PROTECCIÓN DE DATOS DE SALUD Y RESPONSABILIDAD CIVIL: ALGUNOS APUNTES COMPARADOS ENTRE ESPAÑA Y PERÚ*

HEALTH DATA PROTECTION AND CIVIL LIABILITY: SOME COMPARATIVE NOTES BETWEEN SPAIN AND PERU

Actualidad Jurídica Iberoamericana Nº 22, enero 2025, ISSN: 2386-4567, pp. 176-219

Trabajo enmarcado en el Proyecto de Investigación: TED2021-129472B-00/MICINN "Next Generation EU/PRTR". "Contratación de Servicios de Telemedicina: Actualidad y Desafíos Jurídicos". Ministerio de Ciencia e Innovación. Gobierno de España. IP Profa. Dra. Raquel Luquin Bergareche. Ponencia impartida en el "Congreso Internacional de Derecho civil 2024: Cuarenta años después. El Código civil peruano y el Derecho civil del futuro, Universidad de Lima, Lima-Perú, 20 de noviembre de 2024.

Mª Ángeles
EGUSQUIZA
BALMASEDA

ARTÍCULO RECIBIDO: 18 de diciembre de 2024
ARTÍCULO APROBADO: 7 de enero de 2025

RESUMEN: La protección de datos personales conforma un derecho fundamental de tercera generación, consagrado constitucionalmente tanto en Perú como en España. En su proyección sobre los datos de salud, categoría especial de datos, aquella ofrece varios desafíos, y un régimen singular por ser pieza fundamental de la atención sanitaria. Con un planteamiento que persigue el bosquejo comparado del régimen español y peruano, se han tratado los principales retos en cuanto a la discriminación por la información oncológica, la digitalización, el uso secundario de los datos sanitarios, el tratamiento de la información por los profesionales de la salud, su deber de confidencialidad, el acceso a la historia clínica o la forma de comunicación de esa información. Se finaliza con el análisis de la responsabilidad -civil y patrimonial- por la infracción de la normativa de protección de datos y la principal doctrina jurisprudencial sobre los elementos que han de concurrir para su estimación, singularmente respecto a la valoración y cuantificación del daño moral.

PALABRAS CLAVE: Intimidad; protección de datos; datos personales; datos de salud y responsabilidad civil.

ABSTRACT: *The protection of personal data is a fundamental right of the third generation, constitutionally recognized in Peru and Spain. In its projection on health data, a special category of data, it offers several challenges, and a unique regime because it is a fundamental piece of health care. With an approach that pursues the comparative outline of the Spanish and Peruvian regime, the main challenges have been addressed in terms of discrimination due to oncological information, digitalization, the secondary use of health data, the processing of information by healthcare professionals, their duty of confidentiality, access to medical history or the way that information is communicated. The study ends with the analysis of liability - civil and patrimonial - for the violation of data protection regulations and the main jurisprudential doctrine on the elements that must be present for its estimation, particularly with respect to the assessment and quantification of moral damage.*

KEY WORDS: *Privacy; data protection; personal data; health data and civil liability.*

SUMARIO.- I. DESAFÍOS EN LA PROTECCIÓN DE DATOS DE SALUD.- 1. Marco jurídico general.- 2. Datos de salud como categoría especial de datos personales.- A) El reto de la no discriminación.- B) El reto de la amplitud de la categoría de los datos de salud.- C) Los retos de la digitalización y uso secundario de los datos sanitarios.- II. TRATAMIENTO DE LOS DATOS DE SALUD POR LOS PROFESIONALES DE LA MEDICINA: ¿QUÉ DATOS DE MI SALUD PUEDE TRATAR LEGÍTIMAMENTE EL MÉDICO?- 1. Excepciones a la necesidad de prestación del consentimiento.- 2. Confidencialidad como base de la relación: deber de secreto profesional.- 3. Acceso a la historia clínica por los profesionales de la salud.- III. ACCESO A LOS DATOS DE SALUD CONTENIDOS EN EL HISTORIAL CLÍNICO POR PARTE DE TERCEROS ¿HASTA QUÉ PUNTO PUEDEN SABER DE MIS ENFERMEDADES O TRATAMIENTOS?- 1. Acceso a la historia clínica con fines de investigación, judiciales y de salud pública.- 2. Acceso a la historia clínica por los progenitores.- IV. INFORMACIÓN SOBRE LA SALUD. LA COMUNICACIÓN POR WHATSAPP DE CIRCUNSTANCIAS DE SALUD ¿UN PROBLEMA JURÍDICO?- 1. Información sobre la salud de personas con relieve público.- 2. Forma de comunicación de los datos de salud.- V. RESPONSABILIDAD CIVIL POR VULNERACIÓN DE LA NORMATIVA DE PROTECCIÓN DE DATOS.- 1. Vías y requisitos para su exigibilidad.- 2. Casuística indemnizatoria.- 3. Información sobre la propia salud a familiares: ¿cabe la responsabilidad civil?

I. DESAFIOS EN LA PROTECCIÓN DE DATOS DE SALUD.

1. Marco jurídico general.

Uno de los retos, actuales y de futuro, a los que se enfrenta el Derecho civil es la tutela de la persona respecto a la protección de sus datos, y, en particular, de los datos o informaciones sobre la salud.

Reconocida la protección de datos personales como un derecho fundamental de tercera generación, en el avance del uso de la tecnología e intromisión en la vida privada e intimidad de la persona física -art. 12 Declaración de Derechos Humanos de 1948 y art. 17 del Pacto Internacional de Derechos civiles y Políticos de 1966-, esa se ha implementado con la seguridad digital -derecho humano de quinta generación-, habiéndose producido su consagración legislativa en la mayor parte de los ordenamientos jurídicos avanzados.

En la Unión Europa el derecho a la protección de datos constituye uno de los pilares básico de su construcción e identidad como espacio social ciudadano[1]. Tras un largo proceso previo[2], en el año 2000 se recogió en el art. 8 de la Carta Europea

1 Di Pizzo Chiacchio A.: *La expansión del derecho al olvido digital*, Atelier, 2018, pp. 33 y ss.

2 En estos antecedentes deben destacarse el art. 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales de 1950, que estableció el principio de protección de la intimidad; el Convenio n.º 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal de 1981 que garantizó la protección de datos frente al tratamiento automatizado, la Directiva 1995/46, relativa a la protección de las personas físicas en lo que respecta al

• Mª Ángeles Egusquiza Balmaseda
Catedrática de Derecho civil, Universidad Pública de Navarra. Correo electrónico: egusquiza@unavarra.es

de Derechos Fundamentales de la Unión Europea[3], ofreciéndose una configuración autónoma e independiente como derecho fundamental. El Tratado de Lisboa de 2007 lo asumió como estructural y vinculante, incorporándose al Tratado de Funcionamiento de la Unión Europea - art. 16- y al Tratado de Unión Europea - art. 39 -. Su desarrollo normativo y aplicación en la praxis diaria tiene como referente 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), norma que derogó la Directiva 95/46/CE, y que resulta de aplicación directa en todos los países de la Unión Europea. En el caso de España a ello hay que unir la regulación complementaria que ofrece la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDPGDD)[4].

Cabe recordar que, en España, el derecho fundamental a la protección de datos fue aquilatado por vía de la doctrina constitucional -SSTC 94/1998, de 4 de mayo y 292/2000, de 30 de noviembre-, en interpretación del art. 18.4 de la Constitución Española, en la que literalmente se reconoce que "la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

Un camino paralelo se ha transitado en esta materia por el ordenamiento jurídico peruano. La protección de datos personales se configura como un derecho fundamental al amparo del artículo 2.6 de la Constitución Política del Perú, al disponer que "toda persona tiene derecho (…) a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar". Con el desarrollo legislativo llevado a cabo por la Ley Nº. 29733 –Ley de Protección de Datos Personales (LPDP)-, promulgada en el año 2011, y su desarrollo reglamentario por Decreto Supremo Nº. 003-2013-JUS, se ha fijado el marco de actuación y aplicación general para hacer efectivo este derecho.

tratamiento de datos personales y a la libre circulación de estos datos, le siguieron otras directivas en la materia, y la reforma en 1997 del Tratado de la Comunidad Europea (Tratado de Ámsterdam). Este incluyó, en su art. 286, un mandato de respeto y observancia a ese derecho dirigido a las instituciones y organismos de la UE, que se materializó en el Reglamento 45/2001, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos.

3 Artículo 8. Protección de datos de carácter personal
1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.
2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.
3. El respeto de estas normas quedará sujeto al control de una autoridad independiente.

4 La preocupación en España por la protección de datos se remonta a la Ley Orgánica 5/1992, de 29 de octubre, de Tratamiento Automatizado de Datos de Carácter Personal, derogada por Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, que incorporó al ordenamiento español la Directiva de la UE 1995/46.

2. Datos de salud como categoría especial de datos personales.

A) El reto de la no discriminación.

En los sistemas jurídicos europeo-español y peruano las informaciones sobre la salud, datos de salud, conforman una categoría especial de datos sujeta a un régimen singular. El RGPD, en Europa, los incluye dentro de las categorías especiales de datos personales, art. 9.1, prohibiendo su tratamiento sin consentimiento del "interesado". En el caso de Perú, con una visión pareja, se les califica, en el art. 5 de la LPDP, como "datos sensibles", siguiendo la terminología utilizada por la anterior legislación europea y española. El motivo, la relevancia y transcendencia que podría tener el acceso y uso de esa información para la persona física. Desde la perspectiva personal, tales datos pueden influir sobre la imagen, la consideración o el juicio de valor social sobre el sujeto, al desvelar aspectos íntimos de su comportamiento – caso de la vida sexual, enfermedades estigmatizadoras, o los usos y las costumbres derivados de adicciones o dependencias, como la nomofobia o drogadicción-. Pero también puede ir más allá e implicar su discriminación con efectos relevantes en distintos ámbitos de la vida, los más significativos son la obtención de empleo o su mantenimiento por un futuro rendimiento -piénsese en el caso de quien sufre insuficiencia cardiaca crónica o una esquizofrenia-, o el acceso a la contratación de determinados bienes o servicios, como el seguro de vida o de salud, o la obtención de crédito.

En relación con esa última cuestión, cabe destacar las acciones que se han venido desplegando en Europa, auspiciadas por la Resolución del Parlamento Europeo de 16 de febrero de 2022, para impulsar el llamado "derecho al olvido oncológico" y evitar que quien sanó, tras un proceso de curación sin recidivas, resulte discriminado. En España esas medidas se han implementado, en el ámbito del seguro de vida, por el Real Decreto-ley 5/2023, de 28 de junio, art. 209, a fin de que el tomador o asegurado, cuando "hayan transcurridos cinco años desde la finalización del tratamiento radical sin recaída posterior", quede liberado de informar sobre la salud pasada, indicando la norma que "no está obligado a declarar" respecto a "si él o el asegurado han padecido cáncer" (art. 10.1 y 4 de la Ley del Contrato de Seguro -LCS-)[5]. El sentido de esta previsión se extiende, por el art. 210 del RDL 5/2023, al ámbito contractual de consumo a través de la disposición adicional única del TRLGDCU. Este precepto establece la nulidad de las "cláusulas, estipulaciones, condiciones o pactos" que excluyan a uno de los contratantes por padecer VIH/SIDA u otras condiciones de salud[6], extendiéndose

5 Egusquiza Balmaseda, M.A.: "Olvido oncológico protección de datos de salud y no discriminación", *Revista de Derecho, Empresa y Sociedad (REDS)*, 22-23,2023, pp. 24 y ss.; Torrelles Torrea, E.: *El derecho al olvido oncológico*, Atelier, 2024, pp. 79 y ss.

6 García Goldar, M.: "Disposición adicional única", en Cañizares Laso A. (dir.), *Comentarios al Texto Refundido de la Ley de Consumidores y Usuarios*, Tirant lo Blanch, T. II., 2022, pp. 2466 y ss.

el régimen a quienes padecieron "cáncer antes de la fecha de suscripción del contrato o negocio jurídico, una vez que hayan transcurrido cinco años desde la finalización del tratamiento radical sin recaída posterior". Y se impone la sanción de nulidad de las que, "de forma previa a la suscripción de un contrato de consumo, independientemente del sector", exijan "solicitar a la persona consumidora información oncológica una vez que hayan transcurrido cinco años desde la finalización del tratamiento radical sin recaída posterior".

La inquietud por este tema se comparte en Perú, que encamina su regulación por derroteros legislativos próximos al existente en España. Así, la Comisión de Salud y Población de Perú ha aprobado el 5 de marzo de 2024 una propuesta normativa, recogiendo los Proyectos de Ley 5790/2023-CR y 6297/2023-CR[7], sobre el olvido oncológico en la contratación de servicios y seguros de salud; hallándose ésta, en el momento presente, en tramitación parlamentaria.

