisión de Inteligencia Artificial.

56 Artículo 74.9 del Reglamento Europeo de IA.

57 Artículo 3.19 Reglamento de IA.

58 Organismo de evaluación de la conformidad: un organismo independiente que desempeña actividades de evaluación de la conformidad, como el ensayo, la certificación y la inspección. Artículo 3.21. Reglamento de IA.

59 Artículo 28.1 y 70.1 del Reglamento de IA.

que siguen el NML son actualmente Direcciones Generales o Subdirecciones Generales integradas dentro de un Ministerio determinado[60].

Teniendo en cuenta que en virtud del Reglamento de IA pueden existir diferentes organismos notificados en función del sistema de IA, es posible que también puedan existir diferentes autoridades notificantes para notificar y designar en función del ministerio que asuma las potenciales competencias.

Dicho lo cual, tendría sentido que al menos existiera una autoridad notificante que coordine al resto de autoridades notificantes que puedan estar presentes para los diferentes ámbitos donde operen los sistemas de IA. Pensamos que esa autoridad notificante central en España para el cumplimiento del Reglamento de IA sería algún órgano administrativo del Ministerio de Transformación Digital, ya que es este último que tiene asignadas las competencias en materia de inteligencia artificial[61].

Estas autoridades notificantes deberán organizarse de forma que las decisiones relativas a la notificación serán adoptadas por personas competentes distintas a las que realizaron la evaluación de los organismos de evaluación de la conformidad. Al igual que se exigía para los organismos notificados, el personal de las autoridades notificantes deberá ostentar conocimientos especializados en ámbitos como la tecnología de la información, la inteligencia artificial y los derechos fundamentales[62].

2. Funciones de la autoridad notificante.

A la hora de llevar a cabo las actividades asignadas, la autoridad notificante no podrá ejercer ninguna actividad que efectúen los organismos notificados. Además, deberán evitar cualquier conflicto de intereses que pueda surgir entre los organismos de evaluación de la conformidad y éstas. Se pretende conseguir que la evaluación y notificación de los organismos de evaluación de la conformidad se realice de la forma más objetiva posible por parte de la autoridad notificante.

Entre las funciones que se asignan a la autoridad notificante cabe destacar el proceso de notificación de organismos de evaluación de la conformidad.

A) La notificación de organismos de evaluación de la conformidad.

60 El listado completo de autoridades notificantes se puede consultar en: https://webgate.ec.europa.eu/single-market-compliance-space/#/notified-bodies/notifying-authorities?filter=countryId:724

61 Es muy posible que ese órgano administrativo sea la Secretaría de Estado para la Digitalización y la Inteligencia Artificial o alguna de sus direcciones o subdirecciones inferiores. Estas son: Dirección General de Digitalización e Inteligencia Artificial y dentro de ésta última la Subdirección General de Inteligencia Artificial y Tecnologías Habilitadoras Digitales. Real Decreto 210/2024, de 27 de febrero, por el que se establece la estructura orgánica básica del Ministerio para la Transformación Digital y de la Función Pública.

62 Artículo 28.7 Reglamento de IA.

A través de la notificación, la autoridad notificante comprueba que una organización que realiza evaluaciones de conformidad cuenta con los medios y recursos necesarios para llevar a cabo evaluaciones de conformidad de sistemas de IA de acuerdo a los requisitos exigidos por el Reglamento de IA.

Para que un organismo de evaluación de la conformidad pase a considerarse notificado del Reglamento de IA se deberá seguir un procedimiento específico.

En primer lugar, corresponde al organismo de evaluación de la conformidad presentar ante la autoridad notificante una solicitud de notificación. En esta solicitud se indicarán el módulo o módulos de evaluación de la conformidad y tipos de sistemas de IA para los cuales considera que tiene los medios para llevar a cabo tal proceso de evaluación de la conformidad previsto en el Reglamento de IA. Se deberá aportar además un certificado de acreditación[63] por parte de ENAC que certifique que el organismo de evaluación de la conformidad cumple con los requisitos para ser organismo notificado en virtud del Reglamento de IA[64]. En el caso de que no se aporte el certificado de ENAC, el organismo de evaluación de la conformidad deberá aportar los documentos y pruebas que justifiquen el cumplimiento de los requisitos exigidos por el Reglamento de IA para ser organismo notificado.

En segundo lugar, una vez que la autoridad notificante compruebe que se cumplen todos los requisitos, esta autoridad notificará a la Comisión y a los demás Estados miembros tal situación. Si la autoridad notificante no considera que se dan los requisitos, denegará la designación como organismo notificado. En estos casos habrá que estar al procedimiento administrativo que cada Estado miembro configure[65].

En tercer lugar, en caso favorable, remitida esa información por parte de la autoridad notificante, tanto la Comisión como los Estados miembros disponen del plazo de dos semanas para plantear las objeciones que estimen oportunas sobre la notificación. Si en el plazo de dos semanas no se plantean objeciones, el

63 Artículo 29.2 del Reglamento de IA.

64 El organismo nacional de acreditación en España es ENAC. Artículo 1. Real Decreto 1715/2010, de 17 de diciembre, por el que se designa a la Entidad Nacional de Acreditación (ENAC) como organismo nacional de acreditación de acuerdo con lo establecido en el Reglamento (CE) nº 765/2008 del Parlamento Europeo y el Consejo, de 9 de julio de 2008, por el que se establecen los requisitos de acreditación y vigilancia del mercado relativos a la comercialización de los productos y por el que se deroga el Reglamento (CEE) nº 339/93.

65 Por ejemplo, en el ámbito del sector de las telecomunicaciones opera el silencio administrativo negativo si en el plazo de 6 meses desde que se planteó la solicitud la autoridad notificante no contesta. Se habilita al fabricante para la interposición del recurso de reposición o en su caso acudir directamente a la vía judicial. Apartados 6 y 7 del artículo 27. Real Decreto 188/2016, de 6 de mayo, por el que se aprueba el Reglamento por el que se establecen los requisitos para la comercialización, puesta en servicio y uso de equipos radioeléctricos, y se regula el procedimiento para la evaluación de la conformidad, la vigilancia del mercado y el régimen sancionador de los equipos de telecomunicación.

proceso de notificación se entenderá resuelto y el organismo de evaluación de la conformidad pasará a ser considerado organismo notificado de los módulos y sistemas de IA para los cuales haya sido validado. La Comisión le asignará un número de identificación a ese organismo notificado[66].

B) Modificaciones de las notificaciones.

Durante el transcurso de las actividades que llevan a cabo los organismos notificados es posible que surjan diferentes situaciones que pueden llevar a la alteración de la notificación inicial para la cual fueron designados. El Reglamento de IA contempla distintos procedimientos en los que participan esencialmente la autoridad notificante y los organismos notificados, estos son los siguientes.

En primer lugar, cuando el organismo notificado pretenda ampliar al ámbito de aplicación de su notificación, éste deberá plantear una nueva solicitud a la autoridad notificante y seguir el procedimiento previamente explicado en el apartado anterior, es decir, el de la solicitud de notificación. Esto ocurriría cuando dicho organismo notificado quiera por ejemplo aumentar la tipología de sistemas de IA que pretende verificar.

En segundo lugar, cuando un organismo notificado pretenda poner fin a sus actividades de evaluación de la conformidad, éste deberá de informar a la autoridad notificante y a los proveedores. En estos supuestos, los certificados que haya emitido podrán ser válidos durante al menos nueve meses después del cese de las actividades siempre que otro organismo notificado asuma la responsabilidad de los sistemas de IA cubiertos por dichos certificados.

En tercer lugar, la notificación también puede variar cuando la autoridad notificante llegue a la conclusión de que el organismo notificado no cumple con los requisitos exigidos para éstos por parte del Reglamento de IA. En estos supuestos, esta autoridad limitará, suspenderá o retirará la designación de dicho organismo notificado. De ello se deberá informar a la Comisión y a los Estados Miembros. En función de si se limita, se suspende o se retira la designación, los certificados emitidos por el organismo notificado se mantendrán más o menos tiempo[67].

En cuarto lugar, cuando la Comisión determine que un organismo notificado no cumple o ha dejado de cumplir los requisitos para su notificación, informará al Estado miembro donde haya sido notificada y obligará a éste a que lleve a cabo las medidas correctoras para corregir esta situación.

66 Artículos 30.4 y 35.1 del Reglamento de IA. Los proveedores están obligados a señalar el código del organismo notificado que haya evaluado su sistema de IA junto con el Marcado CE. Esta obligación no existe cuando el proveedor simplemente haya acudido de forma voluntaria a dicho organismo notificado. STJUE 11 julio 2018, asunto C-192/17. Fundamento 50.

67 Artículo 36. Reglamento de IA.

IV. CONCLUSIONES.

El Reglamento de IA es la primera norma a nivel europeo que trata de afrontar los principales riesgos que generan los sistemas de inteligencia artificial. Para ello contempla toda una serie de reglas que pretenden asegurar que un sistema de IA que se pone en el mercado es seguro y confiable. El Reglamento de IA sigue la estructura marcada por el Nuevo Marco Legislativo. Este modelo lleva ya años aplicándose a diferentes productos como puede ser la maquinaria o los productos sanitarios. El legislador europeo ha considerado adecuado replicar este modelo para regular el desarrollo y despliegue de los sistemas de IA. Será por tanto un reto para las instituciones europeas y los Estados miembros la aplicación adecuada de este modelo al diseño y uso de sistemas de IA.

Entre los mecanismos que se establecen para alcanzar ese objetivo se configuran varias entidades que tienen un papel esencial durante el despliegue y sobre todo en el diseño de los sistemas de IA. Esas entidades son la autoridad notificante y los organismos notificados.

Los organismos notificados son las entidades encargadas de llevar a cabo las evaluaciones de la conformidad de los sistemas de IA antes de éstos que se puedan utilizar. Por su parte, las autoridades notificantes son las autoridades públicas encargadas de evaluar y designar a los organismos notificados.

Ambas organizaciones son piezas esenciales en el puzle que ha desarrollado el Reglamento de IA.

BIBLIOGRAFÍA

Álvarez García, V.: *Industria*, Iustel, 2010.

Álvarez Lata, N.: "¿Responden los organismos notificados por los daños producidos por los productos auditados por ellos frente a los consumidores? Comentario a la STS, de 18 de enero de 2021", *Cuadernos Civitas de jurisprudencia civil*, 2021, núm. 117.

Bernárdez García, B.: "El papel de los organismos de control en el aseguramiento de la seguridad industrial", *Economía industrial,* 2015, núm. 396.

Guía azul sobre la aplicación de la normativa europea relativa a los productos de 2022 de la Comisión Europea.

ISO/IEC 17000:2004. Conformity assessment — Vocabulary and general principles.

