LOS PRINCIPIOS ESTRUCTURALES DEL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS*

STRUCTURAL PRINCIPLES OF THE GENERAL DATA PROTECTION REGULATION

Actualidad Jurídica Iberoamericana Nº 20, febrero 2024, ISSN: 2386-4567, pp. 1322-1341

* Este trabajo ha sido realizado en el marco del proyecto de investigación "Inteligencia artificial, Justicia y Derecho: ¿irrupción o disrupción tecnológica en el proceso penal?" (PID2020-119324GB-I00), financiado por el Ministerio de Ciencia e Innovación. Período de ejecución 2021-2023.

Moisés BARRIO ANDRÉS

ARTÍCULO RECIBIDO: 11 de noviembre de 2023
ARTÍCULO APROBADO: 12 de enero de 2024

RESUMEN: El RGPD se ha convertido en el modelo global de privacidad. Ello es así por dos razones. En primer lugar, por los criterios de aplicación territorial que establece su artículo 3. En segundo lugar, por las imprescindibles transferencias internacionales de datos, lo cual implica que se tenga que aplicar el RGPD. Dada su influencia planetaria, resulta de utilidad esbozar unos supraprincipios que han de inspirar la aplicación e interpretación del RGPD, y que también sintetizan el espíritu, sentido y finalidad de esta norma jurídica, a lo cual se destina este trabajo. Se acuñan así seis supraprincipios: legitimidad, proporcionalidad, empoderamiento, transparencia, responsabilidad proactiva y seguridad, que desarrollaremos en las próximas páginas.

PALABRAS CLAVE: Protección de datos; reglamento general de protección de datos; RGPD; legitimidad; proporcionalidad; empoderamiento; transparencia; responsabilidad proactiva; seguridad.

ABSTRACT: *The GDPR has become the global model for privacy. There are two reasons for this. Firstly, because of the territorial application criteria established in Article 3. Secondly, due to the essential international transfers of data, which implies that the GDPR must be applied. Given its global influence, it is useful to outline some supra-principles that should inspire the application and interpretation of the GDPR, and that also summarize the spirit, meaning and purpose of this regulation, which is the purpose of this paper. Six supra-principles are thus coined: legitimacy, proportionality, empowerment, transparency, accountability and security, which we will address in the following pages.*

KEY WORDS: *Data protection; general data protection regulation; GDPR; legitimacy, proportionality; empowerment; transparency; accountability; security.*

I. INTRODUCCIÓN.

El tratamiento de datos personales ha sido objeto de atención universal tras la adopción 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, el Reglamento General de Protección de Datos (RGPD)[1].

EL RGPD comparte los principios y objetivos de la 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 respeta al tratamiento de datos personales y a la libre circulación de estos datos, a la que ha sucedido, pero instituye un conjunto mucho más detallado y actualizado de reglas[2] que además son directamente aplicables en todos los Estados miembros de la Unión.

Pocas normas jurídicas de la Unión Europea han atraído una atención ciudadana y mundial similar. El RGPD es probablemente el exponente más significativo del denominado "efecto Bruselas", dado que, según la tesis de la profesora BRADFORD[3], la Unión Europea con sus normas jurídicas "acaba influyendo más a nivel mundial que Estados Unidos con su poder militar o China con sus proyectos en el extranjero". En este caso, el RGPD ha trascendido con creces las fronteras del Espacio Económico Europeo y se ha convertido en un estándar internacional *de facto*, con más de 160 países del mundo con su legislación inspirada en nuestro reglamento europeo.

Tras cinco años de aplicación del RGPD, podemos subrayar que esta norma del Derecho de la Unión Europea ha consolidado un marco jurídico estable y

1 Sobre el mismo, puede verse López Calvo, J. (coord.): *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD*, Madrid, Bosch-Wolters Kluwer, 2019; Rallo Lombarte, A. (dir.): *Tratado de Protección de Datos*, Valencia, Tirant lo Blanch, 2019; o Domínguez Álvarez, J.L.: *Tratado de protección de datos personales*, A Coruña, Colex, 2023.

2 Barrio Andrés, M.: *Manual de Derecho Digital*, Valencia, Tirant lo Blanch, 2022, 2.ª edición, capítulos 11 y 12.

3 Bradford, A.: *The Brussels Effect: How the European Union Rules the World*, Nueva York, Oxford University Press, 2020, pág. 1.

• Rosa Lapiedra Alcamí
Letrado del Consejo de Estado. Profesor de Derecho digital y Director del Diploma de Alta Especialización en Legal Tech y transformación digital (DAELT) de la Escuela de Práctica Jurídica de la Universidad Complutense de Madrid. ORCID: https://orcid.org/0000-0002-2877-5890. Correo electrónico: moises.barrio@consejo-estado.es

seguro para el tratamiento de datos personales. Y ha hecho eficaces en la práctica al menos dos de sus propósitos nucleares. El primero, ha generalizado una cultura de protección de datos tanto entre los responsables del tratamiento como entre los ciudadanos en el contexto del mercado digital europeo. El segundo, está asegurando que los tratamientos de datos de cualquier naturaleza respeten el derecho fundamental a la protección de datos, lo que a la postre entronca con el sistema europeo iusfundamental[4] de libertades, derechos y garantías.

Asimismo, el RGPD se ha convertido en el modelo global de privacidad. Ello es así por dos razones. En primer lugar, por los criterios de aplicación territorial que establece su artículo 3. En segundo lugar, por las imprescindibles transferencias internacionales de datos, lo cual implica que se tenga que aplicar el RGPD, con lo cual la implantación de esta norma es prácticamente universal.