Ese texto sustitutorio del proyecto normativo fija como finalidad, art. 1, la garantía del derecho a la igualdad y no discriminación de las personas que hubieran superado una patología oncológica, circunscribiendo su ámbito de actuación a los servicios o seguros de salud. Se deja fuera, quizá por ahora, la contratación financiera.

En el art. 2 se delimita qué se entiende por el derecho al "olvido oncológico": la no consideración de los antecedentes sobre la enfermedad de las personas que la hayan superado, a los efectos de aquellas contrataciones. Para ello se requiere un "diagnóstico de la patología oncológica" y que hayan transcurrido "cinco años desde que la persona contratante superó la enfermedad". Se plantea un modelo parecido al fijado en España y Francia que no fija salvedades para esta exigencia en función de la edad, apartándose del Proyecto 5790/2023-CR, que reducía a 3 años el plazo para el caso de los menores de 18 años. Los problemas sustantivos relevantes sobre el "dies a quo" del inicio del plazo, qué ha de entenderse por "superación de la patología oncológica" y a qué actos o tratamientos médicos habría que ligarlos -cirugías, trasplantes, inmunoterapias, etc.-, la definición de "episodios de recurrencia", así como la manera que deberá acreditarse todo ello, se dejan para el ulterior desarrollo reglamentario. Previsión que resulta especialmente oportuna para conjugar la necesaria efectividad del derecho del particular con la demanda de seguridad jurídica que reclama el sector asegurador.

Finalmente, el art. 3 concreta el alcance del "olvido oncológico", delimitando los tres derechos de interesado:

7 En cuanto a estos textos previos, cfr. Torrelles Torrea, E.: *El derecho,* cit., 2024, pp. 203 a 205.

1º) El acceso a la contratación de servicios o seguros de salud para los "expacientes" oncológicos; esto es, las personas que han sido dadas de alta y, estimados como "curados", se encuentren en esa situación, tras cinco años sin "episodios de recurrencia". Ello no implica que se garantice, en todo caso, la contratación. Esta podría ser denegada por motivos o circunstancias que afecten a otros aspectos de la vida o salud de la persona.

2º) La consideración y declaración de "nulidad de las cláusulas, condiciones, exclusiones, restricciones o discriminación de cualquier forma en la contratación de los servicios o seguros de salud". El texto de la norma no anuda explícitamente, y de forma clara, tal sanción a la superación de la enfermedad oncológica y transcurso de los cinco años, lo cual bien podría dar lugar a una intelección abierta del sentido de la discriminación que comprenda otras situaciones. No obstante, dado que tales previsiones se hallan ligadas al supuesto de hecho definido, que es el "olvido oncológico", la interpretación más acorde del precepto tendría que estar ligada únicamente a este supuesto.

3º) La obligación del prestador del servicio o asegurador, consecuente al derecho del titular, de que no pueda "considerar(se) la existencia de antecedentes oncológicos para los efectos de la contratación", lo cual supondrá que haya que adoptar medidas adecuadas para que ese dato de salud no se requiera en los cuestionarios de declaración del riesgo y no tenga entidad para la valoración actuarial en cuanto a la contratación de (art. 8 y 13 Ley de Contrato de Seguro, nº 29946).

B) El reto de la amplitud de la categoría de los datos de salud.

En el momento presente el tratamiento de la información de los datos relativos a la salud plantea también otros desafíos que parten de la propia dimensión de esas informaciones digitalizadas. Cabe recordar que, según el art. 4. 15 del RGPD de la UE, son "datos relativos a la salud":

"(los) datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud".

Aclarándose en el considerando 35 del Reglamento que:

"Entre los datos personales relativos a la salud se deben incluir todos los datos relativos al estado de salud del interesado que dan información sobre su estado de salud física o mental pasado, presente o futuro. Se incluye la información sobre la persona física recogida con ocasión de su inscripción a efectos de asistencia sanitaria, o con ocasión de la prestación de tal asistencia, de conformidad con la

Directiva 2011/24/UE del Parlamento Europeo y del Consejo (1); todo número, símbolo o dato asignado a una persona física que la identifique de manera unívoca a efectos sanitarios; la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente, por ejemplo un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in vitro".

Por tanto, la consideración como dato de salud no sólo se halla ligada a la asistencia sanitaria directa o indirecta de los entornos hospitalarios o de mutuas de salud laboral, sino que comprende cualquier contexto en el que se ofrezca esa información.

A ese respecto resulta interesante lo destacado por la reciente STS de España, de 8 octubre 2024, dictada por la Sala Tercera, de lo Contencioso-administrativo, n.º 1568/2024[8], en relación con la actuación de la Agencia Española de Protección de la Salud en el Deporte (AEPSAD), que negaba que los "datos de dopaje" pudieran ser considerados datos personales de salud, con el régimen de protección reforzada previsto en la normativa de protección de datos de carácter personal, y que le fuera aplicable el régimen sancionador dispuesto en la LOPDGDD y RGPD. La cuestión fáctica de fondo, la publicación en la página web de dicha Agencia de una resolución en la que se incluían las alegaciones, con nombre y apellidos de los afectados, sobre la ingesta de un medicamento al que se achacaba el dopaje, y denuncia a la Agencia Española de Protección de Datos (AEPD) de la vulneración por AEPSAD de la normativa de protección datos. El tema tiene su interés por cuanto la lucha contra el dopaje en el deporte tiene una dimensión especial, como se reconoce en la resolución:

"esta Sala considera que el Tribunal de instancia ha realizado una interpretación que estimamos adecuada y razonable del término 'datos referentes a la salud', a que alude el artículo 7.3 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en relación con la inclusión en esta categoría de datos aquellos datos relacionados con el dopaje de los deportistas, a los efectos de dispensar al tratamiento de esta clase de datos la protección reforzada que garantizaba dicha Ley Orgánica, y considerar aplicable, en los supuestos de incumplimiento, las sanciones correspondientes al tipo de infracción muy grave previsto en el artículo 44.4 b) de la citada Ley Orgánica.

8 https://www.poderjudicial.es/search/: ECLI: ES:TS: 2024:4954

En efecto, sostenemos que esta interpretación del artículo 7.3 de la Ley Orgánica 15/1999 se revela conforme con la legislación de la Unión Europea y la normativa estatal en materia de protección de datos personales y se ajusta, también, a la normativa nacional e internacional antidopaje, cuya finalidad es garantizar la equidad y la igualdad en las competiciones deportivas, asociado al concepto de juego limpio, promover la salud de los deportistas, y proteger y tutelar el bien comunitario de la salud pública, en la medida que estos datos, que conciernen a las condiciones fisiológicas o genéticas, o al estado de salud física o mental de los mismos, pueden tener repercusiones significativamente negativas para los interesados.

Por ello, debemos descartar, en primer término, que la sentencia impugnada haya efectuado una incorrecta interpretación del término 'datos de salud' del 7.3 de la Ley Orgánica, 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, a partir del artículo 4.15 y el considerando 35 del Reglamento general de protección de datos, que no es conforme -según aduce la defensa letrada de la parte recurrente- con la aplicación e interpretación retroactiva de la disposición adicional décimo séptima de la Ley Orgánica 3/2013, de 20 de junio, de protección de la salud del deportista y lucha contra el dopaje en la actividad deportiva, referido a los tratamientos de datos de salud, ya que apreciamos que el enunciado de diversas leyes referidas a la protección de la salud, no invalida la consideración de los datos referidos al dopaje como datos de salud.

Cabe subrayar, al respecto, que la lectura del artículo 4.15 y del considerando 35 del Reglamento General de Protección de Datos avalan, tal como sostiene la sentencia de la Audiencia Nacional impugnada, la inclusión de la noción de 'datos relativos a la salud' de los datos referidos al estado de salud de los deportistas, pues, aunque la normativa de la Unión Europea no contiene ninguna previsión especifica acerca de los datos relacionados con la aplicación de las técnicas de control del dopaje, define en un sentido amplio el tratamiento de los datos de salud".

La conclusión a la que llega el Tribunal Supremo, manteniendo la sanción por la falta de anonimización de la resolución publicada por AEPSAD, tanto en cuanto al nombre del interesado como al borrado de la información sobre los aspectos de la ingesta del medicamento, es que:

"(…) los datos de carácter personal referidos a información sobre el estado de salud física o mental de los deportistas, relacionados con la aplicación de las técnicas del control de dopaje, (como los concernientes a la detección de la presencia de sustancias dopantes o de resultado de pruebas analíticas antidopaje), tienen el carácter tipológico o categorial de datos relativos a la salud, a los efectos de que el tratamiento, cesión o comunicación de dichos datos goce de la protección

reforzada que contempla la normativa estatal y la legislación de la Unión Europea sobre protección de datos personales aplicable".

Estas consideraciones son igualmente aplicables al régimen jurídico de protección de datos que rige en Perú. A este respecto cabe recordar que el Reglamento de la LOPD (Decreto Supremo n.º 003-2013-JUS) acota, en su art. 5, que conforma dato personal relacionada con la salud: "aquella información concerniente a la salud pasada, presente o pronosticada, física o mental, de una persona, incluyendo el grado de discapacidad y su información genética".

Dentro de este ámbito se incluyen también, aunque no seamos conscientes, la información que proporcionamos con wearables y apps, por ejemplo, de wellness, fitness, contador de calorías o pasos, así como otras informaciones que se encuentran vinculadas a la salud, o prestación de servicios sanitarios públicos o privados. Buena parte de esa información, incluida la que se recoge en los actos médicos a los que nos hemos sometidos, se refleja en la historia clínica que, en el momento presente, se encuentra generalmente digitalizada.

C) Los retos de la digitalización y uso secundario de los datos sanitarios.

Como en ningún otro sector, la digitalización de los servicios de salud y la obtención de valor de los datos sanitarios se perciben como una necesidad para hacer sostenible el sistema de atención sanitaria pública, y que ésta llegue a toda la población a un coste razonable, se pueda responder a las amenazas por pandemia, así como avanzar en el conocimiento y tratamiento médico personalizado con la asistencia de la Inteligencia Artificial (IA). En el centro de todo ello se encuentra el tratamiento de los datos de salud y el reto que supone la protección del derecho individual versus el logro de esos objetivos.

En la Unión Europea, tras la experiencia vivida con el Covid-19, se ha acelerado el proceso para lograr esos objetivos, avanzándose en la norma que servirá de base jurídica para ello, el inminente Reglamento sobre el Espacio Europeo de Datos de Salud (REEDS)[9]. El objetivo de aquella, descrito en su Considerando 1º[10]:

"… es crear el Espacio Europeo de Datos de Salud (EEDS) con el fin de mejorar el acceso por parte de las personas físicas a sus datos de salud electrónicos personales y su control de dichos datos, en el contexto de la asistencia sanitaria, así como de alcanzar mejor otros fines para los que se necesite el uso de datos de

9 Alkorta Idiakez, I.: *El espacio europeo de datos sanitarios: nuevos enfoques de la protección e intercambio de datos sanitarios*, Thomson-Reuters Aranzadi, 2022, pp. 253 y ss.; Navas Navarro, S.: *Datos sanitarios electrónicos. El espacio europeo de datos sanitarios,* Reus, 2023, pp. 13 y ss.

10 Se corresponde con la versión de la Propuesta de Reglamento UE del Parlamento y del Consejo relativo al Espacio Europeo de Datos de Salud, y por el que se modifican la Directiva 2011/24/UE y el Reglamento (UE) 2024/2847 de 27 de noviembre de 2024.

salud electrónicos en el sector de la asistencia sanitaria y en el sector asistencial que beneficiarían a la sociedad, como, por ejemplo, la investigación, la innovación, la formulación de políticas, la preparación y respuesta ante las amenazas para la salud, incluidas la prevención y respuesta ante futuras pandemias, la seguridad de los pacientes, la medicina personalizada, las estadísticas oficiales o las actividades de regulación. Además, la finalidad del presente Reglamento es mejorar el funcionamiento del mercado interior mediante el establecimiento de un marco jurídico y técnico uniforme, en particular en lo que respecta al desarrollo, la comercialización y el uso de los sistemas de historia clínica electrónica (en lo sucesivo, 'sistemas HCE') de conformidad con los valores de la Unión. El EEDS va a ser una pieza clave para la creación de una Unión Europea de la Salud fuerte y resiliente".