Memoria anual 2022 del Centro Nacional de Certificación de Productos Sanitarios: Organismo Notificado 0318 y entidad acreditada para la certificación norma en ISO 13485.

Palma Ortigosa, A.: "La evaluación de la conformidad en el diseño y producción de sistemas basados en IA en el contexto del "Nuevo Marco Legislativo", en AA.VV.: *Tratado sobre el Reglamento Europeo de Inteligencia Artificial* (dir. por L. Cotino Hueso y P. Simón Castellano), Thomson-Aranzadi, 2024.

METAVERSO, VIOLENCIA DE GÉNERO Y ORDEN DE ALEJAMIENTO VIRTUAL*

METAVERSE, GENDER-BASED VIOLENCE AND VIRTUAL RESTRAINING ORDER

Actualidad Jurídica Iberoamericana Nº 21, agosto 2024, ISSN: 2386-4567, pp. 618-643

* Como asistente de estilo y corrección gramatical del presente trabajo se ha hecho uso de la herramienta de IA ChatGPT-4o, desarrollada por OpenAI. Los análisis exploratorios, reflexiones y recomendaciones son exclusivas de sus autoras.

Elisa SIMÓ SOLER y Hernán LÓPEZ HERNÁNDEZ

ARTÍCULO RECIBIDO: 4 de marzo de 2024
ARTÍCULO APROBADO: 18 de abril de 2024

RESUMEN: El metaverso, como espacio digital tridimensional e interconectado, plantea desafíos jurídicos significativos que exigen una reflexión sobre la posible adaptación del marco legal destinada a mantener un equilibrio entre la innovación tecnológica y la seguridad de las personas usuarias. El artículo explora la extrapolación de las órdenes de alejamiento al metaverso, un entorno virtual donde la estructura espacio-temporal se diluye y la creación de múltiples identidades es facilitada a través de Inteligencia Artificial. Se propone en el supuesto de hecho de la violencia contra las mujeres, un fenómeno que muta y hace uso de los desarrollos tecnológicos para ejercer control. Poder formular propuestas regulativas eficaces exige una comprensión en profundidad de las dinámicas del metaverso, de sus potencialidades y sus límites, con el fin de anticipar futuros escenarios que permitan reconsiderar la respuesta judicial frente a estos nuevos escenarios en los ordenamientos chileno y español.

PALABRAS CLAVE: Metaverso; Inteligencia Artificial; orden de Alejamiento; violencia de género.

ABSTRACT: *The metaverse, as a three-dimensional and interconnected digital space, presents significant legal challenges that require a reflection on the possible adaptation of the legal framework to maintain a balance between technological innovation and user safety. This article explores the extrapolation of restraining orders to the metaverse, a virtual environment where the spatiotemporal structure is diluted, and the creation of multiple identities is facilitated through Artificial Intelligence. In the context of violence against women, a phenomenon that evolves and utilizes technological developments to exert control, effective regulatory proposals necessitate a deep understanding of the dynamics of the metaverse, its potential, and its limitations. This understanding is crucial to anticipate future scenarios that allow for reconsideration of judicial responses to these new situations within the Chilean and Spanish legal systems.*

KEY WORDS: *Metaverse; Artificial Intelligence; restraining order; gender violence.*

I. INTRODUCCIÓN.

El metaverso, una convergencia revolucionaria de mundos virtuales, realidad aumentada y espacios digitales interconectados, está emergiendo como un eje central en la confluencia de la tecnología y la sociedad. Originado en la ciencia ficción, este concepto se ha materializado gracias a avances tecnológicos exponenciales, convirtiéndose en una realidad palpable que promete transformar radicalmente la manera en que interactuamos, trabajamos y vivimos.

El término "metaverso" alude a un universo digital persistente, accesible y escalable que coexiste con el mundo físico, ofreciendo experiencias inmersivas que trascienden las limitaciones espaciales y temporales.

De acuerdo con Martínez-Blass: "El metaverso es una evolución de Internet que nos muestra la información plana, en 2D, dentro de un navegador o una aplicación. Por tanto, el metaverso es un nuevo Internet Tridimensional (3D) en el que sentimos presencia gracias a los visores virtuales con los que accedemos a él. Dentro de este escenario virtual, podemos andar, interactuar, hablar, etc. e incluso sentir que somos parte de la acción, pero la gran diferencia con el anterior concepto de Internet es que aquí hacemos actividades, pertenecemos a un mundo que se despliega ante nosotros y que es susceptible de ser modificado según nuestras actuaciones"[1].

La relevancia de esta tecnología no solo se ancla en su capacidad de redefinir el entretenimiento y la interacción social, sino que también, se posiciona como una tecnología disruptiva dentro de la Cuarta Revolución Industrial. Expertas como Barona Vilar, señalan que: "La Cuarta Revolución Industrial llega en un momento histórico, político y económico, como sucediera en las tres revoluciones industriales anteriores… subrayando la idea que… La sociedad analógica fue dando paso poco

1 Martínez-Blass, E.: *Metaverso: pioneros en un viaje más allá de la realidad*, LID Editorial, Madrid, 2022, p.13.

• Elisa Simó Soler
Profesora Ayudante Doctora de Derecho procesal, Universitat de València: elisa.simo@uv.es

• Hernán López Hernández
Profesor Ayudante Módulo Jean Monnet: IA y Derecho Privado Europeo, Universidad Autónoma de Chile y Doctorando en programa de Sostenibilidad y Paz en la Era Posglobal, Universitat de València: hernan.lopez@uautonoma.cl

a poco al mundo digital, con la aparición del internet y la transformación digital, que favoreció el impulso de mejora de los procesos operativos empresariales, amén de generar nuevos modelos de negocio"[2].

Esta tecnología, tiene un potencial para remodelar sectores como la educación, el comercio, las finanzas, la propiedad virtual, incluso el intercambio distópico y más pertinente para esta discusión, el ámbito legal.

Desde una perspectiva jurídica, el metaverso -y también multiversos[3]- plantea retos dogmáticos y casuísticos inéditos y amplifica problemáticas preexistentes, demandando un análisis meticuloso y una reflexión profunda. La naturaleza inmaterial y descentralizada[4] del metaverso desafía los paradigmas legales tradicionales[5], cuestionando nociones establecidas de jurisdicción, propiedad, identidad y privacidad. La interacción en multiversos, la propiedad de activos digitales[6], la autenticación de identidades y la gestión de datos personales son solo algunos de los aspectos que requieren una reevaluación normativa y doctrinal en la era del metaverso.

En este contexto, es conveniente que el Derecho, como regulador social y facilitador de la coexistencia pacífica, aborde estas cuestiones emergentes de

2 Barona Vilar, S.: "Cuarta revolución industrial (4.0.) o ciberindustria en el proceso penal: revolución digital, inteligencia artificial y el camino hacia la robotización de la justicia", *Revista Jurídica Digital UANDES*, 2019, vol. 3, núm. 1, p. 2.

3 Los multiversos se refieren a la teoría de que existen múltiples universos además del nuestro, cada uno con sus propias leyes físicas. Esta idea se sostiene en dos pilares principales: la inflación cósmica y la mecánica cuántica. Según la inflación cósmica, tras el Big Bang, el universo experimentó una rápida expansión que pudo haber creado diversas "burbujas" o regiones dentro del espacio-tiempo, cada una convirtiéndose en un universo separado. La mecánica cuántica añade que cada evento cuántico con múltiples posibilidades puede generar universos paralelos, donde cada uno sigue una de las posibles ramas del evento.

4 Explicado de forma breve según OpenSea, uno de los sitios más icónicos de intercambio sobre esta base tecnológica, define la cadena de bloques, o blockchain, como un sistema de registro digital descentralizado que almacena datos en bloques vinculados cronológicamente. Cada bloque contiene un conjunto de transacciones que, una vez completado, se vincula al bloque anterior en la cadena, formando un libro de registros inmutable y permanente. Este proceso asegura la integridad y la verificabilidad de los registros sin necesidad de una autoridad central, lo que diferencia a la blockchain de las bases de datos tradicionales que suelen estar centralizadas y controladas por una sola entidad. Para más información, ver la web oficial de OpenSea disponible en: https://opensea.io/learn/blockchain/what-is-blockchain, visitado el día 10 de mayo de 2024.

5 El metaverso presenta desafíos legales notables, especialmente en áreas como la propiedad intelectual, la privacidad, y la jurisdicción. Por ejemplo, las creaciones dentro del metaverso podrían ser únicas o replicar elementos del mundo real, planteando preguntas sobre los derechos de autor. Además, las interacciones en el metaverso podrían involucrar datos personales sensibles, cuya protección y jurisdicción pueden no estar claramente definidas por las leyes actuales.

6 Citamos como ejemplo la noticia de que Microsoft ha anunciado la compra de Activision Blizzard por aproximadamente $70.000 millones, la mayor adquisición en la historia de la compañía y de la industria de videojuegos, con el objetivo de liderar el desarrollo del metaverso, un universo digital paralelo que podría representar el futuro de internet. Esta transacción destaca la importancia de las inversiones estratégicas en el metaverso, ya que integra populares títulos de videojuegos a la plataforma Xbox y posiciona a Microsoft para capitalizar el mercado emergente, estimado en $800.000 millones para 2024. Las grandes tecnológicas como Meta, Apple y Amazon también están invirtiendo fuertemente en este campo, anticipando que la creación de espacios virtuales y las mejoras en hardware serán cruciales para dominar este nuevo terreno digital. Noticia completa disponible en: https://www.bbc.com/mundo/noticias-60075400, visitado el día 20 de mayo de 2024.

manera proactiva. No solo para salvaguardar derechos y libertades fundamentales, sino también para fomentar un ambiente propicio para la innovación y el desarrollo de este nuevo horizonte digital. Así, la relevancia del metaverso en el ámbito legal radica en las incógnitas que plantea y en las oportunidades que ofrece para repensar y renovar el marco jurídico, adaptándolo a las exigencias de una realidad cada vez más digitalizada e interconectada.

Es esta conexión online prácticamente permanente y naturalizada la que han aprovechado algunos hombres para ejercer violencia contra las mujeres a través de las tecnologías de la información y la comunicación (TIC). La creciente incidencia de la violencia en plataformas digitales ha llevado a un reconocimiento de la necesidad de extender la protección legal a estos espacios. En este sentido, parece razonable pensar que si las condiciones en las que se produce la violencia exigen adoptar medidas que impidan el contacto entre dos sujetos en el mundo físico, esas prohibiciones deben poder ser pensadas y en su caso darse también en el metaverso. Surge entonces la base de la discusión de este artículo: la viabilidad de la extrapolación de la orden de alejamiento al metaverso.