Dada su influencia planetaria, resulta de utilidad esbozar unos supraprincipios que han de inspirar la aplicación e interpretación del RGPD, y que también sintetizan el espíritu, sentido y finalidad de esta norma, a lo cual destinaremos el próximo epígrafe.

II. LOS SUPRAPRINCIPIOS O PRINCIPIOS ESTRUCTURALES DEL RGPD.

Entendemos por tales las ideas directrices del RGPD que inspiran, orientan, relacionan y estructuran sus distintos elementos y normas jurídicas.

Sentado lo anterior, el objetivo de este artículo es destilar los 173 considerandos y 99 artículos del RGPD en seis supraprincipios o principios estructurales que ayuden en el conocimiento, comprensión, aplicación e interpretación de este reglamento europeo. Se proponen así seis supraprincipios:[5] legitimidad, proporcionalidad, empoderamiento, transparencia, responsabilidad proactiva y seguridad, que desarrollaremos en las próximas páginas.

A pesar de la importancia de la intimidad y el tratamiento de datos personales, la jurisprudencia del Tribunal de Justicia de la Unión Europea (TJUE) sobre esta materia resulta todavía limitada. Ahora bien, y dada la continuidad de los principios, la jurisprudencia relativa a la derogada Directiva 95/46/CE sigue siendo relevante y trasladable aquí.

4 García Roca, J. y Santaolalla, P. (coords.): *La Europa de los Derechos. El Convenio Europeo de Derechos Humanos*, Madrid, Centro de Estudios Políticos y Constitucionales, 2023, 4.ª edición, capítulo I.

5 El artículo 5 del RGPD, titulado "Principios relativos al tratamiento", prescribe siete principios generales que se incorporan a su articulado. Estos principios no resumen el RGPD ni tienen la misma importancia.

1. Legitimidad.

Los debates sobre la intimidad y la privacidad tienen ya una cierta antigüedad[6], y el derecho a la intimidad desempeña un papel cardinal tanto en la democracia como en la autonomía individual, donde debe alcanzarse un equilibrio entre la esfera individual y la colectiva; ambas son necesarias para desarrollar la democracia y el libre desarrollo individual.

El derecho a la intimidad, incluido la protección de los datos personales, está consagrado al máximo nivel[7] en el Derecho de la Unión Europea como derecho fundamental, es decir, a nivel de derecho primario[8], junto con otras libertades democráticas como la libertad de pensamiento y expresión. El considerando 4 del RGPD subraya que "el tratamiento de datos personales debe estar concebido para servir a la humanidad".

En este marco, el derecho fundamental a la protección de datos personales (art. 8 CDFUE y art. 18.4 CE) –derecho autónomo incluido dentro del derecho a la intimidad– no sólo protege los datos íntimos, sino todos los datos personales, afecten o no a la intimidad de las personas, incluidos los datos públicos, ya que lo que es objeto de protección por este derecho es el poder de disposición que tiene una persona sobre todos sus datos.

Estos derechos pueden ser analizados y estudiados desde una perspectiva sociopolítica, psicológica, histórica e incluso evolutiva. Y es importante tener en cuenta que el Derecho no puede explicar en su totalidad los mismos, ya que nuestra disciplina refleja las decisiones de política legislativa adoptadas por el legislador de la Unión Europea. Este hecho no hace en absoluto que la norma jurídica sea superflua o carezca de relevancia, especialmente si se tiene en cuenta el riesgo de multas según el RGPD alcanza hasta 20.000.000 de euros o el 4 % del volumen de negocios total anual en todo el mundo (la cifra que sea más alta).

La normativa sobre protección de datos es una materia compleja, no tanto por la falta de claridad de las disposiciones aplicables, sino más bien porque es imprescindible una compleja ponderación de intereses. Como se desprende del propio considerando 4 del RGPD: "El derecho a la protección de los datos personales no es un derecho absoluto sino que debe considerarse en relación

6 Warren, S.D. y Brandeis, L.D.: "The Right to Privacy", *Harvard Law Review*, 1890, Vol. 4, Núm. 5, , pp. 193-220; Westin, A.F.: *Privacy and Freedom*, Londres, The Bodley Head, 1970, capítulo I.

7 Castillejo Manzanares, R.: "Nuevas tecnologías y prueba en el proceso penal. Especial incidencia en Inteligencia Artificial", *Derecho Digital e Innovación*, 2022, Núm. 11; y Matia Portilla, F.J. (coord.): *De la intimidad a la vida privada y familiar*, Valencia, Tirant lo Blanch, 2020, pp. 60-63.

8 Véanse los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea (CDFUE), así como el artículo 6 del Tratado de la Unión Europea (TUE) y el artículo 8 del Convenio Europeo de Derechos Humanos (CEDH).

con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad".

Los datos personales pueden tratarse con fines legítimos específicos y explícitos. Los datos recogidos no podrán ser tratados posteriormente de manera incompatible con los fines para los que fueron recogidos (art. 5, apdo. 1, letra b) RGPD).

La legitimidad puede describirse como el principio estructural que incluye el requisito general de tratamiento leal y lícito (art. 5, apdo. 1, letra a) RGPD). Cuando las empresas utilizan datos personales que están protegidos como derecho fundamental, son ellas las que deben garantizar que el tratamiento es legítimo. El derecho a la protección de datos, y en último término la salvaguardia de la privacidad, exige que las excepciones y limitaciones sólo se apliquen en la medida estrictamente necesaria[9], y que las excepciones se interpreten de forma restrictiva[10].