Las lógicas reticencias de un uso secundario de los datos de salud[11] que pueda perjudicar directa o indirectamente a la persona física están presentes en el texto de la norma. Por ello, además de que los datos se encuentren bajo el control y supervisión de los "organismos de acceso a los datos de salud" (art. 55.1 REEDS)[12], que serán los que den "acceso" a ellos, el tratamiento tendrá que realizarse,

11 El art. 51 REEDS identifica como categoría mínima de datos secundarios a los siguientes: a) datos de salud electrónicos procedentes de HCE; b) datos sobre factores que influyen en la salud, incluidos los socioeconómicos, ambientales y de comportamiento determinantes para la salud; c) datos agregados sobre las necesidades de asistencia sanitaria, los recursos asignados a la asistencia sanitaria, la prestación de asistencia sanitaria y el acceso a la misma, el gasto de asistencia sanitaria y su financiación; d) datos sobre patógenos que influyen en la salud humana; e) datos administrativos relacionados con la asistencia sanitaria, incluidos los datos sobre dispensación, solicitudes de reembolso y reembolsos; f) datos genéticos, epigenómicos y genómicos humanos; g) otros datos moleculares humanos, como datos proteómicos, transcriptómicos, metabolómicos, lipidómicos y otros datos ómicos; h) datos de salud electrónicos personales generados automáticamente mediante productos sanitarios; i) datos procedentes de aplicaciones de bienestar; j) datos sobre la situación profesional, la especialización y el establecimiento de los profesionales sanitarios que dispensan tratamiento a una persona física; k) datos procedentes de registros de datos de salud de base poblacional (como, por ejemplo, registros de salud pública); l) datos procedentes de los registros médicos y los registros de mortalidad; m) datos procedentes de ensayos clínicos, estudios clínicos, investigaciones clínicas y estudios de rendimiento a los que se aplica el Reglamento (UE) n.º 536/2014, el Reglamento (UE) 2024/1938 del Parlamento Europeo y del Consejo35, el Reglamento (UE) 2017/745 o el Reglamento (UE) 2017/746; n) otros datos de salud procedentes de productos sanitarios; o) datos procedentes de los registros de medicamentos y productos sanitarios; p) datos procedentes de grupos de investigación, cuestionarios y encuestas relacionadas con la salud, tras la primera publicación de los resultados correspondientes; q) datos de salud procedentes de biobancos y bases de datos asociadas.

12 "Los Estados miembros designarán uno o varios organismos de acceso a datos de salud responsables de cumplir las funciones y obligaciones establecidas en los artículos 57, 58 y 59. Los Estados miembros podrán crear uno o varios nuevos organismos del sector público o recurrir a organismos del sector público existentes o a servicios internos de organismos del sector público que cumplan las condiciones establecidas en el presente artículo. Las funciones establecidas en el artículo 57 podrán repartirse entre diferentes organismos de acceso a datos de salud. Cuando un Estado miembro designe varios organismos de acceso a datos de salud, elegirá a uno de ellos para actuar como coordinador, con la responsabilidad de coordinar las funciones con los demás organismos de acceso a datos de salud, tanto en el territorio de ese Estado miembro como en los demás Estados miembros.
Todos los organismos de acceso a datos de salud contribuirán a la aplicación coherente del presente Reglamento en toda la Unión. A tal fin, los organismos de acceso a datos de salud cooperarán entre sí, con la Comisión y, por lo que respecta a cuestiones relacionadas con la protección de datos, con las autoridades de control pertinentes".

de manera inexorable[13], solo para determinados fines, fijándose un elenco de "numerus clausus" que evite efectos indeseados. Estos son:

"a) el interés público en el ámbito de la salud pública o la salud laboral, por ejemplo actividades destinadas a la protección contra las amenazas transfronterizas graves para la salud, la vigilancia de la salud pública o actividades destinadas a garantizar unos niveles elevados de calidad y seguridad de la asistencia sanitaria, incluida la seguridad de los pacientes, y de los medicamentos o productos sanitarios;

b) las actividades de formulación de políticas y de regulación en apoyo a los organismos del sector público o a las instituciones, órganos u organismos de la Unión, incluidas las autoridades reguladoras, en el sector sanitario o en el sector asistencial en el desempeño de las funciones definidas en sus mandatos;

c) las estadísticas tal como se definen en el artículo 3, punto 1, del Reglamento (CE) n.º 223/2009 como, por ejemplo, las estadísticas oficiales nacionales, plurinacionales y de la Unión relativas al sector sanitario o en el sector asistencial;

d) las actividades de educación o de enseñanza en el sector sanitario o asistencial a nivel de formación profesional o educación superior;

e) la investigación científica relacionada con el sector sanitario o asistencial que contribuya a la salud pública o a la evaluación de tecnologías sanitarias o que procure niveles elevados de calidad y seguridad de la asistencia sanitaria, de los medicamentos o de los productos sanitarios, con el objetivo de beneficiar a los usuarios finales, como los pacientes, los profesionales sanitarios y los administradores sanitarios, incluidas:

i) las actividades de desarrollo e innovación para productos o servicios;

ii) el entrenamiento, la prueba y la evaluación de algoritmos, también con respecto a productos sanitarios, productos sanitarios para diagnóstico in vitro, sistemas de IA y aplicaciones sanitarias digitales;

f) la mejora de la prestación de asistencia, la optimización de los tratamientos y la prestación de asistencia sanitaria, sobre la base de los datos de salud electrónicos de otras personas físicas".

Se ha previsto, igualmente, un régimen de prohibición de utilización que incide en la médula de la defensa que se persigue con la tutela de la protección de los datos personales en este ámbito. Su enunciación resulta por sí misma expresiva y refleja los peores temores del empleo que pudiera darse aquella información. Así,

13 Navas Navarro, S.: *Datos sanitarios*, cit., 2023, pp. 231 y ss.

no podrá accederse para un uso secundario de los datos de salud, según dispone el art. 54 REEDS, cuando la finalidad sea:

"a) tomar decisiones perjudiciales para una persona física o un grupo de personas físicas sobre la base de sus datos de salud electrónicos; para ser calificadas de "decisiones" a efectos del presente punto, deben producir efectos jurídicos, económicos o sociales, o afectar de manera igualmente significativa a dichas personas físicas;

b) tomar decisiones en relación con una persona física o un grupo de personas físicas por lo que respecta a ofertas de empleo, ofrecerles condiciones menos favorables en la provisión de bienes o servicios, incluida la exclusión de dichas personas o grupos del beneficio de un contrato de seguro o de crédito, la modificación de sus cotizaciones y primas de seguro o condiciones de préstamo, o tomar cualquier otra decisión respecto de una persona física o un grupo de personas físicas que resulte en una discriminación contra ellos sobre la base de los datos de salud obtenidos;

c) realizar actividades de publicidad o mercadotecnia;

d) desarrollar productos o servicios que puedan perjudicar a las personas, a la salud pública o a la sociedad en general, por ejemplo, drogas ilegales, bebidas alcohólicas, productos del tabaco y nicotina, armamento o productos o servicios diseñados o modificados de manera que creen adicción, contravengan el orden público o pongan en riesgo la salud humana;

e) realizar actividades que entren en conflicto con disposiciones de Derecho nacional en materia de ética".

Estos apuntes permiten colegir hacia dónde se encamina la tutela de la protección de los datos de salud en un futuro, que ya es una presente real con resabios distópicos.

II. TRATAMIENTO DE LOS DATOS DE SALUD POR LOS PROFESIONALES DE LA MEDICINA: ¿QUÉ DATOS DE MI SALUD PUEDE TRATAR LEGÍTIMAMENTE EL MÉDICO?

1. Excepciones a la necesidad de prestación del consentimiento.

La regla de la prohibición del tratamiento de los datos de salud sin el consentimiento del interesado, persona física a la que se encuentra referida aquellos, presenta también excepciones muy relevantes en las que, incluso en contra de la voluntad del interesado, cabe la posibilidad de acceder a esa

información, transmitirla o procesarla. Ningún derecho tiene carácter absoluto y su virtualidad protectora debe ceder ante determinados intereses colectivos, dignos de respeto, debiéndose armonizar con los restantes bienes a los que el ordenamiento jurídico presta su tutela.

A tal efecto contempla, en la UE, el art. 9.2 del RGPD que se pueden tratar los datos de salud de la persona física, aunque ésta no haya prestado su consentimiento, entre otros casos, cuando:

"c) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento…

h) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3; …

i) el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional".

Ello supone, por ejemplo, que no será preciso pedir autorización para acceder a la historia clínica de quien ha sufrido un accidente o un infarto a fin de realizar la atención médica. Tampoco se precisará tal consentimiento cuando nos incluyan por edad en planes públicos de prevención de determinadas enfermedades en las políticas que se llevan de prevención, por ejemplo, de cáncer de mama para las mujeres mayores de 40 años o del cribado de colón, desarrollado en algunas Comunidades Autónomas en España como es el caso de Navarra. Ni se precisará aquel en el tratamiento de los datos de las enfermedades legalmente previstas como de declaración obligatoria en aras de la vigilancia epidémica -fiebre amarilla, el virus de Nilo, dengue, etc.-, definidas en España por la Orden SSI/445/2015, de 9 de marzo, por la que se modifican los anexos I, II y III del Real Decreto 2210/1995, de 28 de diciembre, por el que se crea la Red Nacional de Vigilancia Epidemiológica, relativos a la lista de enfermedades de declaración obligatoria, modalidades de declaración y enfermedades endémicas de ámbito regional,

y en Perú por la Directiva Sanitaria n.º 406 MINSA/DGE de notificación de enfermedades y eventos sujetos a vigilancia epidemiológica en salud pública.

En todos estos supuestos el tratamiento de los datos tiene como base legitimadora la previsión legal que, en realidad, no hacen más que poner de relieve y concretar el alcance del derecho a la protección de datos cuando colisiona con otros derechos; caso del derecho fundamental de toda persona física a la vida y la integridad física, previsto en España en el art. 15 de la CE, o el derecho colectivo de todos los ciudadanos a la protección de su salud y su garantía de organización y tutela por los poderes públicos, con la dispensa de medidas preventivas, prestaciones y servicios necesarios, al que alude el art. 43.1.2 de la CE.

Tal habilitación va ligada a dos elementos centrales que garantizan que el acceso a esos datos de salud y tratamiento in-consentido resulte adecuado y proporcionado en su conflicto con el derecho individual a la intimidad. Estos son, art. 9.3 del RGPD, la condición de "profesional", de quien ha de desarrollar aquellas labores de atención sanitaria o de salud, y su sujeción "a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con el Derecho de la Unión o de los Estados miembros o con las normas establecidas por los organismos nacionales competentes, o por cualquier otra persona sujeta también a la obligación de secreto de acuerdo con el Derecho de la Unión o de los Estados miembros o de las normas establecidas por los organismos nacionales competentes"; previsión que se fija igualmente en el art. 5 de la LOPDGDD que rige en España[14].

Este mismo planteamiento se acoge en la LPDP de Perú. El título II, dedicado al tratamiento de datos personales, dispone en el art. 14 las limitaciones a la prestación del consentimiento, exonerando de tal exigencia para su tratamiento:

"6. Cuando se trate de datos personales relativos a la salud y sea necesario, en circunstancia de riesgo, para la prevención, diagnóstico y tratamiento médico o quirúrgico del titular, siempre que dicho tratamiento sea realizado en establecimientos de salud o por profesionales en ciencias de la salud, observando el secreto profesional; o cuando medien razones de interés público previstas por ley o cuando deban tratarse por razones de salud pública, ambas razones deben ser calificadas como tales por el Ministerio de Salud; o para la realización

14 "1. Los responsables y encargados del tratamiento de datos, así como todas las personas que intervengan en cualquier fase de este, estarán sujetas al deber de confidencialidad al que se refiere el artículo 5.1.f) del Reglamento (UE) 2016/679.
2. La obligación general señalada en el apartado anterior será complementaria de los deberes de secreto profesional de conformidad con su normativa aplicable.
3. Las obligaciones establecidas en los apartados anteriores se mantendrán aun cuando hubiese finalizado la relación del obligado con el responsable o encargado del tratamiento".

de estudios epidemiológicos o análogos, en tanto se apliquen procedimientos de disociación adecuados".

2. Confidencialidad como base de la relación: deber de secreto profesional.

En el ámbito sanitario la confidencialidad supone una obligación ética exigible y sancionada por los Colegios Profesionales, que se halla plasmada en sus textos deontológicos; en el caso de España, para el sector médico, en el Código de Deontología Médica (CDM). El art. 27.2 del CDM reseña, a este respecto, que el secreto profesional comporta "la obligación de mantener la reserva y la confidencialidad de todo aquello que el paciente le haya revelado y confiado, de lo que haya visto y deducido, incluyendo el contenido de la historia clínica, como consecuencia de su ejercicio profesional, y que tenga relación con la salud y la intimidad del paciente"[15]. Estas previsiones son parejas a las que fijan los arts. 89[16] y 90[17] del Código de Deontología Médica del Perú.