Conscientes del avance acelerado de estos nuevos entornos, desde un ejercicio de prospectiva jurídica se pretenden identificar problemáticas, alejadas de alarmismos y posicionamientos tecnófobos, para poder ofrecer el marco ajustado en el que se desenvuelven las interacciones en el metaverso para poder plantear propuestas regulativas consistentes. Para ello, la mejor aproximación es aquella que recoge y conoce el contexto, que en este caso viene dado por el metaverso, y la potencialidad de la violencia de género para adaptarse a las nuevas realidades.

Dicho de otra forma, el entorno virtual, por su omnipresencia y anonimato, se ha convertido en un espacio apto para violentar y cosificar a las mujeres y el metaverso también lo será si no se adoptan de forma anticipada las medidas preventivas necesarias para evitarlo. La capacidad de cambiar de identidad o de crear múltiples avatares puede permitir a los agresores evadir las restricciones impuestas por las medidas cautelares. Además, la ruptura de equivalencia con la dimensión espacial, la falta de límites físicos, la posibilidad de interactuar a través de diversas plataformas y juegos amplía el campo de acción para la comisión de delitos o el incumplimiento de las medidas.

Plantear la adaptación de medidas legales como las órdenes de alejamiento al contexto virtual es crucial en la lógica preventiva de la violencia de género en estos nuevos espacios digitales. Para ello, es vital profundizar en el entendimiento del metaverso de forma realista, dimensionando adecuadamente las expectativas y los márgenes de acción en esos entornos para elaborar propuestas normativas efectivas y proporcionales en la protección de las víctimas y en la persecución de los agresores.

II. ENTRE REALIDAD Y VIRTUALIDAD: EXPLORANDO EL CONCEPTO DEL METAVERSO.

El metaverso es un término utilizado para describir un espacio digital colectivo y persistente, líquido en lo que a su desarrollo nos podemos referir y con un potencial único, que representa oportunidades de toda índole, pero también potenciales riesgos que advertimos, pero no aún sabemos cómo resolver. Dicho en otras palabras, este concepto deriva del prefijo meta- (más allá) y de universo, es una proyección del pasado, presente y futuro en el que los entornos virtuales interconectados pueden estar integrados a nuestras vidas como el mundo físico.

En su estado actual, el metaverso representa una amalgama de entornos virtuales 2D y espacios inmersivos 3D, donde las experiencias digitales transitan desde simples interfaces gráficas hasta complejas simulaciones que involucran la realidad aumentada (RA) y la realidad virtual (RV). Mientras que los entornos 2D, como las redes sociales y los videojuegos tradicionales, brindan interacciones en un plano bidimensional limitado, los entornos inmersivos buscan simular la totalidad de la experiencia humana, permitiendo a las personas usuarias sentirse presentes en un espacio tridimensional que trasciende las barreras físicas.

Así, el metaverso o también multiverso es el resultado de la fusión de la realidad virtual aumentada y el internet físicamente persistente, permitiendo una experiencia en algunos casos inmersiva (a través de dispositivos "lentes") que nos puede abstraer por completo de la realidad analógica.

Lentes de RV, como las ofrecidas por Pico[7], Meta[8], Samsung[9] y Vrgineers[10], están diseñadas para sumergir completamente a las personas en entornos digitales tridimensionales, ofreciendo una experiencia sensorial que simula la presencia física en mundos virtuales y metaversos. Estos dispositivos utilizan tecnología de pantalla avanzada y sistemas de seguimiento de movimiento para crear una ilusión de profundidad y espacio, permitiendo la interacción con el entorno virtual de manera intuitiva y natural.

Por otro lado, las gafas de realidad mixta (RM), como las desarrolladas por RealWear[11] y también Vrgineers[12], combinan elementos de la RV y la RA,

7 Disponible en: https://www.picoxr.com/es, visitado el día 10 de mayo de 2024.

8 Disponible en: https://www.goertek.com/en/content/details19_470.html, visitado el día 10 de mayo de 2024.

9 Disponible en: https://shop.samsung.com/es/realidad-virtual, visitado el día 10 de mayo de 2024.

10 Disponible en: https://vrgineers.com/xtal-virtual-and-mixed-reality-headsets/, visitado el día 10 de mayo de 2024.

11 Disponible en: https://realwear.com/navigator/, visitado el día 10 de mayo de 2024.

12 Disponible en: https://vrgineers.com/xtal-virtual-and-mixed-reality-headsets, visitado el día 10 de mayo de 2024.

permitiendo ver e interactuar con objetos virtuales superpuestos en el mundo real. Esto no solo enriquece la experiencia del usuario/a al añadir un contexto visualmente integrado, sino que también amplía las posibilidades de aplicación, desde entrenamientos industriales hasta simulaciones interactivas para educación y entretenimiento. La combinación de estas tecnologías promueve una inmersión total en los metaversos, donde las barreras entre lo digital y lo real se difumina, ofreciendo una plataforma expansiva para la exploración, interacción social y comercialización en dimensiones completamente nuevas.

Este concepto, inicialmente explorado, explotado y desarrollado en la literatura y cine de ciencia ficción, ha evolucionado con el avance de la ciencia y la tecnología, poniendo a disposición una nueva herramienta tecnológica, que promueve un ecosistema virtual en el que los y las usuarias pueden interactuar, trabajar y jugar de manera más inmersiva.

1. Diferenciación entre entornos 2D y 3D e inmersivos.

Resulta conveniente partir de la precisión terminológica de ambos entornos. Los entornos 2D son accesibles principalmente a través de pantallas tradicionales, como ordenadores y dispositivos móviles. Se incluyen plataformas como sitios web y juegos bidimensionales donde la interacción es limitada a clics y comandos de teclado, son menos exigentes en términos de hardware, pero ofrecen una experiencia de usuario/a menos inmersiva. Por su parte, los entornos 3D e inmersivos utilizan tecnologías de RV o RA para crear experiencias más envolventes. Permiten a los y las usuarias sentirse parte del mundo digital, interactuando como si estuvieran físicamente presentes a través del uso de cascos de RV, trajes hápticos[13] y otros dispositivos de interfaz avanzada. Estos entornos son especialmente populares en juegos, entrenamientos simulados y experiencias educativas.

Cabe advertir que la Inteligencia Artificial (IA) juega un papel crucial en la operación y evolución del metaverso. En los nuevos entornos virtuales, la IA se utiliza para gestionar y analizar grandes volúmenes de datos de interacción de las personas, optimizar el rendimiento de los sistemas y personalizar las experiencias de los y las usuarias. Además, la IA es fundamental para crear avatares autónomos e inteligentes que pueden interactuar con los y las usuarias de manera realista.

A modo de ilustración, estos mundos virtuales en 2D y 3D pueden ser:

13 Ver ejemplo en: https://teslasuit.io/, "Capabilities of full-body wearable Teslasuit as a self-standing FES device" Disponible en: https://teslasuit.io/use-cases/teslasuit-as-a-self-standing-fes-device/, visitado el día 12 de mayo de 2024

- Horizon Worlds - Meta Platforms (anteriormente Facebook): ofrece este espacio donde los y las usuarias pueden crear y explorar mundos virtuales en 3D[14].

- Second Life: uno de los metaversos pioneros donde los y las usuarias pueden explorar, interactuar y crear contenido en un vasto mundo virtual[15].

- Decentraland: plataforma de realidad virtual basada en blockchain donde los y las usuarias poseen y desarrollan parcelas de tierra virtual[16].

- Roblox: plataforma que permite a los y las usuarias crear juegos y experiencias virtuales que otros pueden explorar y jugar[17].

- Sansar - Similar a Second Life: ofrece un mundo virtual donde los y las usuarias pueden crear, compartir y vender sus experiencias en 3D[18].

La IA no solo mejora la interactividad en el metaverso, sino que también soporta la creación de contenidos generativos y dinámicos que responden y evolucionan en función del comportamiento del usuario/a. Esto incluye desde la generación de entornos que cambian en tiempo real hasta la adaptación de narrativas en juegos o experiencias inmersivas. Así, la IA permite que el metaverso sea un espacio más reactivo y adaptativo, mejorando la inmersión y la experiencia global del usuario/a.

Previo a continuar con el análisis debemos señalar que estos ambientes presuponen un buen y adecuado comportamiento. Son varios los sitios web que sostienen y desarrollan entornos virtuales 2D y 3D que ponen a disposición de las personas usuarias reglas y directrices claras para el uso de sus plataformas, enfocadas en mantener un ambiente acogedor y seguro.

Dentro de estos ecosistemas se valora la diversidad y se prohíbe todo contenido que sea intolerante o discriminatorio hacia cualquier raza, etnia, religión, identidad de género, orientación sexual, capacidad u origen nacional. Además, de acuerdo con sus políticas, se exige que la totalidad de los contenidos compartidos se ajusten a la clasificación del juego o entorno evitando materiales excesivamente violentos o de carácter sexual. Por último, prohíben los contenidos que promuevan actividades ilegales como el acoso, la intimidación, el fraude y la piratería, así como las estafas y las prácticas engañosas, promoviendo el uso

14 Disponible en: https://horizon.meta.com/?locale=en_US, visitado el día 07 de mayo de 2024

15 Disponible en: https://secondlife.com/, visitado el día 07 de mayo de 2024.

16 Disponible en: https://decentraland.org/, visitado el día 07 de mayo de 2024.

17 Disponible en: https://www.roblox.com/es, visitado el día 07 de mayo de 2024.

18 Disponible en: https://www.sansar.com/, visitado el día 07 de mayo de 2024.

de la etiqueta #ReportACreator u otros similares para denunciar situaciones, enfatizando un compromiso con la legalidad y el respeto mutuo[19].

A modo de reflexión preliminar y en términos generales, Roblox y otros entornos similares, que puedan ser conocidas por su capacidad para permitir a los y las usuarias crear y compartir sus propios juegos, también presentan retos complejos en términos de educación, supervisión del contenido e interacción social, como el chat en línea, que pueden exponer a la adolescencia a riesgos de abuso, fraude y otros comportamientos inadecuados.

Así, estas políticas sobre el uso y comportamiento en los entornos virtuales resultan cruciales para proteger a los y las usuarias, con especial atención en los colectivos más jóvenes. Si bien a la adolescencia se le reconoce como nativa digital, muchas veces es solo de redes sociales, desconociendo el potencial virtuoso que pueden tener los entornos digitales. Por tanto, en un entorno digital cada vez más dominado por interacciones virtuales, la línea entre el contenido apropiado y el inapropiado puede ser fácilmente traspasada sin supervisión adecuada.

2. Inteligencia Artificial en el metaverso.

Como hemos anticipado, la IA juega un papel nuclear en la evolución del metaverso, dotándolo de capacidades que van desde la personalización de la experiencia del usuario/a hasta la automatización de entornos complejos y la generación de contenidos.