Las empresas no son "propietarias" de los datos personales, ni están autorizadas *per se* a tratarlos[11]. Sin embargo, sí están autorizadas –con las limitaciones y requisitos establecidos en el RGPD– a conculcar la esfera de intimidad de los ciudadanos.

Una de las características definitorias de los análisis de *big data* de nuestro tiempo es que se basan en probabilidades y, como tales, resultan imprecisos[12]. El principio de exactitud de los datos (art. 5, apdo. 1, letra d) RGPD) tiene una importancia significativa, ya que exige que los datos personales sean "exactos y, si fuera necesario, actualizados". El responsable del tratamiento debe adoptar "todas las medidas razonables" para suprimir o rectificar los datos personales inexactos. En este sentido, deben tenerse en cuenta los fines para los que se tratan los datos. La jurisprudencia del TJUE no ha establecido hasta qué punto el uso de datos probabilísticos es conforme con el principio de exactitud.

Además de servir a una finalidad legítima, los datos personales deben tratarse de forma leal y ampararse en una base jurídica de legitimación para dicho tratamiento, tal y como se expondrá seguidamente en el próximo principio estructural.

9 Sentencia del Tribunal de Justicia (STJUE) de 7 de noviembre de 2013, *Institut professionnel des agents immobiliers (IPI)*, (C-473/12, ECLI:EU:C:2013:715), apdo. 39.

10 STJUE de 11 de diciembre de 2014, *Ryneš*, (C-212/13, ECLI:EU:C:2014:2428), apdo. 29.

11 Barrio Andrés, M.: *Internet de las Cosas*, Madrid, Reus, 2022, 3.ª edición, pp. 106 y ss.

12 Barrio Andrés, M.: "Inteligencia artificial: origen, concepto, mito y realidad", *El Cronista del Estado Social y Democrático de Derecho*, 2022, Núm. 100.

2. Proporcionalidad.

Debido a las múltiples formas que puede adoptar el tratamiento de datos, el principio estructural de legitimidad va acompañado de un principio de proporcionalidad que permea todo el RGPD. Este principio es visible en las frecuentes referencias a lo que es "necesario", "adecuado", "apropiado", "compatible", "razonable", etc.

La legitimidad del tratamiento depende de la naturaleza, el alcance, el contexto y los fines del tratamiento, así como de los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas. Las normas del RGPD pretenden lograr un equilibrio adecuado entre la protección de los derechos del interesado y los intereses legítimos de los responsables del tratamiento, terceros y el interés de la ciudadanía. Así como cumplir con las obligaciones legales de registro y conservación de datos. Por ejemplo, la controvertida videovigilancia puede ser lícita por motivos de seguridad, pero ilícita con fines de marketing.

Según los principios generales establecidos en el artículo 5 del RGPD, los datos personales deben limitarse a lo estrictamente necesario ("minimización de datos") y no deben conservarse más tiempo del necesario ("limitación del plazo de conservación"). En este contexto, la necesidad está relacionada con los fines para los que se tratan los datos personales, como se ha explicado anteriormente en el principio estructural de legitimidad.

El principio de la "limitación de la finalidad", positivizado en el señalado artículo 5.1.b) del RGPD, establece que los datos personales no pueden tratarse "ulteriormente de manera incompatible" con los fines para los que se recogieron (art. 6.4. RGPD), lo que también refleja una manifestación del principio estructural de la proporcionalidad.

El tratamiento de datos personales debe basarse en el consentimiento del interesado[13] o en cualquier otra base legítima establecida por el RGPD. De este modo, debe existir una base legítima para cada finalidad del tratamiento de datos personales.

El consentimiento requiere "una manifestación de voluntad libre, específica, informada e inequívoca del interesado" que signifique su acuerdo con el tratamiento (art. 4.1.11 RGPD). La solicitud de consentimiento debe presentarse de tal forma "que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo" (art. 7 RGPD). No obstante, y pesar del consentimiento, el tratamiento de datos personales sigue estando restringido

13 Sobre su alcance, *vid*. la Sentencia del Tribunal de Justicia (STJUE) de 4 de julio de 2023, *Meta Platforms Inc*., (C-252/21, ECLI:EU:C:2023:537), apdo. 151.

por los principios del tratamiento lícito (art. 5 RGPD), que incluyen la legitimidad y la proporcionalidad.

Ahora bien, los datos personales pueden tratarse sin consentimiento si es necesario, entre otros supuestos, para la ejecución de un contrato o el cumplimiento de una obligación legal. En conjunto, estas bases de legitimación justifican el tratamiento necesario para la entrega de productos y el cumplimiento de obligaciones fiscales y contables.

El tratamiento también es lícito sin consentimiento cuando supera el juicio de ponderación (*balancing test),* que hasta cierto punto puede utilizarse para justificar el tratamiento con fines comerciales. Este juicio de ponderación[14] permite al responsable del tratamiento tratar los datos personales cuando el tratamiento es necesario para fines legítimos, a menos que prevalezcan los intereses o los derechos y libertades fundamentales del interesado (art. 6.1.f) RGPD). Y debe subrayarse que el concepto de "necesidad"[15] posee su propio significado autónomo en el Derecho de la Unión y debe interpretarse de manera que refleje los objetivos de la legislación sobre protección de datos.

Como se expone más adelante en el principio estructural de empoderamiento, el consentimiento y el juicio de proporcionalidad comparten la desventaja de que el interesado puede o bien retirar el consentimiento o, en el segundo caso, oponerse al tratamiento. En caso de oposición, el responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones. En cambio, el interesado no puede oponerse si el tratamiento es realmente necesario para la ejecución de un contrato.