Esta obligación de secreto profesional, sin embargo, implica y va mucho más allá. Conforma una obligación jurídica cuyo incumplimiento se encuentra sujeto a la máxima reacción que fija el ordenamiento, como es la sanción penal. Un incumplimiento injustificado de la confidencialidad o deber de secreto por el profesional sanitario da lugar a la comisión del delito de descubrimiento y revelación de secretos, tipificado en el art. 199.2 del Código Penal español[18] y en el art. 165 del Código Penal peruano[19].

Aunque no nos detendremos a analizar el tema de los supuestos en los que ese deber de sigilo puede quedar atemperado, sí que resulta interesante recordar las situaciones en las que la ley limita ése[20]. En España son los supuestos

15 Código de Deontología Médica. Guía de ética Médica, Organización médica colegial de España (OMC). Consejo General de Colegios Oficiales de Médicos, 2022, p. 35.

16 El médico debe mantener el secreto profesional para proteger el derecho paciente a la confidencialidad de los datos que le ha proporcionado, no debiendo divulgarlos, salvo expresa autorización del paciente.

17 El médico debe guardar reserva o la confidencialidad sobre el acto médico practicado por él o del que hubiere podido tomar conocimiento en su condición de médico consultor, auditor o médico legista. Este deber se extiende a cualquier otra información que le hubiere sido confiada por el paciente o por su familia con motivo de su atención o de su participación en una investigación. La muerte del paciente no exime al médico del cumplimiento de este deber.

18 El profesional que, con incumplimiento de su obligación de sigilo o reserva, divulgue los secretos de otra persona, será castigado con la pena de prisión de uno a cuatro años, multa de doce a veinticuatro meses e inhabilitación especial para dicha profesión por tiempo de dos a seis años.

19 El que, teniendo información por razón de su estado, oficio, empleo, profesión o ministerio, de secretos cuya publicación pueda causar daño, los revela sin consentimiento del interesado, será reprimido con pena privativa de libertad no mayor de dos años y con sesenta a ciento veinte días-multa.

20 En España el art. 31.1 del CDM (2022, p. 38) indica "El secreto profesional es la regla y se debe preservar hasta donde sea posible. El médico podrá revelar el secreto en sus justos límites en los siguientes casos: 1. En las certificaciones de nacimiento y defunción. 2. En los partes de lesiones. 3. Cuando actúa como perito inspector médico forense instructor o similar. 4. Cuando es requerido como testigo. 5. En los casos de maltrato. 6. En las enfermedades de declaración obligatoria. 7. En los casos sospechosos de trata de personas y de tráfico de órganos. 8. Cuando sea llamado por el Colegio a testificar en materia disciplinaria. 9. Cuando con su silencio perjudicará de forma grave al propio paciente o a otras personas o produjera un

de colaboración para la persecución de delitos públicos -paciente que recibió un navajazo o disparo- (art. 9.2.f) RGPD y arts. 262 y 263 LECrim); la obligación de información de enfermedades infectocontagiosas sujetas a declaración obligatoria –Orden SSI/445/2015, de 9 de marzo, en España, y la Directiva Sanitaria n.º 406 MINSA/DGE, en Perú-; y la remisión del parte informativo de nacimiento o aborto y defunción al Registro civil -arts. 44 y 62 LRC -.

¿Hay infracción de ese deber de confidencialidad si el médico que conoce de la patología de un paciente, infectado de sífilis o VIH por una relación extramatrimonial, que puede causar un daño a tercero -su cónyuge-, comunica esa información al tercero? Tanto el Código de Deontología Médica de España -art. 31.1.9- como el del Perú -art. 91- eximen al médico de ese deber de confidencialidad en aras de evitar la producción del daño. Esta primera idea queda matizada por el hecho de que, para que tal actuación resulte justificada, ha de existir un peligro actual e inminente de generación del daño y la revelación de la información debe ser el único medio e idóneo para evitar ese peligro[21]. A este respecto, por lo que se refiere al VIH, se ha señalado que ello resultará pertinente cuando: a) el afectado por el virus se ha negado explícitamente a informar sobre su situación a su compañero sexual y a utilizar métodos eficaces de barrera; b) la persona que se encuentra en situación de riesgo debe carecer de razones para sospechar la existencia de ese peligro; c) se ha evaluado el peligro real de infección, ya que la transmisión del VIH se produce por actuaciones concretas; y d) la persona destinataria de esa información es identificable y susceptible de localización[22].

Un caso interesante, en el que se planteó esta cuestión, ligada al ámbito del deber de secreto profesional y comunicación del padecimiento del sida, fue el resuelto por el AAP de Barcelona 1141/2012, de 3 de diciembre de 2012, Rec. 409/2012, (JUR\2013\23888), en el que se decretó el sobreseimiento provisional de la causa penal. Quien la instó se había matriculado en l'Instut d'Educació Secundaría La Ferreira, para cursar el ciclo formativo de grado superior de higiene bucodental, poniendo en conocimiento de su tutora que era portador del VIH. El alumno denunció a su tutora imputándole la comisión del delito de revelación de secreto por haber comunicado este dato de salud a los profesores que impartían docencia de teoría y práctica de higiene bucodental. La Audiencia considera que:

"Es cierto, que hay una diferenciación entre las clases prácticas y las clases teóricas, pese a que al final existe un crédito de síntesis, pero las profesoras que

peligro colectivo. 10. Cuando el paciente a quien se refiere la información solicite o autorice la revelación de la misma".

21 Egusquiza Balmaseda, M.A.: *Protección de datos: intimidad y salud*, Cuadernos de Aranzadi civil, Aranzadi-Thomson Reuters, 2009, pp. 32 y ss.

22 De Miguel Sánchez, N.: *Tratamiento de datos personales en el ámbito sanitario: intimidad "versus" interés público"*, Tirant lo Blanch, Valencia, 2003, pp. 122 y ss.

lo hicieron actuaron creyendo que era imprescindible, tanto para realizar una reasignación y reagrupación de las clases del denunciante para el que resto de los alumnos nada supieran, y por qué entendieron que en el crédito de síntesis participaban todo el profesorado… que si bien revelar la identidad y situación del perjudicado al resto de los profesores no se hizo con la sensibilidad mínima requerida, sin embargo los hechos que se denuncian carecen en sí mismos de relevancia penal, por lo que procede confirmar la resolución recurrida, al no ser constitutivos del delito de revelación de secretos –ex art. 199 C -, como tampoco cabe incardinarlos en el art. 511 CP".

Otra fue la solución que se ofreció por la SAP de Zaragoza de 27 de julio de 2011, n.º 261/2011, Rec. 157/2011, que condenó por revelación de secreto a una profesional técnica de laboratorio que comentó a sus compañeros que había una persona de la Clínica que estaba enferma de sida, dio su nombre, e indicó que no sabía cómo decírselo. Una de las personas a las que aquella le confió tal información, se lo dijo después a otra compañera de trabajo, y ésta le comunicó al interesado lo que la primera había dicho sobre él. A la profesional técnica de laboratorio se le abrió un expediente disciplinario, y se le condenó penalmente con un año de cárcel, argumentándose que:

"es cierto que tal dato fue conocido por la recurrente en el uso de sus obligaciones laborales como técnico de laboratorio, viniendo obligada a la confidencialidad del mismo, confidencialidad que vulneró al propagarlo a terceros extraños al laboratorio, el hecho de que pudieran ser conocidos por los miembros del mismo, no suponen la imposibilidad de punición respecto de la hoy recurrente, pues propago el dato a terceros que no tenían por qué conocerlo".

El interés del pronunciamiento radica, además, en la valoración de la responsabilidad civil derivada de este delito. En la sentencia se apreció la existencia de un daño moral, que habiéndose cuantificado inicialmente en 2.000 euros se elevó por el Tribunal de Apelación a 6.000 euros, bajo la argumentación de que:

"el daño moral es un concepto que acoge, expansivamente, el 'precio del dolor', esto es el sufrimiento, el pesar, la amargura y la tristeza que el delito puede originar, sin necesidad de ser acreditados cuando fluye lógicamente del suceso acogido en el hecho probado. No puede sin embargo soslayarse que ese daño moral se proyecta, dentro del libre arbitrio judicial, en el "cuantum" definitivo que supone la evaluación de unos daños indirectamente económicos porque no tienen una repercusión económica inmediata.

La doctrina jurisprudencial (Sentencias de 28 de abril de 1995 , y 2 de marzo de 1994) tiene señalado que el daño moral solo puede ser establecido mediante un juicio global basado en el sentimiento social de reparación del daño producido

por la ofensa de la víctima, por lo cual deberá atenderse a la naturaleza y gravedad del hecho, no siendo necesario que ese daño moral, consecuencia misma del hecho delictivo no se olvide, tenga que concretarse en determinadas alteraciones patológicas o psicológicas.

Así la cuestión, habida cuenta la consideración peyorativa que implica el conocimiento del dato de la enfermedad que padece - portador del virus de V. I. H-, entiende la Sala que es más ajustado el conceder una indemnización de 6.000 euros, mayor que la exigua concedida en la sentencia y que la excesiva solicitada por las acusaciones tanto pública como privada".

3. Acceso a la historia clínica por los profesionales de la salud.

Llegados a este punto cabe preguntarse por el alcance que tiene esa habilitación legal del profesional sanitario para el conocimiento de los datos de salud del paciente. Dado que, hoy por hoy, el núcleo central de las informaciones sobre la salud de la persona física se condensa en el historial médico con el que se cuenta en los centros sanitarios a los que acudimos, públicos y/o privados, el tema implica la dilucidación de quién puede acceder a la historia clínica y a qué partes de ella. En suma, si padeciendo un problema dermatológico se encuentra legitimado tal especialista para consultar mi historial ginecológico, o si el médico de un centro hospitalario privado puede acceder a la historia clínica que el paciente tenga en un centro sanitario público.

En España la respuesta a estas cuestiones, desde una perspectiva global, parte de lo indicado en la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica (LBAP). Los usos de la historia clínica los regula su art. 16, indicando su número 1 que "Los profesionales asistenciales del centro que realizan el diagnóstico o el tratamiento del paciente tienen acceso a la historia clínica de éste como instrumento fundamental para su adecuada asistencia". En suma, sólo pueden acceder al historial médico los profesionales sanitarios que se encuentran involucrados directamente en el tratamiento del paciente en un momento concreto. Respecto de este personal no se plantea, a priori, restricciones a toda la información médica siempre que la finalidad sea "el diagnóstico o tratamiento" dentro de las necesidades de prestación del servicio -por ejemplo, dermatólogo que accede a la información sobre ginecología por sospecha de problema hormonal-. Por su parte, el personal de administración y gestión de los centros sanitarios, según señala el art. 16.4 de la LBAP, tiene limitado el acceso "a los datos de la historia clínica relacionados con sus propias funciones"[23].

23 Cf. Alkorta Idiakez, I., *El espacio europeo*, cit, 2022, pp. 31 y ss.

La Agencia Española de Protección de Datos, consultada sobre la habilitación del art. 16.1 de la LBAP para el acceso a la historia clínica por el personal de enfermería, en su informe 656/2008 de 7 de enero de 2009[24] indicó que:

"la regla debe ser aplicada con cautela en lo que respecta al personal sanitario que presta asistencia al paciente, dado que no puede, sin más, establecerse una aplicación restrictiva de las normas reguladoras del acceso a la historia clínica que pudiera perjudicar la salud del paciente, dada la finalidad que para la propia historia clínica establece la Ley 41/2002.

Por este motivo, en el supuesto que nos ocupa, la delimitación del acceso a los datos por parte del personal de enfermería, que tiene la condición de personal sanitario conforme a lo dispuesto en la Ley 44/2003, de 21 de noviembre, de Profesiones Sanitarias, también citada por la consultante, quedará limitada en cuanto su extensión a las finalidades descritas en el citado artículo 16.1 de la Ley 41/2002; es decir, dicho acceso siempre será posible y deberá llevarse a cabo con la finalidad de 'garantizar una asistencia adecuada al paciente' y en tanto los datos de la historia constituyan un 'instrumento fundamental para su adecuada asistencia' en cada caso concreto.

Desafortunadamente no es posible, a la vista de lo dispuesto en el citado artículo 16.1, establecer una regla meramente objetiva que pudiera resultar de aplicación en todos los supuestos, debiendo igualmente huirse de fórmulas que, sin más, delimiten el acceso en atención al concreto tratamiento llevado a cabo en relación con el paciente, dado que no es posible conocer a priori si existe o no relación entre los datos referidos a distintos episodios contenidos en la historia clínica.

De este modo, únicamente sería posible establecer una regla mínima de acceso, en cuya virtud el personal de enfermería que desarrolla su actividad en funciones de hospitalización debería acceder a la totalidad de los datos de la historia clínica que o bien se encuentren directamente vinculados al episodio que ha dado lugar a la hospitalización y que se obtengan durante la misma y a aquéllos otros datos de la historia clínica que hubieran sido considerados relevantes para el tratamiento llevado a cabo en relación con la hospitalización concreta respecto de la que se prestan los servicios asistenciales.