La IA no solo facilita la creación de avatares realistas y la simulación de comportamientos humanos, sino que también posibilita la interpretación y respuesta en tiempo real a las acciones de los y las usuarias, creando así una experiencia más rica y envolvente. Además, la IA es fundamental en la gestión y análisis de los grandes volúmenes de datos generados dentro del metaverso, permitiendo una mejora continua y adaptativa de estas plataformas digitales.

Al considerar las implicaciones legales del metaverso, es crucial reconocer que la normativa sobre el uso de datos y la protección de la privacidad varía significativamente entre jurisdicciones. En el caso de Chile y España, estas diferencias son particularmente notables, dada la disparidad legislativa de protección de datos y regulación de entornos digitales.

En Chile, la protección de datos personales está regida principalmente por la Ley N° 19.628 sobre Protección de la Vida Privada. Aunque esta ley ofrece un marco para la protección de datos personales, ha sido objeto de críticas por su falta de

19 Ver ejemplo sobre este tipo de políticas y directrices en: https://safety.epicgames.com/es-ES/sanctions-and-appeals, visitado el día 20 de mayo de 2024.

adaptación a los desafíos del entorno digital actual. No obstante, recientemente se ha estado trabajando en una nueva ley de protección de datos personales que busca alinear las regulaciones chilenas con estándares internacionales, como el Reglamento General de Protección de Datos (RGPD) de la Unión Europea.

En contraste, España, como miembro de la Unión Europea, está sujeta al RGPD[20], considerado uno de los marcos regulatorios más precisos y comprensibles en términos de protección de datos y privacidad. El RGPD no sólo impone obligaciones a las empresas que tratan datos personales, sino que también otorga a las personas una serie de derechos sobre sus datos, incluyendo el derecho a acceder, rectificar y eliminar sus datos personales. Además, el RGPD[21] garantiza el derecho a presentar una reclamación ante una autoridad de control en el Estado miembro de residencia habitual y el derecho a la tutela judicial efectiva conforme al artículo 47 de la Carta de los Derechos Fundamentales de la UE[22]. Esto asegura la protección civil del derecho fundamental de las personas físicas en relación con el tratamiento de sus datos, permitiendo a la persona interesada ejercitar una acción ante los tribunales del mismo Estado miembro para exigir responsabilidad civil. Por último, se aplica no solo a las empresas establecidas en la UE, sino también a aquellas que tratan datos de residentes de la UE, lo que significa que su impacto es global.

La comparativa entre Chile y España ilustra la diversidad de enfoques regulatorios y subraya la importancia de una comprensión detallada de los términos y condiciones aplicables en diferentes jurisdicciones. En el contexto del metaverso, esta complejidad se magnifica, ya que los y las usuarias pueden interactuar con plataformas y entidades que operan bajo distintas regulaciones legales, planteando cuestiones relevantes en términos de cumplimiento, gobernanza de datos, protección de la privacidad y jurisdicción.

Como lo indicamos al inicio, la IA de la mano de complejos algoritmos, supone la libertad para diseñar un avatar según los deseos personales y permite a las personas expresar aspectos de su identidad que podrían sentirse incapaces o inseguras de explorar en el mundo físico. Esta flexibilidad podría tener un potencial empoderador, particularmente para aquellas personas que están en proceso de explorar su identidad de género o que pertenecen a comunidades marginadas. Sin embargo, la misma característica que permite una expresión de identidad diversa

20 Disponible en: https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en, visitado el día 20 de mayo de 2024.

21 Muñoz García, C.: *Regulación de la inteligencia artificial en Europa: Incidencia en los regímenes jurídicos de protección de datos y de responsabilidad por productos*, Tirant lo Blanch, Valencia, 2023, pp. 214-216.

22 Disponible en: https://fra.europa.eu/es/eu-charter/article/47-derecho-la-tutela-judicial-efectiva-y-un-juez-imparcial#:~:text=Toda%20persona%20tiene%20derecho%20a,hacerse%20aconsejar%2C%20defender-%20y%20representar, visitado el día 21 de mayo de 2024.

y creativa puede ser explotada para fines menos benignos, como se explorará a continuación.

En el hilo de lo anterior, en Chile, de manera reciente se discute el proyecto de Ley número boletín 15869-19[23] que pretende regular los sistemas de IA, la robótica y las tecnologías conexas, en sus distintos ámbitos de aplicación. La regulación pretendida de los sistemas de IA, como la descrita en el proyecto de ley, es altamente relevante para el desarrollo y la implementación del metaverso, que se puede considerar como un ecosistema digital avanzado donde la IA juega un papel crucial.

En este sentido, podrían existir algunos puntos de conexión entre este proyecto de legislación y el metaverso que conviene destacar:

- Interacción humano e IA: una legislación que exija transparencia sobre cuándo los y las usuarias están interactuando con IA y garantice que los contenidos generados sean identificables como artificiales, sería fundamental para mantener la confianza y la claridad en estas interacciones, asegurando que las denominadas categorías sospechosas susceptibles de especial protección no sufran atentados a sus derechos desde el engaño o la manipulación. Además, cabría atajar desde un inicio los efectos discriminatorios provenientes de los sesgos algorítmicos y la opacidad ya identificados en sistemas de IA[24].

- Protección de datos personales: si se protege adecuadamente el uso de datos personales en el metaverso, incluidos datos biométricos utilizados para la personalización de experiencias, la regulación que establezca lineamientos claros para su uso y manejo ayudaría a prevenir abusos y a garantizar la privacidad de los y las usuarias, asegurando que sus datos no sean explotados ni usados en su contra.

- Impacto social y cultural: si se subraya el impacto social y cultural de la IA en la legislación, un enfoque similar en el desarrollo del metaverso garantizaría que estas nuevas plataformas digitales fomenten la inclusión y no perpetúen la discriminación. Esto sería vital para crear un espacio digital seguro e igualitario.

Por tanto, Chile está avanzando en su regulación de acuerdo con una lógica similar a la europea. De esta manera, la normativa que se encuentra en tramitación sobre IA, y sin perjuicio de lo perfectible que a futuro sea el proyecto, puede

23 Ver más información sobre la tramitación del proyecto de Ley en: https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=16416&prmBOLETIN=15869-19, visitado el día 07 de mayo de 2024.

24 Azuaje Pirela M. y Finol González, D.: "Transparencia algorítmica y la propiedad intelectual e industrial: tensiones y soluciones", *Revista La Propiedad Inmaterial*, 2020, núm. 30, pp. 111-146.

proporcionar un marco legal robusto que entregará más certezas sobre el uso de herramientas de IA.

III. LA CIBERVIOLENCIA CONTRA LAS MUJERES: CONTEXTO ESPAÑA-CHILE.

La violencia de género es la manifestación última de la desigualdad patriarcal y es una de las violaciones de derechos humanos más prevalentes y persistentes en todo el mundo. El ejercicio de violencia contra las mujeres, pese a adoptar múltiples formas, tiene una única finalidad controladora que no permanece en el mundo offline sino que adquiere nuevas dimensiones en el ciberespacio, definido por Lloria García como "un lugar diferente del entorno analógico, un lugar donde se desarrolla la cibersociedad, integrada por aquellos individuos que se relacionan personal, económica y laboralmente en el ciberespacio"[25].

A medida que las interacciones sociales se han trasladado a ese entorno virtual, formas de violencia como amenazas, coacciones, acoso u hostigamiento, vejaciones e injurias han encontrado un nuevo medio para perpetuarse[26]. Raramente, reconoce Wajcman[27], "tenemos la oportunidad de vivir ajenas y ajenos a la tecnología". En este contexto, se reconoce la necesidad de proteger a las mujeres de la ciberviolencia, aquella violencia de género que se perpetra a través de las comunicaciones electrónicas e Internet[28].

En España, la Ley Orgánica 1/2004, de 28 de diciembre, de Medidas de Protección Integral contra la Violencia de Género, pese a pretender un abordaje completo de la violencia de género impulsando medidas desde los ámbitos educativo, sanitario, mediático y judicial, no comprende de forma específica el ámbito digital como nuevo escenario para la comisión de delitos. Sin embargo, ello no ha supuesto una pérdida de atención sobre este fenómeno. En la Memoria de la Fiscalía General de 2023 se pone de manifiesto la proliferación del uso de las TIC en casos de violencia de género y se apunta a dos problemáticas concretas: el anonimato del autor y las dificultades probatorias para determinar justamente la autoría al tener que contar con la colaboración de las empresas prestadoras

25 Lloria García, P.: *Violencia sobre la mujer en el siglo XXI: Violencia de control y nuevas tecnologías*, Iustel, Madrid, 2020, p. 63.

26 Los delitos tecnológicos comprenden en un sentido amplio, los que: i) buscan atacar un sistema informático, ii) se producen en el ciberespacio y iii) los que utilizan la tecnología como medio comisivo. Esta traslación de los delitos clásicos cometidos a través de la tecnología recibe el nombre de "cibercrímenes réplica" por parte de la doctrina. Ídem. pp. 67-68. También Miró Llinares, F.: *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*, Marcial Pons, Madrid, 2012, pp. 51 y ss.

27 Wajcman, J.: *El tecnofeminismo*, Ediciones Cátedra, Madrid, 2006, p. 9.

28 Disponible en: https://eige.europa.eu/publications-resources/thesaurus/terms/1311?language_content_entity=es, visitado el día 10 de mayo de 2024.

de servicios (Instagram, Facebook, Google o Telegram) para la identificación del usuario/a y tráfico de contenidos o tener que recurrir a otros medios de prueba como las capturas de pantalla con la dificultad añadida respecto a su transcripción y cotejo[29].

Sí se incorpora, fruto del nuevo paradigma instaurado con la irrupción de la IA, en la Ley Orgánica 10/2022, de 6 de septiembre, de garantía integral de la libertad sexual. En su ámbito de aplicación incluye las violencias sexuales cometidas en el entorno digital: difusión de actos de violencia sexual, la pornografía no consentida y la infantil en todo caso, y la extorsión sexual a través de medios tecnológicos (art. 3). Asimismo, por Disposición final primera se modifica el artículo 13 de la LECrim adicionando un segundo párrafo que reza: "En la instrucción de delitos cometidos a través de internet, del teléfono o de cualquier otra tecnología de la información o de la comunicación, el juzgado podrá acordar, como primeras diligencias, de oficio o a instancia de parte, las medidas cautelares consistentes en la retirada provisional de contenidos ilícitos, en la interrupción provisional de los servicios que ofrezcan dichos contenidos o en el bloqueo provisional de unos y otros cuando radiquen en el extranjero". Una previsión en la que cabría reflexionar si el metaverso se encuentra incluido al entenderlo, en términos amplios, como una herramienta que requiere internet para su funcionamiento y, de forma más concreta, como una nueva TIC, de acuerdo con la naturaleza y finalidades del mismo.