De este modo, a menos que el tratamiento sea realmente necesario para la ejecución de un contrato con el interesado o que el impacto sobre la intimidad del interesado sea limitado, lo más seguro es obtener su consentimiento. Sin embargo, cuando el tratamiento es realmente necesario para la ejecución de un contrato, el consentimiento no es la base legítima adecuada[16].

14 Casas Baamonde, M.E.: "La plena efectividad de los derechos fundamentales: juicio de ponderación (¿o de proporcionalidad?) y principio de buena fe", *Relaciones laborales. Revista crítica de teoría y práctica*, 2004, Núm. 1, , pp. 141-156.

15 STJUE de 16 de diciembre de 2008, *Huber,* (C-524/06, ECLI:EU:C:2008:724), apdo. 52.

16 Comité Europeo de Protección de Datos (CEPD): *Directrices 2/2019 sobre el tratamiento de datos personales en virtud del artículo 6, apdo. 1, letra b), del RGPD en el contexto de la prestación de servicios en línea a los interesados*, pág. 7.

Cuando se traten datos personales sensibles, o categorías especiales de datos personales[17], con carácter general debe obtenerse el consentimiento (art. 9.2.a) RGPD).

La proporcionalidad también desempeña un papel nuclear en relación con las obligaciones generales del responsable del tratamiento de datos, que se abordan más adelante en el principio estructural de responsabilidad proactiva. Al determinar la responsabilidad del responsable del tratamiento (arts. 24 y 25 RGPD), deben tenerse en cuenta "la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas". Para la aplicación de determinadas medidas, también deben tenerse en cuenta "el estado de la técnica" y "el coste de su aplicación" (arts. 25 y 32 RGPD).

Como se desarrolla más adelante en el principio estructural de seguridad, las medidas técnicas y organizativas deben ser "apropiadas" (art. 5, apdo. 1, letra f) RGPD), y en el contexto de la rectificación y supresión (tratada en el próximo principio estructural relativo al empoderamiento), deben tenerse en cuenta "la tecnología disponible y el coste de su aplicación", así como "el esfuerzo desproporcionado".

Como principio general, del apartado 1 del artículo 52 de la Carta de los Derechos Fundamentales de la Unión Europea (CDFUE) se desprende que las limitaciones a las libertades establecidas en la Carta deben ser necesarias y responder realmente (i) a objetivos de interés general reconocidos por la Unión o (ii) a la necesidad de proteger los derechos y libertades de los demás.

De este modo, el principio estructural de proporcionalidad implicaría que el tratamiento de datos personales no debe exceder de lo necesario para alcanzar los objetivos legítimos. En este sentido, la utilización de medios menos intrusivos[18] con la intimidad también debe tenerse muy en cuenta. Así lo expresa el propio RGPD cuando exige "garantías adecuadas", que pueden incluir la pseudonimización (separación entre la identidad y los datos que se tratan).

3. Empoderamiento.

La responsabilidad individual y el derecho a la autodeterminación son conceptos centrales en la teoría jurídica, así como en la legislación de protección

17 Véase el artículo 9 del RGPD. Se trata de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física.

18 STJUE de 9 de noviembre de 2010, Gran Sala, *Volker und Markus Schecke*, (asuntos acumulados C-92/09 y C-93/09, ECLI:EU:C:2010:662).

de los consumidores, cuyo marco regulador tiene por objeto facultar al ciudadano para que actúe de acuerdo con sus preferencias.

A pesar del empoderamiento, el interesado no tiene un control absoluto sobre qué datos se tratan sobre él y quién los trata. Aquí nos centramos principalmente en los derechos del interesado, que están estrechamente relacionados con la transparencia, de la que nos ocuparemos más adelante.

El consentimiento es uno de los ejemplos más claros del empoderamiento. Además de ser específico e informado, el consentimiento debe darse libremente y constituir una manifestación inequívoca de la voluntad del interesado que signifique su acuerdo con el tratamiento de datos personales (art. 4.1.11 RGPD). El consentimiento reclama tanto transparencia como una clara acción afirmativa que impide que "el silencio, las casillas ya marcadas o la inacción" constituyan auténtico[19] consentimiento.

Y el requisito de libremente otorgado requiere una elección auténticamente libre, lo que no es el caso si el interesado "no goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno" (cdo. 42 RGPD). Del mismo modo, en el apartado 4 del artículo 7 del RGPD se establece que debe tenerse "en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato".

Además de las situaciones en las que se requiere el consentimiento, el interesado puede ejercer los derechos de acceso, rectificación, supresión y oposición, manifestar su voluntad de no ser objeto de decisiones individuales automatizadas e incluso solicitar la portabilidad de sus datos. Los dos primeros derechos están además consagrados en la CDFUE (art. 8.2).

El derecho de acceso supone que el interesado tiene derecho a obtener confirmación sobre si se están tratando o no datos personales que le conciernen[20]. Si se están tratando datos personales que le conciernen, el interesado tiene derecho a acceder a los datos personales, así como a la información sobre los

19 Cdo. 32 RGPD y STJUE de 1 de octubre de 2019, *Planet49,* (C-673/17, ECLI:EU:C:2019:801).

20 La STJUE de 4 de mayo de 2023, *Österreichische Datenschutzbehörde y CRIF*), (C-487/21, ECLI:EU:C:2023:369) ha precisado el contenido de este derecho, indicando que "el derecho a obtener del responsable del tratamiento una copia de los datos personales objeto de tratamiento implica que se entregue al interesado una reproducción auténtica e inteligible de todos esos datos. Este derecho incluye el de obtener copia de extractos de documentos, o incluso de documentos enteros, o de extractos de bases de datos, que contengan, entre otros, dichos datos, si la entrega de tal copia es indispensable para permitir al interesado ejercer efectivamente los derechos que le confiere ese Reglamento. Debe subrayarse asimismo la necesidad de que se tengan en cuenta, a este respecto, los derechos y libertades de los terceros".

fines, las categorías, el periodo previsto de conservación y demás información detallada en el artículo 15 del RGPD.