En relación con los restantes datos, habría de estarse a las circunstancias de cada caso concreto, no pudiendo establecerse una regla objetiva basada simplemente en el carácter reservado o no otorgado por el facultativo en relación con el propio episodio o con episodios anteriores, al no poder deducirse a priori

24 https://www.aepd.es/documento/2008-0656.pdf

si la misma resulta relevante o no para la adecuada asistencia sanitaria del paciente en el caso específico. En consecuencia, se considera que el personal de enfermería al que se refiere la consulta podrá acceder como mínimo a la información obtenida en relación con la hospitalización concreta y a aquélla anterior que se haya considerado relevante para la adecuada asistencia, debiendo en todo caso interpretarse el acceso en los términos que resulten más beneficiosos para lograr la mejor asistencia sanitaria del paciente".

En suma, el acceso a la historia clínica dependerá de lo que deban atender los distintos especialistas médicos, y funciones que desplieguen los distintos sectores de la asistencia sanitaria.

Tales aspectos se encuentran ligados al estricto protocolo y sistema de acceso restringido que el art. 16.7 de la LBAP ha exigido sea desarrollado por las Comunidades Autónomas[25]. Ello supone que, en cada acceso a la historia clínica, quedará identificada y registrada la persona que accede, la fecha y la finalidad; guardándose en el sistema para cada intento de acceso, como mínimo, la identificación del profesional, fecha y hora en la parte de la historia clínica a la que se ha accedido, además del tipo de acceso. Igualmente, en el sistema se registrarán los casos de denegación cuando no se satisficieran los criterios establecidos[26].

Hasta la fecha, la AEPD no ha reconocido que el paciente tenga un derecho específico a conocer la identidad del profesional o profesionales que han accedido a su historial médico[27], aunque sí el derecho de aquel a ese acceso, conforme se dispone en el art. 18 de la LBAP[28]. Este criterio fue ratificado por la Sentencia de la Audiencia Nacional de 4 de marzo de 2013, n.º 971/2013 (ECLI:ES:AN:2013:971), recordando su doctrina en relación con ese derecho:

"La sentencia de este Tribunal de 9 de febrero de 2006 ha destacado que el derecho del afectado consistente en la posibilidad de exigir al responsable del fichero una prestación de hacer consistente en la mera exhibición de sus datos y, en su caso, su rectificación o cancelación. Se trata de un derecho esencial en

25 "Las Comunidades Autónomas regularán el procedimiento para que quede constancia del acceso a la historia clínica y de su uso".

26 Etreros Huerta, J., Alonso Villar C., Marco Cuenca, G., Cabronero Fernández, M., Alfaro Latorre, M.: "El sistema de historia clínica digital del sistema nacional de salud: accesibilidad y protección de la información como elementos clave", *Derecho y Salud*, núm. 18, 2009, pp. 99 - 111.

27 Informe Jurídico 171/2008 y Resolución 948/201, en atención de que se están solicitando datos de terceros y no los datos propios, por lo que no se puede pedir tal información a través del derecho de acceso, salvo que una ley lo contemple.

28 1. El paciente tiene el derecho de acceso, con las reservas señaladas en el apartado 3 de este artículo, a la documentación de la historia clínica y a obtener copia de los datos que figuran en ella. Los centros sanitarios regularán el procedimiento que garantice la observancia de estos derechos…
3. El derecho al acceso del paciente a la documentación de la historia clínica no puede ejercitarse en perjuicio del derecho de terceras personas a la confidencialidad de los datos que constan en ella recogidos en interés terapéutico del paciente, ni en perjuicio del derecho de los profesionales participantes en su elaboración, los cuales pueden oponer al derecho de acceso la reserva de sus anotaciones subjetivas.

la materia, que se encuentra recogido en el art. 8.b y c) del Convenio 108 del Consejo de Europa y 12 y 13 de la Directiva 95/46 CE. Es indiscutibles que el derecho de acceso constituye núcleo esencial del derecho regulado en el art. 18.4 de la Constitución - STC 292/2000-".

Y fundamentó la denegación de la petición formulada por el paciente, atendiendo a la ya derogada LOPD de 1999, que reconocía habilitación legal para el tratamiento de datos por parte de las Administraciones dentro del ámbito de sus competencia -art. 6.2-, cuando está autorizada por ley -art.11.2-, y las previsiones del art. 7, respecto a la gestión de los servicios sanitarios por los profesionales sujetos al deber de secreto, por cuanto:

"Considera la Sala, que los datos no han sido cedidos a terceros, o tal cuestión se trataría en su caso de cuestión de cesión ajena a este recurso -en este sentido STS 27-4-2010, rec. 6371/2006 -. Consta por el INSS que ha comprobado la identidad del personal que ha accedido a sus datos, y que confirma que se trataba de personal con justificación y acreditación a nivel orgánico y de funciones, por lo que de esta forma se está garantizando el uso al que se someten los datos personales".

En el fondo de esta cuestión se encuentra la consideración de que ha de haber un equilibrio entre la tutela del derecho a la protección de datos y la gestión de la información sanitaria, que no termine imposibilitando la actividad de prestación asistencial y actuación médica.

No obstante, sobre los aspectos indicados, el REEDS ha incluido varias previsiones que pueden mutar los criterios seguidos hasta la fecha. En su regulación sobre el "Acceso a los datos electrónicos personales para uso primario y transmisión de esos datos", el art. 3 del REEDS, en sede de "Derechos de las personas físicas en relación con el uso primario de sus datos sanitarios electrónicos", ha previsto que:

"9. No obstante lo dispuesto en el artículo 6, apartado 1, letra d), del Reglamento (UE) 2016/679, las personas físicas tendrán derecho a restringir el acceso de los profesionales sanitarios a la totalidad o parte de sus datos sanitarios electrónicos. Los Estados miembros establecerán las normas y garantías específicas relativas a dichos mecanismos de restricción".

Habrá que ver cómo se dimensiona en la normativa española esta cuestión a fin de que pueda desarrollarse correctamente toda la prestación sanitaria. Precisamente la consciencia sobre las repercusiones negativas que ello pueda implicar motiva que el propio REEDS introduzca una atemperación a ella en la

regulación que efectúa en su art. 5 sobre "el acceso de los profesionales sanitarios a los datos sanitarios electrónicos personales", indicándose que:

"4. Cuando la persona física haya restringido el acceso a los datos sanitarios electrónicos, no se informará al prestador de asistencia sanitaria ni a los profesionales sanitarios del contenido de los datos sanitarios electrónicos sin la autorización previa de la persona física, incluso cuando el prestador o el profesional en cuestión esté informado de la existencia y la naturaleza de los datos sanitarios electrónicos restringidos. En los casos en que el tratamiento sea necesario para proteger los intereses vitales del interesado o de otra persona física, el prestador de asistencia sanitaria o el profesional sanitario podrán tener acceso a los datos sanitarios electrónicos restringidos. Tras dicho acceso, el prestador de asistencia sanitaria o el profesional sanitario informará al titular de los datos y a la persona física afectada o a sus tutores de que se ha concedido el acceso a los datos sanitarios electrónicos. La legislación de los Estados miembros podrá incluir otras garantías adicionales".

Además, aparece también previsto expresamente, entre los derechos del paciente, art. 5 del REEDS, que:

"10. Las personas físicas tendrán derecho a obtener información sobre los prestadores de asistencia sanitaria y los profesionales sanitarios que hayan accedido a sus datos sanitarios electrónicos en el contexto de la asistencia sanitaria. La información se facilitará de forma inmediata y gratuita a través de los servicios de acceso a los datos sanitarios electrónicos".

Fuera de la órbita descrita, un acceso a la historia clínica que no se ajuste a la finalidad de la atención o prestación del servicio sanitario, salvo que tenga por objeto fines de salud pública, prevención, lucha contra enfermedades contagiosas o la investigación científica -art. 9.2.h) y i) RGPD, art. 19.3 LBAP y disp. ad. 16 LOPDGDD-, implicará una "cesión" de datos sólo legítima si media consentimiento del afectado.

El profesional del centro sanitario que acceda a esa información incurrirá en el delito ya reseñado de revelación de secretos del art. 197 del CP. Dado que ésta es la máxima reacción del ordenamiento para el cumplimiento de un deber, hay que destacar que el mero acceso no siempre apareja ese efecto. En tal sentido la STS de 15 de julio de 2020, n.º 392/2020, Rec. 4025/2018 (ECLI: ES:TS:2020:2509) respecto a dos accesos por un médico, cuando era administrador, a la historia clínica electrónica de tercero con la única intención de conocer la existencia de partes de baja por incapacidad temporal laboral, sin conocimiento de otros datos médicos, obteniendo la información de la inexistencia de bajas, que se estimó que objetivamente no era información sensible en el ámbito de la

intimidad más estricta. En cambio, la STS de 23 de septiembre de 2015, Rec. 648/2015 (ECLI: ES:TS:2015:3874), condenó al médico que había accedido hasta en veinticinco ocasiones al historial médico de cinco compañeras. También se estimó tal vulneración, con condena al médico, en la SAP de las Palmas de 12 de marzo de 2021, n.º 76/2021, Rec. 54/2018 (ECLI: ES: APGC:2021:8), por el acceso al historial clínico de su esposa, que era su paciente, en el que introdujo los datos sobre el diagnóstico de personalidad narcisista y trastorno esquizoide de la personalidad, información que utilizó durante el proceso de divorcio en la entrevista que mantuvo con la Psicóloga Forense.

Cabe preguntarse sobre qué pasa en el caso de que un paciente sea derivado a otro centro de salud u hospital distinto al que se custodia la historia clínica y si se precisaría el consentimiento para la cesión de esa información. A este respecto, conforme se deriva del art. 14. 2, d) del RGPD, habrá que diferenciar si la cesión de información se realiza entre centros públicos, caso en el que bastará que se le informe al interesado, o bien se trasmita a un centro privado, supuesto para el que parece se requerirá consentimiento expreso del paciente. Este aspecto se suele satisfacer, en la práctica, dando al paciente los informes para que los entregue personalmente al profesional médico del centro privado que le atienda. Precisamente el REEDS persigue atajar los problemas que plantea el acceso e intercambio de la información clínica cuando los pacientes reciben atención sanitaria en un país distinto del que residen. A este respecto cabe recordar que, al amparo del art. 14 de la Directiva 2011/24 UE, relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza, se ha creado una red transfronteriza de sanidad electrónica eHealth Network, configurándose una infraestructura digital de intercambio de datos sanitarios -Ehealth Digital Service Infraestructure (eHDSI)- a través de la que se posibilita el intercambio de recetas electrónicas, historiales clínicos electrónicos e historias clínicas abreviadas de los pacientes europeos[29].

Las soluciones y experiencia indicadas coinciden sustancialmente con lo que es la práctica vivida en estos temas en Perú, por aplicación de su normativa -art.14.6 y 9, 19 y 29 de la LOPD y arts. 12, 14, 16 del Reglamento de la Ley N° 29414, norma que establece los Derechos de las Personas Usuarias de los Servicios de Salud-. Prueba de ello son, entre otros, el Informe Jurídico n.º 10-2020-JUS/DGTAIPD, sobre los "Alcances del literal h) del artículo 25 de la Ley Nro. 26842, General de Salud en el marco de la protección de datos personales", y la Opinión Consultiva n.º 07-2019-JUS/DGTAIPD, relativa a las "Limitaciones al consentimiento cuando

29 Para un mayor detalle Alkorta Idiakez, I., *El espacio europeo*, cit., 2022, pp. 36 y 37; Nicolás Jiménez, P., Armaza, E.J., y Perin, A., "Impact of the Directive 2011/24/UE on the application of patient`s rights in cross-border healthcare. A comparative analysis", *Revista de derecho y genoma humano: genética, biotecnología y medicina avanzada/Law and the human genomereview: genetics, biothechnology and advanced medice*, 44, 2016, pp. 53-64.

se dé tratamiento a datos relacionados a la salud, de conformidad al artículo 14, numeral 6, de la LOPD".

III. ACCESO A LOS DATOS DE SALUD CONTENIDOS EN EL HISTORIAL CLÍNICO POR PARTE DE TERCEROS ¿HASTA QUÉ PUNTO PUEDEN SABER DE MIS ENFERMEDADES O TRATAMIENTOS?

1. Acceso a la historia clínica con fines de investigación, judiciales y de salud pública.

Desde una perspectiva legal, existe legitimación para acceder a los datos recogidos en la historia clínica sin el consentimiento expreso del interesado, art. 9.2 del RGPD, cuando:

"f) el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial…

j) el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado".