A diferencia de España, que cuenta con una ley integral de violencia de género y una específica para la violencia sexual, en Chile existe una dispersión normativa que sanciona la violencia por parcelas. De acuerdo con el Ministerio de la Mujer y Equidad de Género chileno, la violencia contra la mujer, se define en palabras simples como: "Las mujeres, sólo por el hecho de ser mujeres, viven diversas formas de violencia de parte de sus parejas o de su entorno que van desde el control hasta la agresión física. Esto se justifica porque en muchas culturas, incluida la chilena, todavía se cree que los hombres tienen derecho a controlar la libertad y la vida de las mujeres"[30].

Realizando un breve barrido legislativo, existen avances que se relacionan con la protección específica de las mujeres, entre los que cabe señalar:

- Ley N°21.645 (vigencia: 29 de diciembre de 2023) que modifica el Código del Trabajo para regular el trabajo a distancia y teletrabajo, enfocado en personas con responsabilidades de cuidado no remunerado, permitiendo jornadas laborales flexibles.

29 Disponible en: https://www.fiscal.es/memorias/memoria2023/FISCALIA_SITE/index.html, visitado el día 10 de mayo de 2024.

30 Consultar sitio web oficial del Ministerio de la Mujer y Equidad de Género de Chile, disponible en: https://minmujeryeg.gob.cl/?page_id=1359, visitado el día 10 de mayo de 2024.

- Ley N°21.565 (vigencia: 09 de mayo de 2023) que establece un régimen de protección y reparación para familias de víctimas de femicidio, incluyendo pensiones de reparación para hijos menores de las víctimas.

- Ley N°21.523 (vigencia: 31 de diciembre de 2022) que modifica leyes para proteger a las víctimas de delitos sexuales, mejorando sus garantías procesales y privacidad en el proceso judicial.

- Ley N°21.378 (vigencia: 4 de octubre de 2021) que establece el monitoreo telemático para asegurar el cumplimiento de medidas de restricción en contextos de violencia familiar o penal.

- Ley N°21.212 (vigencia: 4 de marzo de 2020) que amplía la definición y penalizaciones para el femicidio, incluyendo femicidio íntimo y por razón de género.

- Ley N°21.153 (Vigencia: 3 de mayo de 2019) que tipifica el delito de acoso sexual en espacios públicos y mejora la protección en casos de abuso sexual.

También podemos destacar el proyecto de ley sobre el derecho de las mujeres a una vida libre de violencia, ingresado el 5 de enero de 2017 bajo el Boletín N°11.077-07[31], una iniciativa de mensaje presidencial actualmente en su segundo trámite constitucional. Este proyecto está siendo discutido con urgencia inmediata por las comisiones unidas de la Mujer y la Equidad de Género, y de Constitución, Legislación, Justicia y Reglamento del Senado. Sus objetivos principales, similares al modelo español, incluyen: i) el establecimiento de una ley marco de protección integral contra la violencia de género dirigido a niñas y mujeres; ii) el fortalecimiento de acciones sectoriales para la prevención y erradicación de la violencia de género; iii) el reconocimiento de las distintas manifestaciones de la violencia de género para alinearlas con tratados internacionales y facilitar el desarrollo de políticas y programas adecuados, y iv) la creación de un sistema integrado de información y comisión interinstitucional para el seguimiento de medidas en favor de las víctimas y para coordinar las iniciativas estatales de prevención, sanción y erradicación de la violencia.

Este conjunto de normas demuestra la necesidad de tomar en consideración el ciberespacio como entorno propicio para el ejercicio de la violencia contra las mujeres. No obstante, la velocidad de los avances tecnológicos y sus amplias posibilidades de desarrollo devuelven constantemente al Derecho al punto de salida.

31 La tramitación del proyecto de ley se puede revisar en el siguiente enlace: https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=11592&prmBOLETIN=11077-07, visitado el día 10 de mayo de 2024.

El metaverso, como nuevo espacio para la interacción social, introduce complejidades adicionales a las ya expuestas. Al igual que en las redes sociales y otros espacios digitales, el metaverso tiene el potencial de ser un espacio donde se manifieste la violencia contra las mujeres. Sin embargo, su efecto inmersivo y la profundidad de las interacciones a través de avatares pueden intensificar los impactos de esta violencia. Subrayando los obstáculos antes mencionados con las plataformas tradicionales, en el metaverso el anonimato se refuerza con la creación de identidades múltiples y cambiantes, las capturas de pantalla pierden toda operatividad y las medidas cautelares no parecen previstas para este entorno, puesto que no se comparten todos los rasgos que caracterizan a los delitos tecnológicos, en concreto, la permanencia y la viralidad[32].

IV. LA ORDEN DE ALEJAMIENTO EN EL METAVERSO.

La orden de alejamiento tiene por finalidad evitar el acercamiento entre dos individuos con la imposición de unos metros de distancia que no se pueden rebasar. Tradicionalmente, se han adoptado en el contexto físico, pero la evolución del acoso y la violencia hacia espacios digitales exige un examen de su aplicación en el metaverso. De ahí que el interrogante inicial a formular sea si existe la posibilidad de acordar una orden de alejamiento en el metaverso. La respuesta requiere un análisis detallado de varios factores clave.

- Distancia y velocidad: la dinámica relacional en el metaverso implica una ruptura fundamental con la noción tradicional de espacio (en qué lugar estamos) y distancia (dónde queremos estar). En el metaverso, las barreras físicas se desvanecen y la inmediatez de las interacciones digitales redefine la dinámica entre agresor y víctima, pudiendo un agresor "teletransportarse en términos digitales" instantáneamente a cualquier lugar donde se encuentre la víctima. ¿Cómo calcular entonces los 500 metros de alejamiento? Esta ruptura con la dimensión espacial, requiere de soluciones creativas y complejas, más allá de la simple extrapolación de las medidas del mundo físico al metaverso.

- Tamaño y pluralidad de mundos: el vasto tamaño del metaverso (aparentemente infinito en sus espacios virtuales) y la variedad de interacciones posibles (una persona usuaria puede entrar y salir de diferentes lugares y modificar su apariencia) complejizan la aplicación de prohibiciones. Es esencial especificar qué actividades y espacios están restringidos o qué tipo de verificación digital se requiere para participar de diferentes lugares. Además, la imposibilidad de considerar un domicilio en el metaverso, también dificulta los puntos referenciales para el alejamiento.

32 Lloria García, P.: *Violencia sobre la mujer,* cit. pp. 68-69.

- Anonimato y cambio de identidad: el anonimato y la capacidad de cambiar de identidad fácilmente en el metaverso fuerza a preguntarse acerca de la conveniencia de aunar criterios y definir una única identidad digital. Es crucial desarrollar mecanismos para verificar y autenticar las identidades, sin comprometer la privacidad y la libertad de los y las usuarias legítimas, pero que permita identificar con precisión a la persona que opera tras ese perfil o avatar.

- Bien jurídico protegido: constituido, en esencia, por la integridad y seguridad de la víctima. Sin embargo, en el metaverso, la naturaleza de este bien jurídico adquiere nuevas dimensiones. No se trata solo de proteger la integridad física, sino también de salvaguardar la identidad digital, la privacidad y el bienestar psicológico de las personas. La orden de alejamiento en el metaverso debe, por lo tanto, ser diseñada para proteger contra las formas de violencia que son específicas de estos entornos digitales, asegurando que las víctimas se sientan seguras, no sólo en el mundo físico sino también en el espacio virtual.

Asumidos los elementos que caracterizan el metaverso en relación a la orden de alejamiento y lo problematizan, conviene profundizar en algunos supuestos con su potencial puesta en práctica.

En el caso de España al igual que en Chile, para su adopción deben concurrir los presupuestos generales conocidos como "fummus boni iuris" y "periculum im mora". El primero hace referencia a la existencia de indicios suficientes de la comisión de un delito (delitos de homicidio, aborto, lesiones, contra la libertad, de torturas y contra la integridad moral, trata de seres humanos, contra la libertad e indemnidad sexuales, la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, el honor, el patrimonio, el orden socioeconómico y las relaciones familiares, atendiendo a la gravedad de los hechos o al peligro que el delincuente represente) y, el segundo, a la acreditación de una situación objetiva de riesgo para la víctima que requiera la adopción de medidas de protección[33].

El auto -sentencia interlocutoria en el caso chileno- que acuerde la medida debe detallar la distancia mínima entre el investigado y la víctima que se deberá respetar bajo apercibimiento de incurrir en un delito de quebrantamiento de medida cautelar (64.3 LOVG y 468 CP).

En el metaverso, el desafío de confirmar el abandono de un espacio por parte de una persona sujeta a restricciones judiciales requiere soluciones tecnológicamente avanzadas debido a la naturaleza inmaterial de los espacios virtuales. Tanto

33 Siguiendo a Barona Vilar, las medidas que tienen por finalidad proteger a las víctimas no constituyen medidas cautelares, sino medidas preventivo-represivas o incluso interdictivas en determinados casos. Barona Vilar, S.: "Medidas cautelares específicas", en AA.VV.: *Proceso Penal. Derecho Procesal III* (coord. por J.L. Gómez Colomer y S. Barona Vilar), Tirant lo Blanch, Valencia, 2023, p. 334.

en Chile como en España, las leyes sobre violencia de género contemplan la prohibición de acercarse a la víctima o a lugares frecuentados por ella, y permiten la supervisión adicional mediante monitoreo telemático. Sin embargo, ninguna de estas disposiciones considera los espacios virtuales como el metaverso.

¿Cómo se puede decretar un alejamiento en estos entornos digitales? ¿Cómo se fiscaliza y sanciona? Una estrategia viable incluye la implementación de una solución informática compleja como sería el geovallado virtual[34], lo que en términos sencillos se refiere a la implementación de perímetros virtuales donde el agresor sería automáticamente expulsado o bloqueado al acercarse a la víctima, "solución" que requiere de una tecnología avanzada y cooperación entre las plataformas que interactúan dentro del metaverso. Este tipo de tecnología puede delimitar digitalmente áreas específicas prohibidas para el individuo restringido, el sistema permitiría una supervisión automática y continua, activando alertas en caso de que el individuo intente violar las restricciones impuestas. Este enfoque no solo adapta las restricciones legales del mundo físico al dinámico entorno del metaverso, sino que también asegura la seguridad y privacidad de las partes involucradas[35].