El derecho a obtener la rectificación de los datos personales inexactos sin dilaciones indebidas se reconoce en el artículo 16 del RGPD y está en consonancia con el principio de exactitud, mencionado anteriormente en el principio estructural de legitimidad.

El denominado "derecho al olvido" del artículo 17 del RGPD implica que el interesado puede solicitar la supresión incluso de los datos exactos sin dilaciones indebidas. Sin embargo, este derecho está limitado a determinados motivos o presupuestos habilitantes, como que los datos ya no sean necesarios para el fin perseguido o que se haya retirado el consentimiento (y no exista ninguna otra base de legitimación para el tratamiento). El responsable del tratamiento puede anonimizar los datos para atender la solicitud.

Como ya se ha mencionado en el principio estructural de proporcionalidad, el interesado puede retirar su consentimiento en cualquier momento (art. 7, apdo. 3 RGPD).

Cuando el interés legítimo o el cumplimiento de una misión realizada en interés público constituya la base legítima del tratamiento, el interesado tendrá derecho a oponerse al tratamiento (art. 21.1 RGPD). El responsable del tratamiento debe acatar la decisión, a menos que "acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones".

Cuando los datos personales se traten con fines de mercadotecnia directa, el interesado podrá oponerse en cualquier momento a dicha mercadotecnia. El uso de *cookies* y del correo electrónico con fines comerciales está regulado en la 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), reformada en 2009, y normalmente se requiere el consentimiento. Las *cookies* pueden almacenarse y accederse sin consentimiento[21] cuando "el almacenamiento técnico o el acceso sean estrictamente necesarios" para permitir "el uso de un servicio específico solicitado específicamente por el abonado o usuario".

21 Considerando 66 de la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) nº 2006/2004 sobre la cooperación en materia de protección de los consumidores.

Otros derechos del interesado incluyen el derecho a la portabilidad de los datos (art. 20 RGPD) y el derecho a no ser objeto de decisiones individuales automatizadas, incluida la elaboración de perfiles[22] (art. 22 RGPD).

4. Transparencia.

La transparencia es un principio estructural[23] del Derecho de la Unión Europea, y el tratamiento transparente de los datos personales es un requisito previo para la rendición de cuentas ante las autoridades, así como para el empoderamiento del interesado. Y este principio estructural está estrechamente relacionado con la legitimidad y la proporcionalidad.

La transparencia afecta asimismo de forma muy relevante a la obtención del consentimiento, que debe ser específico e informado. Además, la solicitud de consentimiento debe presentarse de manera que se distinga claramente de otras cuestiones, como las condiciones contractuales (art. 7, apdo. 2 RGPD).

Los artículos 13 y 14 del RGPD contienen requisitos de información exhaustivos para informar al interesado sobre la identidad y los datos de contacto del responsable del tratamiento, los fines y las categorías de los datos personales tratados y los derechos del interesado, así como otra información necesaria para garantizar un tratamiento leal y transparente con respecto al interesado. Cuando el responsable del tratamiento invoque el interés legítimo como base de legitimación para el tratamiento, el interesado deberá ser informado de los intereses legítimos perseguidos.

En el marco de la toma de "decisiones individuales automatizadas, incluida la elaboración de perfiles"[24] (art. 22 RGPD), la transparencia[25] implica proporcionar al interesado "información significativa sobre la lógica implicada", así como "la importancia y las consecuencias previstas de dicho tratamiento para el interesado" (art. 14.2.g) RGPD). A mi juicio, esta obligación podría servir de inspiración para garantizar la transparencia general en el contexto de los modelos empresariales basados en datos[26]. El señalado artículo 22 del RGPD, aplicable tanto al sector

22 STJUE de 7 de diciembre de 2023, *SCHUFA Holding (Scoring)*, (C-634/21, ECLI:EU:C:2023:957).

23 Ortega Giménez, A. (dir.): *Responsabilidad social y transparencia. Una lectura desde el Derecho internacional privado*, Pamplona, Aranzadi, 2022, pág. 220; o Bermúdez Sánchez, J. y Marcos Fernández, A. (coords.): *Transparencia, lobbies y protección de datos*, Pamplona, Aranzadi, 2020; pág. 104 y ss., así como pp. 381-382.

24 Jiménez-Castellanos Ballesteros, I.: "Decisiones automatizadas y transparencia administrativa. Nuevos retos para los derechos fundamentales", *Revista española de la transparencia*, 2023, Núm. 16, pp. 191-215.

25 Véase la STJUE de 1 de octubre de 2019, *Planet49*, (C-673/17, ECLI:EU:C:2019:801), cuyo apartado 74 establece: "una información clara y completa debe permitir al usuario determinar fácilmente las consecuencias de cualquier consentimiento que pueda dar y garantizar que dicho consentimiento se otorgue con pleno conocimiento de causa. Debe ser claramente comprensible y suficientemente detallada para que el usuario pueda comprender el funcionamiento de las cookies empleadas".