Estas previsiones hay que cohonestarlas con las fijadas en el art. 16.3 de la LBAP que reconoce, la posibilidad de acceso a "la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia", conforme a la "legislación vigente en materia de protección de datos personales, y en la Ley 14/1986, de 25 de abril, General de Sanidad, y demás normas de aplicación en cada caso", fijándose como regla general la anonimización, y mantenimiento separado de los datos de identificación personal del paciente de los de carácter clinicoasistencial, "salvo que el propio paciente haya dado su consentimiento para no separarlos".

Esta regla de la anonimización tiene tres excepciones:

1.- Los supuestos de investigación previstos en el apartado 2 de la Disposición adicional decimoséptima de la LOPDPGDD: b) en situaciones de excepcional relevancia y gravedad para la salud pública cuando las autoridades sanitarias e instituciones públicas con competencias en vigilancia de la salud pública lleven a cabo estudios científicos; c) reutilización de los datos para investigación de salud y biomédica prestado el consentimiento para un fin concreto; y d) tratamiento de datos de salud seudonimizados con fines de investigación de salud y biomédica.

2.- Los supuestos de investigación de la autoridad judicial en los que se considere imprescindible la unificación de los datos identificativos con los clinicoasistenciales. En estos casos se precisará la pertinente petición de información por jueces y tribunales en el proceso de que se trate, sea laboral, contencioso-administrativo, penal o civil. El acceso a los datos y documentos de la historia clínica se limitarán estrictamente a los fines específicos en cada caso.

Cuando no existe un mandamiento judicial o requerimiento del Ministerio fiscal que dé cobertura a la cesión, se ha venido planteado si el requerimiento de la policía judicial puede ser suficiente para facultar el acceso a esa información. Inicialmente, la AEPD, en sus informes 297/2005 y 133/2008, se mostró favorable si se cumplían las exigencias siguientes: a) la acreditación de que los datos a obtener fueran necesarios para la prevención de un peligro real y grave de seguridad pública o represión de infracciones penales, así como los fines de la investigación; b) que la petición cursada fuera concreta y específica, no resultando compatible con ello una solicitud masiva de datos; c) que hubiera una motivación que justificara esos aspectos; d) que, en cumplimiento del artículo 22.4 de la LOPD de 1999, los datos se cancelaran "cuando no (fueran) necesarios para las averiguaciones que motivaron su almacenamiento". En tiempo posterior la AEPD parece haber reconsiderado su postura en su informe 60/2017, aunque los términos en los que se expresa no denotan una idea clara[30]. En cambio, la Agencia Catalana de Protección de datos -Dictámenes CNS 42/2014, CNS 47/2018 y CNS 15/2021- sí que se ha pronunciado en sentido positivo, considerando que la cesión de datos en tal caso estaría habilitada al abrigo del artículo 282 de la LECRIM y artículo 549.1.a) de la LOPJ. La STS de 16 de diciembre de 2022, n.º 971/2022, Rec. 10245/2022 (ECLI: ES:TS:2022:4754), ha cerrado la cuestión negando tal posibilidad, abundado en el tenor del art. 16 de la LBAP y las previsiones de 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 dictada en la trasposición de la Directiva (UE) 2016/680.

3.- La prevención de un riesgo o peligro grave para la salud de la población, caso en el que "las Administraciones sanitarias a las que se refiere la Ley 33/2011, de 4 de octubre, General de Salud Pública, podrán acceder a los datos identificativos de los pacientes por razones epidemiológicas o de protección de la salud pública.

30 El dictamen se indica que: "En definitiva, y sin perjuicio de que pueda existir un mandamiento judicial o solicitud del ministerio fiscal en el ejercicio de sus funciones que las fuerzas y cuerpos de seguridad estén ejecutando en su función de policía judicial, no se considera de conformidad con la legislación de protección de datos una solicitud por parte de dichas fuerzas de seguridad relativa a la información médica de la posible víctima que vaya más allá de lo estrictamente necesario y pertinente para determinar la situación del lesionado en relación con el delito público que la ley de enjuiciamiento criminal obliga a denunciar al profesional médico cuando una persona hubiere sido víctima de lesiones, y que se contiene en el Parte Judicial de Lesiones. En estos casos, y salvo que hubiera mandamiento judicial o solicitud del ministerio fiscal, se considera necesario el consentimiento del afectado para la entrega de la información médica a que hace referencia la consulta".

El acceso habrá de realizarse, en todo caso, por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta, asimismo, a una obligación equivalente de secreto, previa motivación por parte de la Administración que solicitase el acceso a los datos". El supuesto nos recuerda la situación generada por el Covid-19 y la gestión que hubo de realizarse para superar la pandemia.

2. Acceso a la historia clínica por los progenitores.

Desde la perspectiva material, se plantean otras cuestiones que se ligan al hecho de que pueden aparecer en la historia clínica otras informaciones que involucran a terceros; caso, por ejemplo, de los datos personales o de salud de los progenitores de paciente menor de edad o mayor con dependencia. En estos supuestos se suscita la cuestión de si esos terceros podrían acceder al contenido y datos del historial clínico del paciente.

A ese respecto conviene recordar que el art. 9.4 de la LBAP establece, en sede de prestación del consentimiento informado para los actos médicos de los que se nutre el historial médico, que "cuando se trate de menores emancipados o mayores de 16 años que no se encuentren en los supuestos b) y c) del apartado anterior -paciente con medidas de apoyo o que no sea capaz intelectual ni emocionalmente de comprender el alcance de la intervención-, no cabe prestar el consentimiento por representación". En España con 16 años se inicia la plenitud de la capacidad jurídica para la autodeterminación de las decisiones sobre salud.

En cuanto a la protección de datos, el art. 7 de la LOPDGD, que ha mantenido sustancialmente el criterio precedente, dentro del marco del art. 8 RGPD,[31] prevé que:

"1. El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años.

Se exceptúan los supuestos en que la ley exija la asistencia de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento.

2. El tratamiento de los datos de los menores de catorce años, fundado en el consentimiento, solo será lícito si consta el del titular de la patria potestad o tutela, con el alcance que determinen los titulares de la patria potestad o tutela".

31 1. Cuando se aplique el artículo 6, apartado 1, letra a), en relación con la oferta directa a niños de servicios de la sociedad de la información, el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó.
Los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años.

La cuestión del acceso a la historia clínica de los menores de edad ha sido objeto de atención por la AEPD en varias ocasiones. En su informe 0222/2014, en el que se hizo eco del anterior de 15 de abril de 2008, se puso de relieve tanto el carácter de este derecho personalísimo como las obligaciones que, conforme al artículo 154 del Código Civil español, competen a los progenitores en el ejercicio de la patria potestad. La solución que se ofrece aúna estos dos aspectos pues, aun cuando el mayor de 14 años puede acceder a su historia clínica, los padres también cuentan con esa facultad en virtud de su responsabilidad parental. A este respecto se indica en el informe que:

"Las obligaciones establecidas en el Código Civil, en tanto el menor no sea emancipado, permanecen durante toda la minoría de edad del afectado. De este modo, estando obligados los titulares de la patria potestad en los términos que se han descrito no sería oponible a este acceso la mera voluntad del menor sometido a patria potestad, con la única excepción de que una norma con rango de Ley hiciese expresamente primar la voluntad del menor sobre la de los titulares que pretenden el acceso.

Por último, en relación con el ejercicio del derecho por el propio menor, debe tenerse en cuenta que el artículo 9.3 c) de la Ley 41/2002 prevé que el menor tendrá conocimiento del acto médico respeto del que sus padres prestan el consentimiento para la realización. Siendo esto así y estableciéndose, como se indicó al comienzo de esta Agencia por el Reglamento una presunción legal de que el menor cuenta con condiciones suficientes de madurez para el ejercicio de sus derechos relacionados con la protección de datos a partir de los catorce años, sería posible diferenciar entre el derecho a prestar el consentimiento y los vinculados al acceso a la historia clínica.

Así, si bien será precisa la prestación del consentimiento por los padres o tutores, sí cabría considerar que el menor de edad podría ejercer el derecho de acceso a partir de los catorce años, si bien este ejercicio no puede entenderse como limitación al derecho de los titulares de la patria potestad del menor no emancipado a acceder a su historia clínica en los términos que acaban de indicarse en el presente informe.

En conclusión, y atendiendo a las cuestiones planteadas, debe señalarse brevemente lo siguiente:

El consentimiento para el tratamiento de los datos de los menores de edad en las historias clínicas queda supeditado a lo dispuesto en el artículo 9.3 c) de la Ley 41/2002.

El menor de edad mayor de catorce años podrá, en general, ejercitar por sí solo el derecho de acceso a la historia clínica.

- Los titulares de la patria potestad podrán también acceder a los datos del menor de edad sujeto a aquélla mientras esa situación persista, para el cumplimiento de las obligaciones previstas en el Código Civil.

- No podrá oponerse a ese acceso la mera oposición del menor salvo que así lo reconociera una norma con rango de Ley".

En el caso de que esos hijos sean mayores de edad, emancipados o superen los 14 años, parece que la única vía sería, conforme al art. 9.2 del RGPD, la representación voluntaria o la concedida expresamente por intervención judicial. En cuanto a ello, resulta especialmente interesante la SAN de 16 de septiembre de 2021, n.º 3678/2021 (ECLI:ES:AN:2021:3678), en la que se planteaba la denegación a un padre del acceso a la historia clínica de un hijo mayor de edad por el Servicio de Salud de Castilla-La Mancha (SESCAM), a pesar de haber aportado aquel un poder notarial general otorgado por su hijo a su progenitor. La Audiencia Nacional confirma el criterio de la SESCAM y deniega la pretensión sobre la base de la argumentación que:

"el poder notarial de 17 de enero de 2012 que D. Damaso (nacido en 1988), otorgó en favor de su padre D. Maximino y que éste aportó ante el SESCAM para que se le concediera el acceso a un informe médico de su hijo, de junio de 2019, no puede servir de cobertura para ello, por cuanto de su lectura y de una interpretación sistemática del mismo, se desprende que se trata de un poder general para practicar cualesquiera actos y negocios de "administración, adquisición, enajenación, gravamen y disposición, sin limitación alguna", como se indica en la página 6 del mismo, en sentido amplio.

Es decir, se trata de un poder general comúnmente conocido como de administración, pero no en él no se faculta por el poderdante de modo específico a su padre, para que en su representación pueda acceder a sus datos médicos.

Téngase en cuenta que los datos médicos o datos relativos a la salud, entran dentro de una categoría especial de datos personales, ex artículo 9 del Reglamento General de Protección de Datos, para cuyo tratamiento se requiere el "consentimiento explícito" del interesado, según el apartado 2.a) de dicho precepto, salvo que resulte de aplicación alguna de las excepciones que se recogen en los restantes apartados del citado artículo 9.2, que aquí no concurren.

Por tanto, si bien el artículo 12.1 de la LOPDGDD establece que los derechos reconocidos en los artículos 15 a 22 del RGPD podrán ejercitarse directamente o por medio de representante legal o voluntario, cuando se ejercite el derecho de acceso (al que se refiere el artículo 15 del RGPD) a datos de salud por representante, deberá contar éste con el consentimiento explícito del titular de

los datos para ello, consentimiento que no consta de forma específica en el poder notarial aportado, por lo que la denegación del informe solicitado resulta, en suma, ajustada a Derecho".

Este parecer se ajusta a los dictados de la Resolución de 27/02/2009, sobre uso, acceso, cesión de datos y conservación de la Historia Clínica en el ámbito del SESCAM, que determina, en la Comunidad Autónoma de Castilla-La Mancha, los requisitos y documentación que se deben aportar para el acceso a la historia clínica. Para el acceso por representación se requiere expresamente que se habrá de "aportar escrito original de la autorización con firma manuscrita del paciente o apoderamiento notarial". Exigiéndose que "la autorización será específica e inequívoca para el ejercicio de este derecho y para este caso en concreto, sin que resulte válidos los poderes "generales para pleitos". En todo caso se deberá detallar de forma específica en qué términos se autoriza la representación". Tales requisitos, si se piensa en el contexto de las personas con discapacidad, con el régimen que se implantó en España por la Ley 8/21 de 2 de junio, en cuanto a las medidas preventivas de apoyo -arts. 256 a 262 del CC-, a buen seguro plantearán problemas de futuro.

IV. INFORMACIÓN SOBRE LA SALUD. LA COMUNICACIÓN POR WHATSAPP DE CIRCUNSTANCIAS DE SALUD ¿UN PROBLEMA JURÍDICO?

1. Información sobre la salud de personas con relieve público.

La comunicación de la información sobre la salud, según sean las circunstancias en las que ésta se plantea y manera en la que se transmite, genera también otras cuestiones.