Es importante señalar que, ante la existencia de indicios de quebrantamiento, es posible solicitar a las compañías proveedoras de servicios el registro de comunicaciones, una petición que podría incluir también a las empresas del metaverso, siendo el Tribunal quien considere dentro de su resolución emitir un mandamiento a la empresa respectiva a fin de que ésta dé cumplimiento a la orden de alejamiento en el entorno virtual[36].

Parece más sencilla de implementar la prohibición de comunicación. El auto que la acuerde debe indicar el medio a través del cual se impide la puesta en contacto (postal, telefónico, SMS, correo electrónico, redes sociales), en el que

34 Para más información sobre el uso frecuente de "geovallado" se sugiere la lectura del artículo de Vera Martín, P.; Rodríguez, R. A. y Delgado, C. D.: "Desarrollo de aplicaciones con Geovallas para la asistencia de personas mediante el monitoreo", *Latin-American Journal of Computing*, 2022, vol. 9, núm. 1, pp. 98-107.

35 A este respecto, se plantean dos cuestiones de interés en el intento de extrapolación de las medidas al espacio del metaverso. La primera surge de un posible encuentro fortuito o casual. En ese caso, es el investigado quien debe abandonar el lugar. La segunda refiere a la voluntad de la víctima de no querer ser localizable. En ese caso, la prohibición de aproximación comprenderá únicamente su persona y no se recogerán datos que permitan determinar su ubicación. La pregunta que sigue entonces es si ambas respuestas podrían mantenerse en el metaverso.

36 También es posible que el mismo usuario denuncie este hecho ante la empresa respectiva. Por ejemplo, Roblox proporciona una serie de herramientas y procesos para denunciar comportamientos inapropiados y contenido que infrinja las reglas de la comunidad Entrega la posibilidad de bloquear a los y las usuarias como también la función de "Denunciar abuso", que se traduce en una herramienta central para informar sobre abusos o contenidos inapropiados directamente a las y los moderadores de Roblox, quienes pueden tomar medidas contra los infractores recurrentes. También es posible denunciar durante una experiencia de juego o fuera. Por su parte, los y las usuarias en la UE tienen procedimientos específicos que pueden seguir para denunciar contenido bajo la Ley de Servicios Digitales. Ver más información en: https://en.help.roblox.com/hc/es/articles/203312410-C%C3%B3mo-denunciar-Infracciones-de-las-Reglas, visitado el día 10 de mayo de 2024 y también ver formulario que está asociado a La Ley de Servicios Digitales (DSA) de la UE. Disponible en: https://www.roblox.com/es/illegal-content-reporting, visitado el día 10 de mayo de 2024.

cabría incluir el metaverso. No obstante, surge una preocupación compartida para ambas prohibiciones y es la posibilidad, ya anticipada, de crear avatares que pueden ser un reflejo fidedigno de la apariencia física del usuario/a en el mundo real, pero también encarnar una identidad totalmente alejada de ese perfil con la que, por momentos, las y los usuarios se pueden sentir más cómodas que con las propias en la vida real.

Conviene anotar que el metaverso introduce una nueva dimensión en la conceptualización y administración de la identidad personal. En estos espacios digitales, la identidad se manifiesta a través de avatares, representaciones digitales que los y las usuarias eligen o crean para interactuar en entornos virtuales. Como se ha mencionado, estos avatares pueden reflejar fielmente la apariencia física real de la persona, representar una versión idealizada o, incluso, encarnar una identidad completamente diferente.

Este fenómeno abre un abanico de posibilidades para la expresión de la identidad, pero también presenta interrogantes en términos de seguridad, privacidad y ética social: ¿Es reprochable que la identidad de género en espacios virtuales sea diferente al espacio físico? ¿El género y la expresión de este solo se reconoce y garantiza en espacios físicos y no virtuales? ¿Requieren una nueva definición legal? ¿Cuándo es relevante jurídicamente este tipo de preguntas o conceptualizaciones? ¿Puede el uso de avatar camuflar actos violentos y evadir órdenes de alejamiento? Todos estos interrogantes abren un nuevo paradigma respecto a la construcción de la identidad y a la necesidad de repensar las identidades digitales y el peso -relevancia jurídica- que trae consigo el uso de esta herramienta tecnológica[37].

Así las cosas, podríamos pensar en la imposibilidad de imputar la conducta delictiva a quien en el metaverso se comporta como un personaje mágico, una persona famosa o que, incluso, decide cambiar de sexo. No obstante, bien podría resolverse la cuestión del mismo modo que en los casos de creación de identidades falsas a través de Deepfakes porque, más allá de la máscara que puedan crear los óculos, el sujeto que actúa sigue siendo el mismo[38].

37 Además, el metaverso, como espacio virtual en desarrollo, nos invita a reconceptualizar el sexo, el género y su expresión, ofreciendo un entorno donde las personas pueden explorar y expresar su identidad de género sin las limitaciones y el escrutinio del mundo físico. Si bien proporciona un espacio seguro y libre de juicios, también plantea debates éticos y filosóficos sobre la validez de la identidad y la expresión de género en contextos virtuales versus espacios físicos. ¿Quiénes somos realmente? ¿Es cuestionable que una persona opte por presentarse como transgénero en el metaverso y cisgénero en el mundo físico? ¿Es la expresión de género en el metaverso menos válida o real que en el mundo físico? Estas cuestiones desafían las nociones tradicionales de identidad y género, sugiriendo que la comprensión y aceptación de estas expresiones deben extenderse más allá de los límites físicos. La complejidad de estas reflexiones e interrogantes serán analizadas en un trabajo aparte.

38 Simó Soler, E.: "Retos jurídicos derivados de la Inteligencia Artificial Generativa. Deepfakes y violencia contra las mujeres como supuesto de hecho", *InDret*, 2024, núm. 2, pp. 493-515.

En todo caso, la multiplicidad de escenarios y el progreso incesante de la tecnología convierte en prioritaria la revisión y adaptación significativa de la legislación al contexto actual para adecuarla a las interacciones virtuales que están en permanente desarrollo con una redefinición de los parámetros que se manejan en los tribunales ("aproximación", entre otros) al espacio del metaverso.

1. Precedentes jurisprudenciales de interés en España.

La evolución normativa no progresa a la misma velocidad que lo hace la revolución tecnológica. Habiendo tenido lugar algún episodio previo que anuncia futuras situaciones críticas, la capacidad anticipatoria del Derecho debe intentar evitar nuevos agravios a los derechos de las personas. Esto es, se aprende del pasado para proteger el futuro, teniendo que adaptar las respuestas al contexto presente.

Esta reacción no siempre viene propiciada por la promulgación de una norma reguladora, sino que son los tribunales quienes toman la iniciativa (con interpretaciones extensivas, analógicas, contextuales, ajustadas a la realidad social del momento en que deben aplicarse las leyes) y adelantan la respuesta judicial adoptando en sus resoluciones medidas tendentes a la salvaguarda de bienes jurídicos[39].

De hecho, aunque no en materia penal, se encuentran antecedentes jurisprudenciales que extienden las medidas al metaverso. Con motivo de la celebración del Mobile World Congress en Barcelona, los Jueces de lo Mercantil de Barcelona y los Jueces de lo Mercantil de Alicante (Tribunal de Primera Instancia de Marca de la Unión Europea) establecieron conjuntamente un Protocolo de servicio de guardia y de actuación rápida para la resolución de los conflictos que pudieren darse entre compañías titulares de derechos de propiedad intelectual e industrial y la adopción de medidas cautelares.

En la letra g) se presenta la posibilidad de: "Adoptar y extender la ejecución inmediata de las medidas cautelares y/o diligencias urgentes, anteriormente relacionadas, en particular cuando comprendan actos de presentación, exhibición, promoción, ofrecimiento o venta, realizadas o que se vayan a realizar por los expositores y participantes con ocasión de este congreso, en el metaverso o cualquier otro tipo de entornos y mundos virtuales o plataformas online'"[40].

39 No es pacífica la consideración de este tipo de ejercicios pudiendo argumentarse un desvío de las funciones del Poder Judicial pretendiendo asumir un rol de legislador.

40 Disponible en: https://www.poderjudicial.es/cgpj/es/Poder-Judicial/Tribunales-Superiores-de-Justicia/TSJ-Cataluna/En-Portada/Los-juzgados-mercantiles-de-Barcelona-activan-el-protocolo-de-guardia-durante-la-celebracion-del-Mobile-World-Congress-2024, visitado el día 10 de mayo de 2024.

A lo anterior podemos añadir el auto 21 octubre 2022 del Juzgado de lo Mercantil núm. 9 de Barcelona, en el que se adopta una medida cautelar en el contexto del blockchain. La demanda de VISUAL ENTIDAD DE GESTIÓN DE ARTISTAS PLÁSTICOS (VEGAP) contra PUNTO FA, S.L. (Grupo Mango) alega infracción de derechos de propiedad intelectual por el uso no autorizado de obras de arte en plataformas digitales y físicas. VEGAP sostiene que PUNTO FA utilizó obras de Agustín, Alejo y Alfredo en LinkedIn, Instagram, TikTok, Decentraland, Opensea y una tienda física en Nueva York, solicitando cesación del uso, remoción de las obras y una indemnización.

La demandada negó la infracción, argumentando que el uso digital y la creación de NFTs no violaban los derechos de los artistas, ya que los NFTs no se comercializaron ni se transfirieron. Sin embargo, el Juzgado de Barcelona encontró indicios suficientes de riesgo de inefectividad de la sentencia final sin la adecuada custodia de los NFTs. El fallo estimó parcialmente la aplicación de medidas cautelares, requiriendo "a la sociedad Ozone Networks Inc (responsable de la plataforma Opensea), a través de su dirección de correo electrónico copyright@openseahelp.zendesk.com, para que en el plazo de 2 días, transfiera a la wallet física que la actora designe los citados NFT's , para que queden bajo la custodia del Letrado de la Administración de Justicia hasta que el procedimiento finalice por resolución firme"[41].

Este caso representa de forma tangible cómo el derecho entra a conocer, valorar y resolver nuevos paradigmas, cómo da respuestas a cuestiones que tiene una afectación tanto en el plano real como virtual y que requieren una comprensión integral sobre este tecno-escenario. Siendo el metaverso un entorno digital, resulta igualmente apto para un abordaje legal.

Asimismo, ya en el orden penal, aunque no relacionado con el metaverso, pero sí con la posible comisión de delitos en entornos virtuales, resulta interesante la STS 2 junio 2022[42], que analiza por primera vez, y respalda, la aplicación de la prohibición de acudir al lugar del delito, entendiendo por lugar, "lugares virtuales" como YouTube.