26 Barrio Andrés, M.: "Modelos de negocio basados en datos, publicidad programática, inteligencia artificial y regulación: algunas reflexiones", *IDP. Revista de Internet, Derecho y Política*, 2022, Núm. 36.

público[27] como al privado, contiene una prohibición general de adopción de decisiones totalmente automatizadas que produzcan efectos jurídicos sobre las personas físicas o que les afecten significativamente de un modo similar, prohibición que solo puede ser exceptuada en las circunstancias del apartado 2 (ser necesaria para la celebración o ejecución de un contrato; está autorizada por el Derecho de la Unión o del Estado miembro respectivo y se establezcan "medidas adecuadas[28] para salvaguardar los derechos y libertades y los intereses legítimos del interesado"; o se basa en el consentimiento del interesado).

Una reciente[29] sentencia del TJUE establece que el concepto de decisión automatizada que afecta al interesado del señalado artículo 22 del RGPD debe interpretarse en sentido amplio. Por eso, el Tribunal de Justicia ha destacado que la prohibición y restricciones específicas que establece esta norma pretenden hacer frente a los riesgos específicos que las decisiones automatizadas generan en relación con potenciales efectos discriminatorios en las personas físicas (apdo. 59). En concreto, esa interpretación amplia se considera imprescindible para evitar lagunas jurídicas en situaciones en las que están implicados varios actores, como es habitual, por ejemplo, cuando la herramienta de IA se utiliza por el prestador de un servicio para generar cierta información o valoración y comunicarla a quien posteriormente toma la decisión de contratar o no con el interesado. La nueva sentencia aclara que no solo esa última decisión puede quedar dentro del ámbito de aplicación del artículo 22 del RGPD, sino también la valoración previa en la que se basa.

Por su parte, el derecho del interesado a oponerse al tratamiento de datos personales con fines de mercadotecnia directa o basado en el interés legítimo debe hacerse constar explícitamente a más tardar en la primera comunicación con el interesado (art. 21.4 RGPD). Del mismo modo, antes de otorgar su consentimiento, el interesado debe ser informado de su derecho a retirarlo en cualquier momento (art. 7.3 RGPD).

La información facilitada al interesado debe presentarse por escrito o por otros medios (como una comunicación de voz), incluso por medios electrónicos, y

27 En España, las principales normas que establecen un régimen jurídico específico de la actuación administrativa automatizada y de la inteligencia artificial (IA) son los arts. 41 y 42 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (LRJSP). Regulan la llamada "actuación administrativa automatizada". Es conveniente precisar que no toda actuación administrativa automatizada utiliza inteligencia artificial. Pero cualquier sistema de IA sí utiliza procesos automatizados, al menos en alguna fase.

28 El considerando 71 del RGPD incluye entre tales medidas "la información específica al interesado y el derecho a obtener intervención humana, a expresar su punto de vista, a recibir una explicación de la decisión tomada después de tal evaluación y a impugnar la decisión", medidas que tienen un paralelismo con garantías básicas del procedimiento administrativo como son el derecho de audiencia, el deber de investigación minuciosa del asunto y el deber de motivación que forman parte del derecho fundamental a una buena administración del artículo 41 de la CDFUE.

29 STJUE de 7 de diciembre de 2023, *SCHUFA Holding (Scoring)*, (C-634/21, ECLI:EU:C:2023:957).

en "forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo" (art. 12.1 RGPD).

El RGPD no exige expresamente que el responsable del tratamiento publique una política de privacidad en su sitio web, pero a menudo es una forma eficaz de informar al interesado –por ejemplo, mediante un enlace o hipervínculo, o una información por capas[30]– y también de organizar el registro de actividades de tratamiento que se examina más adelante en el próximo apartado relativo a la responsabilidad proactiva.

5. Responsabilidad proactiva.

Una parte significativa de las normas sustantivas del RGPD proceden de la precitada Directiva sobre protección de datos de 1995[31], sustituida como quedó apuntado por el RGPD. Sin embargo, un cambio significativo en el modelo de cumplimiento es la adopción de un sistema de responsabilidad proactiva que enuncia el artículo 5.2 del RGPD: "[e]l responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»)".

Este principio se reitera en el artículo 24 del RGPD, según el cual el responsable del tratamiento debe aplicar "medidas técnicas y organizativas apropiadas" para garantizar y poder demostrar que el tratamiento se realiza de conformidad con el RGPD.

Estas medidas deben mantenerse actualizadas y, como se ha comentado anteriormente en el principio estructural de la proporcionalidad, deben tener en consideración la naturaleza, el alcance, el contexto y los fines del tratamiento. Los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas también deben tenerse en cuenta. La aplicación de estas medidas debe incluir cuando sean proporcionadas en relación con las actividades de tratamiento "la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos" (art. 24.2 RGPD).

En relación con el consentimiento, se exige que el responsable del tratamiento pueda demostrar que el interesado ha consentido el tratamiento (art. 7.1 RGPD).

30 Para dar cumplimiento a este derecho, la Agencia Española de Protección de Datos (AEPD) recomienda que esta información se suministre por capas o niveles de manera que se facilite al usuario una información básica en un primer nivel, de forma resumida, en el mismo momento y en el mismo medio en que se recojan los datos personales. Y, por otra parte, se le remita el resto de las informaciones detalladas en un medio más adecuado para su presentación, compresión y, si se desea, archivo.

31 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 respeta al tratamiento de datos personales y a la libre circulación de estos datos.