Un primer tema, apuntado al inicio, es hasta dónde alcanza el derecho a la protección de datos en situaciones en las que el derecho del individuo a su privacidad pugna con otros derechos fundamentales, o hay que articular para la comunicación de la información medidas excepcionales.

Como elementos de reflexión y discusión nos podemos plantear el caso de aquellas informaciones sobre la salud de personas públicas en las que el derecho a la libertad de prensa e información se enfrenta al de la protección de datos. Hay que tener en cuenta que, respecto a la UE, el art. 9.2.e) del RGPD excluye la necesidad de consentimiento si "el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos". Previsión que, por lo que respecta a España, se conjuga con la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

El Tribunal Supremo de España esta cuestión se presentó en su sentencia de 17 de septiembre de 2014, n.º 469/2014, Rec. 3371/2012 (ECLI: ES:TS:2014:3524), en relación con la información ofrecida por un periódico relativa a la indisposición de un presidente de Comunidad Autónoma durante un mitin en campaña electoral, que atribuyó a una afección de oído, estrés y tensión alta, patologías que no eran del todo exactas. El aspecto central del pronunciamiento, que fue desestimatorio de la vulneración de la intimidad y protección de datos, se centró en la tensión entre el derecho a la libertad de información y el derecho que aquí nos ocupa. A este respecto se recuerda en la sentencia que:

"1ª) Como declara el Tribunal Constitucional, 'el padecimiento de una enfermedad se enmarca en la esfera de la privacidad, tratándose de un dato íntimo que puede ser preservado del conocimiento ajeno. El derecho a la intimidad comprende la información relativa a la salud física y psíquica de las personas' (STC 159/2009, con cita de la STC 70/2009).

2ª) Sin embargo, también ha declarado el Tribunal Constitucional que 'aunque el art. 18.1 CE no prevé expresamente la posibilidad de un sacrificio legítimo del derecho a la intimidad -a diferencia de lo que ocurre en otros supuestos, como respecto de los derechos reconocidos en los arts. 18.2 y 3 CE-, su ámbito de protección puede ceder en aquellos casos en los que se constata la existencia de un interés constitucionalmente prevalente al interés de la persona en mantener la privacidad de determinada información' (STC 159/2009).

3ª) En el caso examinado, el derecho a la intimidad del demandante D. Celestin, comprensivo de la información relativa a su salud física y psíquica, se encontraba limitado por el derecho a informar a la opinión pública de un episodio muy concreto que afectó a su salud pero que guardaba una relación directa con su actividad política, es decir limitado por el derecho de los demandados a comunicar libremente información veraz (art. 20.1.d. de la Constitución), pues la información se publicó en un periódico del Principado de Asturias, el Sr. Celestino era presidente de esta comunidad autónoma, se encontraba en un acto de campaña electoral cuando sufrió un episodio que afectaba a su salud y, en fin, es una evidencia tanto el interés de la sociedad por conocer el estado de salud de sus dirigentes como la constante información que se ha facilitado a los medios cuando los más altos dignatarios, tanto españoles como extranjeros, han visto afectada su salud o se han sometido a intervenciones quirúrgicas.

Concurrían, por tanto, los dos elementos -carácter público de la persona afectada (elemento subjetivo) y relevancia pública de los hechos objeto de información (elemento objetivo)- que la STC 176/2013 considera precisos para proteger las informaciones que afecten a la intimidad personal".

Frente al alegato de que la información ofrecida no era del todo exacta, por lo que resultaría cuestionable que pudiera ceder el derecho a la protección de datos -art. 18.2 CE- frente a la libertad de información -art. 20.1.d CE-, se indicó lo siguiente:

"5ª) Según la doctrina del Tribunal Constitucional, 'tratándose de la intimidad, la veracidad no es paliativo, sino presupuesto, en todo caso de la lesión' (STC 20/1992), aunque también se puntualiza que 'en modo alguno puede exigirse a nadie que soporte pasivamente la difusión periodística de datos, reales o supuestos, de su vida privada que afecten a su reputación' (asimismo STC 20/1992), de lo que se sigue que no siempre la veracidad es presupuesto de la lesión porque entonces esta no podría producirse por la difusión de datos supuestos. De ahí que esta Sala haya declarado, sobre este punto, que 'la intromisión en la intimidad puede resultar agravada precisamente por la falta de veracidad de la información si esta falta de veracidad contribuye a presentar ... una situación de los demandantes aún más reservada o sustraída a los ojos de los demás que la situación real' (STS 12-9-2011 en rec. 941/07).

6ª) En el presente caso la falta de exactitud de la información no puede determinar por sí sola, una vez sentada la licitud de informar sobre el episodio de salud del demandante D. Celestino, la existencia de intromisión ilegítima en su derecho a la intimidad personal, porque la atribución del mareo a la tensión alta y al estrés, además de a la afección de oído, no ahondaba significativamente en ese ámbito de la vida privada constituido por la salud física y psíquica: primero, porque la hipertensión y el estrés no tienen hoy el carácter peyorativo que reiteradamente se afirma en el recurso, al ser notorio que ambas afectan a miles de personas y que el estrés aparece frecuentemente asociado a determinadas profesiones sin que por ello incapacite a las personas que la ejercen y padezcan de estrés; y segundo, porque la hipertensión y el estrés, sobre todo este último, son entendidas por la opinión pública como algo perfectamente explicable ante el ritmo que la actividad política, especialmente en campaña electoral, impone hoy a los dirigentes".

El otro aspecto relevante de la resolución tiene que ver con la imposibilidad de que este tipo de información pudiera hallarse incursa en el régimen de la protección de datos, lo cual no deja de resultar curioso e interesante toda vez que la información personal sobre el estado de salud es un dato personal de salud, aunque no se extraiga de una historia clínica (art. 4.15 RGPD), afirmándose que:

"confunde la finalidad de la LO 15/1999, de 13 de diciembre, de protección de datos de carácter personal, que es 'garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar' (art. 1), con su ámbito de aplicación, que son 'los datos de

carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento' y 'toda modalidad de uso posterior de estos datos por los sectores público y privado' (art. 2), y en el presente caso los demandados no han hecho uso de datos del demandante que estuvieran registrados en un soporte físico, ni siquiera en los términos del art. 3.b LOPD, que define el fichero como un 'conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso', sino que, en la divulgación de la noticia del episodio padecido por el demandante en una campaña electoral han aludido a dos datos afectantes a su salud que resultaron ser inexactos, sin que hubiesen tratado, cedido o manipulado fichero alguno y, por tanto, hubiese incurrido en alguna de las infracciones previstas en el art. 44 LOPD, con lo que, al no haberse infringido dicha ley orgánica por los demandados, no es aplicable su art. 19, que reconoce el derecho a ser indemnizados únicamente a quienes sufran lesión en sus bienes o derechos 'como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el responsable o el encargado del tratamiento'".

2. Forma de comunicación de los datos de salud.

Por lo que se refiere a la manera en la que se comunica la información de salud, los centros y profesionales de la salud están profundamente sensibilizados y han implementado medidas efectivas para evitar la cesión inconsentida de datos -llamada por número en las consultas, envío cifrado de documentación con código proporcionado sólo al interesado, etc.-[32]. La cultura y sensibilidad en este tema no siempre se comparte por el ciudadano que, incluso, puede ver como un engorro algunas de las medidas implantadas en aras del respeto a la protección de datos –por ejemplo, la denegación de información sobre el número de habitación del ingresado en hospital-.

Tratándose de instituciones o empresas cuya actividad central no se encuentra ligada a la actividad curativa y de la salud nos encontramos con la cuestión de que, como responsables de todo el conjunto de datos que se tratan, se tienen que haber previsto "medidas técnicas y organizativas apropiadas" para la protección de datos "desde el diseño y por defecto", art. 25 del RGPD, atendiendo "al estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas".

Un ejemplo en el que falló ese aspecto es el enjuiciado por la SAN de 2 de octubre de 2018, Rec. 900/2016 (ECLI: ES:AN:2018:3661). En el caso objeto de resolución se había remitido a una Guardia Civil por el correo corporativo interno

32 A este respecto resulta interesante la Guía para profesionales del sector sanitario de la AEPD que se comparte en el portal de la Autoridad Nacional de Protección de Datos de Perú, o la elaborada por este organismo para el tratamiento de los datos de salud del Covid.

la resolución de su petición de comisión de servicios, solicitada para atender a sus abuelos enfermos. La contestación se acompañó de toda la documentación que había aportado, incluidos los informes médicos de aquellos. La queja que presentó a sus superiores por tal hecho, ya que no sabía si podía haber accedido a esa información quien no era su superior, no fue atendida, y la petición que cursó a la AEPD para que sancionara a la Institución por tal circunstancia fue desestimada. Sin embargo, la Audiencia Nacional sí consideró que los hechos debían, al menos, ser investigados, indicando que:

"en contra del contenido de la respuesta que se le ofrece por las autoridades de la Guardia Civil ante la queja presentada, los datos que se incorporaron al correo corporativo, sí que contienen datos personales relacionados con la salud mental y física de los abuelos de la recurrente, pues según consta en el expediente se trata de dos hojas para cada uno de los abuelos de la recurrente, en cuya primera página, ciertamente solo aparece una resolución que les reconoce un determinado grado de discapacidad, pero en la segunda página, se recogen datos relativos a la salud mental y física, con diagnósticos médicos y etiología de la enfermedad, que deben reputarse como datos sensibles y sujetos a especial protección.

En otro orden de cosas, si bien es cierto que al tratarse de un correo corporativo, no tienen acceso otras personas que no pertenezcan al Cuerpo de la Guardia Civil, ello no exime a los responsables a adoptar las medidas necesarias para la debida protección de dichos datos ni mucho menos obliga a la denunciante a acreditar cuantas personas accedieron a dicho correo, como argumenta la resolución combatida".

En respuesta a la cuestión que se ha planteado en el título, si resulta buena idea comunicar información por whatsapp, sobre todo tratándose de datos de salud, parece que aquella se inclina hacia una vertiente negativa, aunque se trate de un chat privado y tengamos el consentimiento del afectado, pues en estos casos se produce una pérdida de control sobre la información.

Cabe destacar que la AEPD ha sancionado en diversas ocasiones el envío por whatsapp de diversa información, caso de la Comunidad de Vecinos que remitió imágenes captadas por las cámaras de videovigilancia de la comunidad (Expediente N.º: EXP202204461) -2.000 euros-, abogada que envió una sentencia por ese medio con los datos personales para poder promocionarse profesionalmente sin consentimiento del interesado (Expediente n.º EXP202202963) -4.000 euros-, o la difusión de imágenes captadas en la vía pública de un policía municipal que intervino en una agresión -2000 €-. A este respecto, la Sala de lo Penal del Tribunal Supremo, sentencia de 27 de septiembre de 2023, n.º 693/2023, Rec. 6019/2021, ha declarado que la publicación de fotos íntimas de una mujer sin su consentimiento

en el estado de whatsapp de un sujeto constituye un delito de descubrimiento y revelación de secretos del art. 197.7 del CP.

V. RESPONSABILIDAD CIVIL POR VULNERACIÓN DE LA NORMATIVA DE PROTECCIÓN DE DATOS.

1. Vías y requisitos para su exigibilidad.

Hasta aquí se han visto los aspectos generales de la protección de los datos de salud, cabe preguntarse por la responsabilidad que puede anudar la vulneración del derecho fundamente a la protección de datos desde perspectiva de la reparación del daño irrogado a la persona titular de ésos. A este respecto hay que tener en cuenta algunas cuestiones derivadas del régimen legalmente establecido para su reclamación.

En el marco europeo, el art. 82 del RGPD ha previsto expresamente en su n.º 1, que "(t)oda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del presente Reglamento tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos". Para ello, en su n.º 6, indica que "las acciones judiciales en ejercicio del derecho a indemnización se presentarán ante los tribunales competentes con arreglo al Derecho del Estado miembro que se indica en el artículo 79, apartado 2".

Ello supone de partida, en el caso de España, la remisión a las reglas del régimen de la responsabilidad civil, si el responsable o encargado del tratamiento se encuentra en la órbita particular y la infracción se produjo inter-privatos en un contexto de relación contractual o extracontractual; o a la disciplina de la responsabilidad patrimonial de la administración, cuando el tratamiento se efectúe por persona o ente público, produciéndose aquella vulneración por un funcionamiento normal o anormal de los servicios públicos. Por ende, además, conlleva la necesidad de que tengan que concurrir, y se deban acreditar, todos los requisitos que se exigen para que surja y se reconozca uno u otro tipo de responsabilidad.