El TS impone, como ya hiciera el Juzgado de lo Penal núm. 9 de Barcelona, en la sentencia núm. 243/2019, 29 de mayo, la pena accesoria de prohibición por 5 años de acudir al lugar de delito, la red social YouTube, con el consiguiente cierre del canal y la imposibilidad de crear nuevos durante ese tiempo. La medida se adopta tras la comisión de un delito contra la dignidad moral de una persona sin hogar. El *youtuber* aceptó un reto de sus seguidores/as consistente en rellenar un

41 AJM B 21 octubre 2022 (1900/2022).

42 STS 2 junio 2022 (ROJ 2356/2022).

paquete de galletas Oreo con pasta de dentífrica y ofrecérselo a una persona en situación de vulnerabilidad para que lo ingiriera, como ocurrió. El reto fue grabado y compartido en su canal.

Dado el establecimiento de esa pena, se presenta una discusión jurídica de máxima relevancia que comportó la adición de un voto particular concurrente, firmado por los magistrados del Moral García y Hernández García que se distanciaron de forma definitiva de la opinión mayoritaria. El debate pivota en torno a la interpretación extensiva del lugar del delito y a la previsión legal de dicha pena en el Código Penal. Para ambos magistrados, "la red ni es un lugar donde se haya cometido el delito -es el medio utilizado para cometerlo- ni, desde luego, es un lugar donde resida la víctima o sus familiares"[43].

Sostienen, además, que este tipo de interpretaciones "distorsiona el sistema y abre las puertas a entender, con el único poco taxativo límite de la necesaria proporcionalidad, que nuestro Código permite, en delitos no necesariamente graves, la prohibición de acceder durante años a internet, o de volver a televisión, o de entrar en Instagram o cualquier otra red social".

Tomando en consideración este punto para la reflexión, y asumiendo la dificultad añadida en el caso de tratarse de medidas cautelares personales en fase de instrucción cuando la presunción de inocencia continúa vigente y se requieren juicios de ponderación de derechos e intereses ajustados[44], no hay que olvidar que en los supuestos de violencia contra las mujeres es imprescindible evaluar las medidas atendiendo al contexto.

Según un informe sobre violencia digital de género del Observatorio Nacional de Tecnología y Sociedad (ONTSI), adscrito al Ministerio de Asuntos Económicos y Transformación Digital, el 54% de las mujeres que ha sufrido acoso a través de redes sociales ha experimentado ataques de pánico, ansiedad o estrés y el 42% de las niñas y jóvenes que ha sufrido acoso online mostraron estrés emocional, baja autoestima y pérdida de autoconfianza. Además, se recogen datos de otro estudio de Amnistía Internacional que muestra un rechazo por parte de las mujeres al uso de las TIC (el 57% tuvo una sensación de aprensión al pensar en utilizar Internet o las redes sociales y el 54% experimentó dicha sensación al recibir correos electrónicos o notificaciones de redes sociales), llegando a traspasar la percepción

43 Aplicado al caso del metaverso quizá esta imposibilidad podría cambiar, siendo posible la comisión de delitos en dicho entorno. En especial, como anticipa Lloria García, cuando el desarrollo tecnológico (por ejemplo, con el uso de trajes hápticos) permita a las personas sentir las acciones que se cometen en espacios virtuales. Ver intervención en: https://www.youtube.com/watch?v=0iseBwZOsLQ&ab_channel=Fundaci%C3%B3nCa%C3%B1adaBlanch, visitado el día 20 de abril de 2024.

44 González Uriel, D.: "La prohibición de acudir al "ciberlugar" de comisión del delito", *Revista Aranzadi Doctrinal*, 2023, núm. 3, p. 9.

de inseguridad al mundo real: el 41% de las mujeres acosadas online sintieron que su seguridad física estaba amenazada[45].

Otro elemento a resaltar del informe es que son las mujeres las que se plantean y, en ocasiones, optan por abandonar el espacio virtual debido a los ataques que sufren. De ahí que se considere, sin pretender asumir una postura punitivista, que la adopción de medidas restrictivas debe pasar por atender a cuál de las partes debe cargar con las consecuencias de la posible comisión de un delito, esto es, cuál de las dos debe ver limitados sus derechos. El Objetivo de Desarrollo Sostenible número 5 de la Agenda 2030 plantea como meta "mejorar el uso de la tecnología instrumental, en particular la tecnología de la información y las comunicaciones, para promover el empoderamiento de las mujeres"[46], de modo que las instituciones deberían tener presenta la meta y los datos de este ODS a fin de que la tecnología -metaversiva- no hipoteque los derechos que las mujeres han ganado en la sociedad física con una potencial cesión de espacios de poder en el diseño de las estrategias de política criminal.

Para ello, y compartiendo algunas ideas de Ramos Martínez y Ruiz[47], dado que históricamente la industria tecnológica ha sido dominada por hombres, el uso del metaverso y la tecnología debe enfocarse en empoderar a las mujeres, abordando ciertas amenazas como el miedo al acoso, la hipersexualización de avatares y la falta de inclusión en el diseño de dispositivos. De ahí que resulte esencial implementar la perspectiva de género interseccional en los planes de innovación tecnológica.

Esta sentencia marca un importante precedente en la evolución de la jurisprudencia al reconocer los entornos virtuales como espacios relevantes para la aplicación del derecho penal y da cuenta de la urgencia por comprender el funcionamiento de las plataformas para poder abordar la multitud de supuestos de hecho que pueden darse.

IV. CONSIDERACIONES FINALES.

El metaverso representa la actual y próxima frontera en la interacción digital, combinando entornos 2D y experiencias inmersivas con las capacidades avanzadas de la IA para crear un espacio digital que es cada vez más indistinguible del mundo

45 Observatorio Nacional de Tecnología y Sociedad, Políticas públicas contra la violencia de género 2022. Ministerio de Asuntos Económicos y Transformación Digital, 2022, pp. 3 y 13. Disponible en: https://portal.mineco.gob.es/RecursosNoticia/mineco/prensa/noticias/2022/220429_i_InformeONTSI.pdf, visitado el día 14 de mayo de 2024.

46 Ver el ODS 5, en específicos datos y metas, en: https://www.un.org/sustainabledevelopment/es/gender-equality/, visitado el día el 20 de mayo de 2024.

47 Ramos Martínez, P. C. y Ruiz, C. B.: "La "meta" es un uni "verso" con perspectiva de género", *Informática y Derecho: Revista Iberoamericana de Derecho Informático (segunda época)*, 2023, núm. 13, pp. 54.

real, pero en 3D. Esto resalta la importancia de mantener un equilibrio entre innovación y seguridad, garantizando que los avances tecnológicos como la IA contribuyan positivamente a la experiencia del usuario/a mientras se protege su integridad y se promueve un ambiente inclusivo y respetuoso.

A medida que el metaverso evoluciona, también lo debe hacer el conocimiento sobre esta herramienta tecnológica. Emerge también la necesidad de regulaciones y directrices para evitar el traslado o perpetuación de la violencia de género en sus modalidades online. Es sabido que la finalidad de la violencia es el control de las mujeres, de ahí que sus agresores hagan empleo de todos los instrumentos a su alcance para procurar ese estado de sumisión.

Una aproximación cuidadosa, reflexiva y multidisciplinar es esencial para garantizar que las propuestas normativas partan de un aprendizaje riguroso e integral del funcionamiento de las nuevas plataformas de interacción virtual. Sobre la base de la explicación extensa de las virtudes del metaverso, pero también de las limitaciones y riesgos, es posible retomar cuatro ideas fuerza que describen la interacción en el este entorno distópico:

1) El metaverso no es más que una herramienta que nos permite trabajar, estudiar, disfrutar de tiempo de ocio y conocer otros avatares en mundos en desarrollo. Las problemáticas que se presentan derivan de sus potenciales usos y de la complejidad que entraña su estado latente de constante evolución.

2) Como en el caso de los avances en IA, el metaverso puede convertirse en un medio para el ejercicio de la violencia contra las mujeres. Este hecho reclama el replanteamiento de las medidas de protección para impulsar que las mujeres cuenten con espacios seguros allí donde decidan relacionarse.

3) Sin embargo, la dificultad de extrapolación de las medidas en entornos donde los ejes espacio-temporales se desvanecen sumado a los obstáculos para verificar la identidad real detrás de un avatar y la facilidad con la que se pueden crear múltiples identidades, plantean encrucijadas reales para la aplicación de la ley y la protección de las víctimas en el metaverso.

Es desde este prisma que se formulan las siguientes recomendaciones:

- Desarrollo de normas específicas con relación a esta tecnología, debiendo las autoridades legislativas colaborar con equipos expertos en ingeniería, derecho, educación, sociología, psicología y filosofía para crear regulaciones que aborden las particularidades del metaverso y las nuevas reconceptualizaciones de los dispositivos jurídicos.

- Implementación de herramientas de verificación y resguardo para las personas usuarias a través del desarrollo de sistemas robustos de autenticación de identidades y herramientas avanzadas de monitoreo que detecten y prevengan situaciones de violencia en tiempo real, equilibrando la seguridad con la privacidad.

- Articulación internacional y alfabetización digital a partir de la colaboración entre países debido a la omnipresencia de esta tecnología para poder asegurar la efectividad de las medidas de protección en el metaverso. Una educación de calidad sobre esta tecnología es la base primordial para evitar sus riesgos, promoviendo un uso y espacio seguro, apoyando a las mujeres víctimas de violencia digital.

BIBLIOGRAFÍA

Azuaje Pirela M. y Finol González, D.: "Transparencia algorítmica y la propiedad intelectual e industrial: tensiones y soluciones", *Revista La Propiedad Inmaterial*, 2020, núm. 30, pp. 111-146.

Barona Vilar, S.: "Cuarta revolución industrial (4.0.) o ciberindustria en el proceso penal: revolución digital, inteligencia artificial y el camino hacia la robotización de la justicia", R*evista Jurídica Digital UANDES*, 2019, vol. 3, núm. 1, pp. 1-17.

Barona Vilar, S.: "Medidas cautelares específicas", en AA.VV.: *Proceso Penal. Derecho Procesal III* (coord. por J.L. Gómez Colomer y S. Barona Vilar), Tirant lo Blanch, Valencia, 2023, pp. 319-343.

González Uriel, D.: "La prohibición de acudir al "ciberlugar" de comisión del delito", *Revista Aranzadi Doctrinal*, 2023, núm. 3, pp. 1-10.

Lloria García, P.: *Violencia sobre la mujer en el siglo XXI: Violencia de control y nuevas tecnologías*, Iustel, Madrid, 2020.

Martín-Blas, E.: *Metaverso : pioneros en un viaje más allá de la realidad*, LID Editorial, Madrid, 2022.

Miró Llinares, F.: *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*, Marcial Pons, Madrid, 2012.