Una de las medidas más concretas de la responsabilidad proactiva es el requisito de mantener un registro de las actividades de tratamiento (art. 30 RGPD). El registro debe hacerse por escrito, incluso en formato electrónico, y debe contener (a) el nombre y los datos de contacto del responsable del tratamiento, (b) los fines (nótese que está en plural) del tratamiento, (c) una descripción de las categorías de interesados y de las categorías de datos personales, (d) las categorías de destinatarios a los que pueden revelarse los datos personales y (e) las posibles transferencias de datos personales a terceros países (es decir, fuera de la Unión Europea y del Espacio Económico Europeo). Cuando sea posible, el registro también deberá incluir (f) los plazos previstos para la supresión de las distintas categorías de datos y (g) una descripción general de las medidas de seguridad técnicas y organizativas aplicables a cada actividad de tratamiento[32].

El registro de las actividades de tratamiento debe estar a disposición de la autoridad de control, pero no hay obligación expresa de publicarlo, por ejemplo en forma de política de privacidad, aunque a nuestro juicio dicha publicación puede ampararse en el principio estructural de transparencia. No obstante, en la práctica, el registro de actividades de tratamiento no suele ser publicado debido a que se trata de un documento muy dinámico y que sufre un sinfín de actualizaciones.

Antes del tratamiento de datos personales que pueda entrañar un "alto riesgo" para los derechos y libertades de las personas físicas, el responsable del tratamiento debe llevar a cabo una evaluación del impacto sobre la protección de datos (EIPD o PIA, por sus siglas en inglés) del tratamiento previsto (art. 35 RGPD). Esta evaluación es necesaria, entre otros supuestos, en el caso de una "evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar".

Si la evaluación indica que el tratamiento entrañaría un alto riesgo en ausencia de medidas adoptadas por el responsable del tratamiento para mitigar el riesgo, el responsable del tratamiento deberá consultar a la autoridad de control antes del tratamiento (art. 36 RGPD).

En determinadas situaciones, el responsable del tratamiento está obligado a designar un delegado de protección de datos[33], incluso en los casos en que "las actividades principales [...] consistan en operaciones de tratamiento que, en

32 Las organizaciones con menos de 250 empleados solo deben mantener registros de las actividades de tratamiento para los tipos de tratamiento mencionados en las letras a) a c).

33 Plaza Penadés, J.: "El delegado de protección de datos o DPO (Data Protection Officer)", *Revista Aranzadi de derecho y nuevas tecnologías*, 2016, Núm. 42, pp. 19-21.

razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala" (art. 37 RGPD).

Estos requisitos también pueden considerarse ejemplos de proporcionalidad, tal como se ha comentado anteriormente.

El cumplimiento se ve reforzado por el requisito de protección de datos desde el diseño y por defecto (art. 25 RGPD). El responsable del tratamiento debe aplicar "medidas técnicas y organizativas apropiadas" para (i) garantizar el cumplimiento, (ii) integrar las salvaguardias necesarias y (iii) garantizar que sólo se tratan por defecto los datos personales necesarios. Esta disposición es nueva en el RGPD y corrobora todos los principios estructurales acuñados en este estudio.

6. Seguridad.

La seguridad de los datos personales es de vital importancia para evitar el riesgo, por ejemplo, de destrucción accidental o ilícita, pérdida, alteración, divulgación no autorizada o acceso a los datos personales transmitidos, almacenados o tratados de otro modo.

En muchos casos, la amenaza real[34] en el contexto de los datos personales no es la explotación por parte del responsable del tratamiento, sino más bien la falta de medidas de seguridad que da lugar a violaciones de los datos y a su posterior aprovechamiento por parte de terceros, incluidos, por ejemplo, empleados y subcontratistas o cibercriminales. Así, la minimización de datos y la limitación del almacenamiento, tratadas anteriormente en el principio estructural de proporcionalidad, así como la anonimización y la seudonimización, son medios para cumplir el principio de seguridad.

El responsable del tratamiento de datos debe aplicar "medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo" (art. 32 RGPD). Deben tenerse en cuenta "el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas", tal y como se ha tratado anteriormente en el principio estructural de proporcionalidad.

Las medidas de seguridad deben incluir, como mínimo (art. 32.1 RGPD):

- la seudonimización y el cifrado de datos personales;

34 Segura Serrano, A.: *El desafío de la Ciberseguridad Global*, Valencia, Tirant lo Blanch, 2023, p. 24 y ss.

- la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;

- la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;

- un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

El responsable del tratamiento de datos debe tomar medidas para garantizar que cualquier persona física que actúe bajo la autoridad del responsable del tratamiento o del encargado del tratamiento, y que tenga acceso a datos personales, no los trate salvo siguiendo instrucciones del responsable del tratamiento (art. 32.4 RGPD).

En caso de una "violación de la seguridad de los datos personales"[35], el responsable del tratamiento debe notificarlo sin demora injustificada a la autoridad de control (art. 33 RGPD) y a los interesados (art. 34 RGPD). En consonancia con el principio estructural de proporcionalidad, estos últimos sólo deben ser informados cuando sea probable que la violación de los datos personales suponga "un alto riesgo para los derechos y libertades de las personas físicas".

III. CONCLUSIONES.

Según ha quedado expuesto, los contenidos del RGPD pueden sistematizarse en seis grandes principios estructurales:

- Legitimidad. La intimidad y la protección de datos son un derecho democrático fundamental, y para afectar legalmente el derecho de los interesados a su intimidad el responsable del tratamiento debe perseguir un fin legítimo, teniendo en cuenta los intereses legítimos de los interesados, de terceros y del público, así como las obligaciones legales aplicables. Y todo ello de manera justa y ponderada.

- Proporcionalidad. La protección de los datos personales –incluidas las obligaciones del responsable del tratamiento y la necesidad de consentimiento– está en relación con la finalidad legítima perseguida, así como con el impacto sobre el derecho a la intimidad del interesado, incluidos la naturaleza, el alcance, el contexto y los fines del tratamiento.

35 Troncoso Reigada, A.: "Del principio de seguridad de los datos al derecho a la seguridad digital", *Economía Industrial*, 2018, Núm. 410, pp. 127-151.

- Empoderamiento. El interesado gobierna en gran medida qué datos que le conciernen pueden tratarse legalmente, mediante su consentimiento y los derechos de acceso, rectificación, supresión y oposición.

- Transparencia. Para estar empoderado, el interesado debe tener información sobre el responsable del tratamiento y el tratamiento efectuado. También tiene que poder comprender sus derechos y las implicaciones del tratamiento.

- Responsabilidad proactiva. El responsable del tratamiento debe ser capaz de demostrar que cumple el RGPD, por ejemplo manteniendo un registro de las actividades de tratamiento, realizando evaluaciones de impacto de la protección de datos y garantizando la protección de datos desde el diseño y por defecto.

- Seguridad. Cuando se confíen datos personales al responsable del tratamiento, deben aplicarse medidas técnicas y organizativas adecuadas para protegerlos contra el tratamiento no autorizado o ilícito, así como contra la pérdida, destrucción o daño accidentales.

Así las cosas, estos supraprincipios que hemos acuñado, muchos de rango constitucional europeo, integran el ordenamiento jurídico europeo y de los Estados miembros, están dotados de la superioridad normativa que implica su anclaje en el Derecho de la Unión Europea y cumplen una función de auxilio en el conocimiento, comprensión, aplicación e interpretación de este reglamento europeo.

BIBLIOGRAFÍA

Barrio Andrés, M.: "Inteligencia artificial: origen, concepto, mito y realidad", *El Cronista del Estado Social y Democrático de Derecho*, 2022, Núm. 100.

Barrio Andrés, M.: "La reforma de la LOPDGDD por la Ley 11/2023, de 8 de mayo", *Revista La Ley Privacidad*, 2023, Núm. 16.

Barrio Andrés, M.: "Modelos de negocio basados en datos, publicidad programática, inteligencia artificial y regulación: algunas reflexiones", *IDP. Revista de Internet, Derecho y Política*, 2022, Núm. 36.

Barrio Andrés, M.: *Internet de las Cosas*, Madrid, Reus, 2022, 3.ª edición.

Barrio Andrés, M.: *Manual de Derecho Digital*, Valencia, Tirant lo Blanch, 2022, 2.ª edición.

Bermúdez Sánchez, J. y Marcos Fernández, A. (coords.): *Transparencia, lobbies y protección de datos*, Pamplona, Aranzadi, 2020.

Bradford, A.: *The Brussels Effect: How the European Union Rules the World*, Nueva York, Oxford University Press, 2020.

Casas Baamonde, M.E.: "La plena efectividad de los derechos fundamentales: juicio de ponderación (¿o de proporcionalidad?) y principio de buena fe", *Relaciones laborales. Revista crítica de teoría y práctica*, 2004, Núm. 1.

Castillejo Manzanares, R.: "Nuevas tecnologías y prueba en el proceso penal. Especial incidencia en Inteligencia Artificial", *Derecho Digital e Innovación*, 2022, Núm. 11.

Domínguez Álvarez, J.L.: *Tratado de protección de datos personales*, A Coruña, Colex, 2023.

Gamero Casado, E. (dir.), *Inteligencia artificial en el sector público. Retos, límites y medios*, Valencia, Tirant lo Blanch, 2023.

García Roca, J. y Santaolalla, P. (coords.): *La Europa de los Derechos. El Convenio Europeo de Derechos Humanos*, Madrid, Centro de Estudios Políticos y Constitucionales, 2023, 4.ª edición.

Jiménez-Castellanos Ballesteros, I.: "Decisiones automatizadas y transparencia administrativa. Nuevos retos para los derechos fundamentales", *Revista española de la transparencia*, 2023, Núm. 16.

López Calvo, J. (coord.): *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD*, Madrid, Bosch-Wolters Kluwer, 2019.

Matia Portilla, F.J. (coord.): *De la intimidad a la vida privada y familiar*, Valencia, Tirant lo Blanch, 2020.

Ortega Giménez, A. (dir.): *Responsabilidad social y transparencia. Una lectura desde el Derecho internacional privado*, Pamplona, Aranzadi, 2022.

Plaza Penadés, J.: "El delegado de protección de datos o DPO (Data Protection Officer)", *Revista Aranzadi de derecho y nuevas tecnologías*, 2016, Núm. 42.

Rallo Lombarte, A. (dir.): *Tratado de Protección de Datos*, Valencia, Tirant lo Blanch, 2019.

Segura Serrano, A.: *El desafío de la Ciberseguridad Global*, Valencia, Tirant lo Blanch, 2023.

Troncoso Reigada, A.: "Del principio de seguridad de los datos al derecho a la seguridad digital", *Economía Industrial*, 2018, Núm. 410.

Warren, S.D. y Brandeis, L.D.: "The Right to Privacy", *Harvard Law Review*, 1890, Vol. 4, Núm. 5.

Westin, A.F.: *Privacy and Freedom*, Londres, The Bodley Head, 1970.