Muñoz García, C.: *Regulación de la inteligencia artificial en Europa: Incidencia en los regímenes jurídicos de protección de datos y de responsabilidad por productos*, Tirant lo Blanch, Valencia, 2023.

Ramos Martínez, P. C. y Ruiz, C. B.: "La "meta" es un uni "verso" con perspectiva de género", *Informática y Derecho: Revista Iberoamericana de Derecho Informático (segunda época)*, 2023, núm. 13, pp. 45-56.

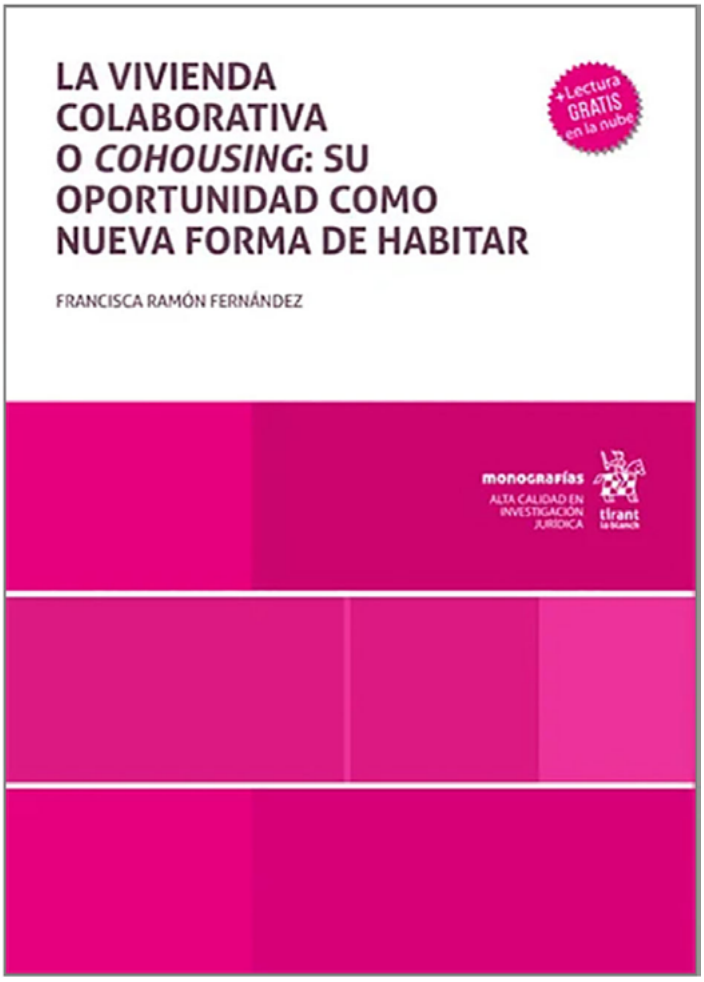
Simó Soler, E.: "Retos jurídicos derivados de la Inteligencia Artificial Generativa. Deepfakes y violencia contra las mujeres como supuesto de hecho", *InDret*, 2024, núm. 2, pp. 493-515.

Vera Martín, P.; Rodríguez, R. A. y Delgado, C. D.: "Desarrollo de aplicaciones con Geovallas para la asistencia de personas mediante el monitoreo", *Latin-American Journal of Computing*, 2022, vol. 9, núm. 1, pp. 98-107.

Wajcman, J.: *El tecnofeminismo*, Ediciones Cátedra, Madrid, 2006.

RECENSIONES

RAMÓN FERNÁNDEZ, Francisca: *La vivienda colaborativa o cohousing: su oportunidad como nueva forma de habitar,* Tirant lo Blanch, Valencia, 2024, 240 páginas. ISBN: 978-84-1056-446-6.



Presentamos la obra *La vivienda colaborativa o cohousing: su oportunidad como nueva forma de habitar* que ha sido recientemente publicada por la editorial Tirant lo Blanch, dentro de la colección de monografías alta calidad en investigación jurídica. Editorial de reconocido prestigio ya que es la mejor valorada en clasificación SPI (Scholarly Publishers Indicators) que realiza el grupo ILÍA del Consejo Superior de Investigaciones Científicas (CSIC). Este prestigioso estudio otorga a la editorial Tirant lo Blanch una valoración de 31.563 puntos.

Nos encontramos ante una obra de una gran actualidad sobre un tema muy novedoso siendo una de las primeras aportaciones monográficas dedicadas a la

vivienda colaborativa después de su regulación autonómica. constituye una obra de gran actualidad y que por su excepcional interés se ha publicado en la citada editorial prestigiosa.

La autora de la obra es la catedrática de Derecho civil de la Universitat Politècnica de València, Francisca Ramón Fernández, y se ha realizado en el marco de del Grupo de Investigación de Excelencia Generalitat Valenciana "Algorithmical Law" (Proyecto Prometeu 2021/009, 2021-2024), Proyecto "Promoting capacity building ande knowledge for the extensión of urban gardens in European cities" (PCI2022-132963) (2022-2025), Investigación competitiva proyectos. Ministerio de Ciencia e Innovación, de la que es investigadora principal, Proyecto Mujeres, cooperativismo y economía social y solidaria. Contribución a una participación igualitaria en la economía y la sociedad, Ministerio de Igualdad (46-12-ID22), y Proyecto de I+D+i "Derechos y garantías públicas frente a las decisiones automatizadas y el sesgo y discriminación algorítmicas" 2023-2025 (PID2022-126439OB-I00) financiado por MCIN/AEI/10.13039/501100011033/FEDER,UE, en los que participa como investigadora.

La propuesta de investigación se presentó a una convocatoria pública competitiva convocada por la Universitat Politècnica de València, obteniendo una ayuda PAIV (Propuestas de Actividades de Innovación en Vivienda), convocatoria 2023 de la Càtedra Innovació en Habitatge de la Universitat Politècnica de València, marco de colaboración entre la Generalitat Valenciana, a través de la Vicepresidencia Segona i Conselleria d'Habitatge i Arquitectura Bioclimàtica y la Universitat Politècnica de València en atención a la valoración de la propuesta que realizó una comisión atendiendo a su interés y viabilidad.

Nos encontramos ante una obra solvente tratada con rigurosidad en el que se dan respuestas a las distintas cuestiones que plantea la vivienda colaborativa o *cohousing*. En la obra de investigación que presentamos se analiza uno de los aspectos más relevantes de la innovación en la forma de habitar espacios, como es la vivienda en la que se comparten espacios comunes y se disponen de espacios de uso individual.

Este estudio también viene propiciado por la oportunidad legislativa que ha supuesto el Plan Estatal para el acceso a la vivienda 2022-2025 en el que se fomenta el modelo *cohousing* y la reciente regulación por la Ley 372023, de 13 de abril, de viviendas colaborativas de la Comunitat Valenciana siendo esta monografía la primera y pionera que se dedica a su estudio y análisis.

La máxima actualidad del objeto de investigación es evidente y se relaciona con otras normas recientemente promulgadas como el Decreto 68/2023, de 12 de mayo, del Consell, por el que se aprueba el Reglamento de vivienda de

protección pública y régimen jurídico de patrimonio público de vivienda y suelo de la Generalitat Valenciana, y el Decreto 80/2023, de 26 de mayo, del Consell, por el que se aprueban las normas de diseño y calidad en edificios de vivienda.

El enfoque del trabajo propia que sea de un alto interés no solamente para el ámbito jurídico, sino también para el técnico siendo de utilidad para los profesionales de la arquitectura, de la construcción y del ámbito empresarial y de la administración de viviendas.

La razón de ser de esta forma de habitar concebida como una alternativa a las residencias en el caso de las personas de edad avanzada también es una opción válida para otros colectivos que quieren vivir compartiendo espacios y entorno. El entramado jurídico queda claramente desarrollado en la presente obra que se centra en los requisitos básicos de los edificios o conjuntos residenciales, las exigencias básicas de funcionalidad, seguridad y habitabilidad y los principios aplicables al diseño y calidad de los materiales y estructuras. Se detiene también la obra en el régimen de los titulares de viviendas colaborativas de interés social, la acción pública respecto a esta tipología de viviendas, el derecho de tanteo y retracto, las medidas de fomento y su régimen sancionador. De igual forma, se analiza la implantación de viviendas colaborativas en suelo no urbanizable en zonas rurales y/o en peligro de despoblamiento, el tratamiento fiscal de estas viviendas, y el concepto de función social en la declaración de cooperativas de utilidad pública.

La obra dispone de una estructura idónea para el análisis de los distintos aspectos y que abarca tres grandes bloques: el primer bloque se detiene en los distintos modelos de vivienda alternativos y se referencia la economía colaborativa como base de su aplicación en la vivienda; las distintas denominaciones como vivienda colaborativa, compartida, covivienda, *cohousing, coliving,* cohabitatge y transvivienda, y un análisis detallado del modelo cooperativo; el segundo bloque presenta el estudio de la cesión de uso, los destinatarios, los requisitos y características, las ventajas y desventajas de este tipo de vivienda y cuáles son las necesidades que se pretenden cubrir con esta modalidad de habitar; el tercer bloque se ocupa de precisar la legislación aplicable y las distintas normas que se han ido promulgando en relación con las viviendas colaborativas principalmente destinadas para la promoción de la autonomía personal y la atención a la dependencia de personas mayores, para, después, analizar con sumo detalle la regulación en la Ley 3/2023, de 13 de abril, de Viviendas Colaborativas de la Comunitat Valenciana.

Concluye el estudio con unas acertadas conclusiones sobre los distintos puntos analizados, un apartado de referencias legislativas y de jurisprudencia en el que se incluyen las sentencias del Tribunal Constitucional, Tribunal de Justicia de la Unión

Europea, Tribunal Supremo y Tribunal Superior de Justicia, así como un apartado de referencias de resoluciones utilizadas.

Se destaca la función de la vivienda colaborativa para acceder a la vivienda, y la consideración de que el envejecimiento activo y sostenibilidad son unos aspectos a tener en cuenta a la hora de decantarse por una vivienda colaborativa. Se considera al *cohousing* como una forma de habitar, pero es mucho más que eso, es un modo de vida en sintonía con un estilo de vida de cooperación y respeto al medio ambiente, con una diversificación de los servicios de atención y cuidado.

Reseñar que la legislación analizada es muy rigurosa a la hora de implementar la vivienda colaborativa exigiendo una serie de requisitos para su viabilidad, así como la forma jurídica adecuada para llevarla a su fin.

En definitiva, en esta obra muy completa se encontrarán respuestas a las distintas cuestiones que puede suscitar la vivienda colaborativa, un modelo que ya es bien conocido en otros países como forma de habitar.

José Ramón De Verda y Beamonte
Catedrático de Derecho civil
Universitat de València