La necesaria interacción de la acción indemnizatoria del art. 82 del RGPD[33] con los presupuestos requeridos en España para la responsabilidad civil -arts. 1902 y ss. del CC- o la responsabilidad patrimonial de la administración -32 y ss. de Ley

33 Rubí Puig, A.: "Daños por infracciones del derecho a la protección de datos personales. El remedio indemnizatorio del artículo 82 RGPD", *Revista de Derecho Civil*, 5 (4), 2018, pp. 58 y ss.; "Problemas de coordinación y compatibilidad entre la acción indemnizatoria del artículo 82 del reglamento general de protección de datos y otras acciones en Derecho Español", *Derecho Privado y Constitución*, 34, 2018, pp. 197-232. Brito Izquierdo, N.: "Recursos, responsabilidad y sanciones (arts. 77-84)" en López Calvo, J. (coord). *El nuevo marco regulatorio derivado del Reglamento Europeo de protección de datos*, Bosch, 2018, pp. 649 a 652.;

40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público- supone que, para que tenga éxito la pretensión, deban concitarse los siguientes presupuestos:

1º.- El actor, que tiene que ser una persona física y haber sufrido la vulneración de su derecho a la protección de datos (art. 1.1 y 2 RGPD), tendrá que acreditar que el demandado es el responsable o encargado de los datos. Este aspecto probatorio será de mayor o menor facilidad según fuera la relación previa -contractual o no-, el carácter de la intervención del demandado y su interacción con otros responsables. La delimitación del infractor, único o no, determinará también quién y cómo se responde conforme a las reglas del art. 82. 2, 3, 4 y 5 RGPD[34] que, en caso de falta de individualización de la responsabilidad, se decanta por su consideración solidaria.

Se ha planteado la legitimación activa para instar la acción "ex" art. 82 del RGPD quien no haya sido objeto del tratamiento y resulte dañado indirectamente; caso, por ejemplo, de revelación indebida de datos médicos sobre enfermedades hereditarias que permiten inferir ciertas características genéticas de los progenitores. No existiendo un tratamiento directo de los datos de éstos, por parte del responsable o encargado del tratamiento, parece que la vía a seguir no será la del RGPD sino la general de la responsabilidad civil extracontractual[35].

2º.- Ha de acreditarse que el responsable del tratamiento de los datos personales ha infringido la normativa de protección de datos prevista en el RGPD; esto es, que la vulneración proviene de acto imputable por incumplimiento de las obligaciones definidas legalmente, hallándose ello ligado al daño producido. Como ha puesto de relieve Rubí Puig, dado que las obligaciones fijadas en el RGPD son de varios tipos, pues unas se formulan como un estándar general abierto, mientras que otras son de medios o de resultados, el criterio de imputación que inicialmente se plantea como responsabilidad objetiva para compensar los daños causados tiene, sin embargo, elementos que son propios de la imputación subjetiva. La estimación

Trujillo Machuca, V., "La reclamación de daños y perjuicios en materia de protección de datos, *Actualidad Civil*, 12, 2020.

34 2. Cualquier responsable que participe en la operación de tratamiento responderá de los daños y perjuicios causados en caso de que dicha operación no cumpla lo dispuesto por el presente Reglamento. Un encargado únicamente responderá de los daños y perjuicios causados por el tratamiento cuando no haya cumplido con las obligaciones del presente Reglamento dirigidas específicamente a los encargados o haya actuado al margen o en contra de las instrucciones legales del responsable.
3. El responsable o encargado del tratamiento estará exento de responsabilidad en virtud del apartado 2 si demuestra que no es en modo alguno responsable del hecho que haya causado los daños y perjuicios.
4. Cuando más de un responsable o encargado del tratamiento, o un responsable y un encargado hayan participado en la misma operación de tratamiento y sean, con arreglo a los apartados 2 y 3, responsables de cualquier daño o perjuicio causado por dicho tratamiento, cada responsable o encargado será considerado responsable de todos los daños y perjuicios, a fin de garantizar la indemnización efectiva del interesado.
5. Cuando, de conformidad con el apartado 4, un responsable o encargado del tratamiento haya pagado una indemnización total por el perjuicio ocasionado, dicho responsable o encargado tendrá derecho a reclamar a los demás responsables o encargados que hayan participado en esa misma operación de tratamiento la parte de la indemnización

35 Rubí Puig, A.: "Daños por infracciones", cit., 2018, p. 61.

de la previsibilidad y gravedad de los riesgos implicados en el tratamiento de los datos personales faculta esa identificación de la vulneración normativa, a la que va ligada el principio general de responsabilidad activa (accountability) que compete al responsable. Este tiene que, desde el diseño y por defecto, hacer una previsión de lo que constituyen daños esperados, para adoptar las medidas y soluciones técnicas que los eviten.

3º.- El reclamante tendrá que probar la existencia, el alcance y la cuantificación del daño de carácter patrimonial o no patrimonial. La acreditación de estos aspectos es una de las cuestiones centrales que plantean mayor dificultad en el ámbito de la salud, pues el daño producido, casi por definición, se desenvuelven en marco del "daño moral". Ello explica el recurso que habitualmente se ha venido efectuando en la praxis del Derecho civil español a la Ley Orgánica 1/1982, por cuanto su art. 9.3 presume la existencia del perjuicio, acreditada la intromisión ilegítima. Reconociendo, además, que "la indemnización se extenderá al daño moral, que se valorará atendiendo a las circunstancias del caso y a la gravedad de la lesión efectivamente producida, para lo que se tendrá en cuenta, en su caso, la difusión o audiencia del medio a través del que se haya producido".

4º.- Por último, debe mediar una relación de causalidad entre la infracción denunciada y el daño sufrido. El ámbito de la protección que dispensa la norma permite la acreditación de este requisito. Hay que tener en cuenta que cabe la producción de daños no derivados de la vulneración de la protección de datos e infracciones de esta normativa que no tengan conexión con los daños efectivamente producidos.

El planteamiento descrito, en cuanto a los elementos que deben concurrir para la reclamación de la responsabilidad por infracción de la normativa de protección de datos, me parece que puede acomodarse sin dificultad al Derecho peruano. Pues, a tenor de lo establecido en el art. 25 de la LOPD, atinente al "derecho a ser indemnizado, se reconoce que "el titular de datos personales que sea afectado a consecuencia del incumplimiento de la presente Ley por el titular o por el encargado de tratamiento de datos personales o por terceros, tiene derecho a obtener la indemnización correspondiente, conforme a ley". Previsiones que trasladan este tema a la rica problemática de las exigencias que suscita el régimen de responsabilidad civil, singularmente extracontractual, de los arts. 1969 y ss. del Código civil peruano, cuyas cuatro décadas se celebran.

Interesa destacar que, de los elementos que deben concurrir para el ejercicio de la acción civil por infracción de la normativa de protección de datos, expuestos sucintamente, los que ofrecen una mayor complejidad y controversia práctica son la determinación de cuándo la vulneración de las obligaciones del RGPD anudan responsabilidad, cómo se valora la existencia de un daño indemnizable y cuál

sea su cuantificación. Respecto de ellos contamos con varios pronunciados del Tribunal de Justicia de la Unión Europea que están acotando la interpretación que debe darse al art. 82 del RGPD[36].

Por lo que se refiere a esa primera la cuestión, la STJUE de 14 de diciembre de 2023, asunto C-340/21, VB y Natsionalna agentsia za prihodite (ECLI:EU:C:2023:986) ha reseñado algunas cosas interesantes. Así, ha entendido que un acceso no autorizado de datos personales por terceros, caso de una brecha de seguridad por ciberataque, no implica por sí que las medidas técnicas y organizativas adoptadas por el responsable del tratamiento no fueran apropiadas con arreglo a los arts. 24 y 32 del RGPD. Además, ha indicado que ese carácter apropiado de las medidas técnicas y organizativas adoptadas por el responsable del tratamiento ha de ser apreciado por los órganos jurisdiccionales nacionales en cada caso concreto, teniendo en cuenta los riesgos vinculados al tratamiento y apreciando si la naturaleza, el contenido y la adopción de esas medidas están adaptados a estos riesgos. También ha afirmado que corre a cargo del responsable del tratamiento la prueba sobre este extremo, no siendo un informe pericial ordenado por el juez sistemáticamente medio de prueba necesario y suficiente. Con todo, quizá por el carácter objetivo de esta responsabilidad, en esta STJUE de 14 de diciembre de 2023, se ha dicho que, aun dándose estas circunstancias, el responsable del tratamiento no puede quedar exonerado de la obligación de indemnizar los daños y perjuicios sufridos por una persona, con arreglo al artículo 82, apartados 1 y 2, de dicho Reglamento, por el mero hecho de que esos daños y perjuicios resulten de una comunicación no autorizada de datos personales o de un acceso no autorizado a esos datos por parte de "terceros", a los efectos del artículo 4, punto 10, del mencionado Reglamento, pues ese responsable debe demostrar que no es en modo alguno responsable del hecho que haya causado los daños y perjuicios en cuestión.

En cuanto a la estimación de la existencia de un daño, resulta de todo punto interesante la doctrina asentada por la STJUE de 4 de mayo de 2023, asunto C-300/21, UI y Österreichische Post AG (EU:C:2023:3709), en la que se reconoce que "no puede considerarse que toda infracción de las disposiciones del RGPD dé lugar, por sí sola, a ese derecho a una indemnización a favor del interesado". Como consecuencia de ello, según se ha detallado por la STJUE de 11 de abril de 2024, C-741/21 (EU:C:2024:288), "la persona que reclama una indemnización por daños y perjuicios inmateriales en virtud de esa disposición debe acreditar no solo la infracción de las normas de dicho Reglamento, sino también que esa infracción le ha causado tales daños y perjuicios relacionados con el tratamiento de datos. Aunque para ello no se precisa que los daños y perjuicios sufridos por

36 Martín Faba, J. M.: "Novedades en materia de indemnización y protección de datos personales", *Revista Cesco de Derecho de Consumo*, 49, 2004, pp. 132 y ss. https://doi.org/10.18239/RCDC_2024.49.3474

el interesado hayan alcanzado cierto grado de gravedad [sentencias de 4 de mayo de 2023, Österreichische Post (Daños y perjuicios inmateriales relacionados con el tratamiento de datos personales), C-300/21, EU:C:2023:370), apartado 51, y de 11 de abril de 2024, juris, C-741/21, EU:C:2024:288), apartado 36]".

Qué sean esos "daños y perjuicios inmateriales", cuya definición no aparece explicitada en el artículo 82, apartado 1, del RGPD, es una cuestión a la que se ha dado respuesta en la citada STJUE de 4 de mayo de 2023, justificando la necesidad de fijar un concepto autónomo y uniforme de ese concepto en el Derecho de la Unión.

En cuanto aquel, se afirma que debe adoptarse una acepción amplia que garantice un nivel elevado de protección de las personas físicas en lo que respecta al tratamiento de sus datos personales. Por ello, se reconoce que "el temor que experimenta un interesado a un potencial uso indebido de sus datos personales por terceros a raíz de una infracción del citado Reglamento puede constituir, por sí solo, un 'daño y perjuicio inmaterial' a los efectos del artículo 82, apartado 1 [sentencia de 14 de diciembre de 2023, Natsionalna agentsia za prihodite, C-340/21, EU:C:2023:986, apartados 79 a 86, y de 25 de enero de 2024, MediaMarktSaturn, C-687/21, EU:C:2024:72, apartado 65]". Pero, además, se afirma que "la pérdida de control sobre los datos personales, incluso durante un breve período de tiempo, puede causar al interesado 'daños y perjuicios inmateriales', en el sentido del artículo 82, apartado 1, del RGPD, que den lugar a un derecho a indemnización, siempre que dicho interesado demuestre que ha sufrido efectivamente tales daños y perjuicios, por mínimos que sean", si bien "la mera alegación de un temor, sin que resulte probada una consecuencia negativa, no puede dar lugar a reparación con arreglo a esa disposición".

A tenor de todo ello se concluye que "el artículo 82, apartado 1, del RGPD debe interpretarse en el sentido de que, para fundamentar un derecho a indemnización, basta el temor padecido por una persona a que, como consecuencia de una infracción de este Reglamento, sus datos personales hayan sido divulgados a terceros, sin que pueda demostrarse que tal ha sido efectivamente el caso, siempre que ese temor, junto con sus consecuencias negativas, resulte debidamente probado".

En cuanto a la determinación del importe derivado de la responsabilidad, la STJUE de 11 de abril de 2024, C-741/21 (EU:C:2024:288) aclara varias cuestiones:

En primer lugar, dado que el RGPD no contiene ninguna disposición que tenga por objeto establecer las normas relativas a la determinación del importe de la indemnización por daños y perjuicios a la que tiene derecho el interesado, dice que "corresponde al ordenamiento jurídico interno de cada Estado miembro establecer los tipos de acciones que permitan garantizar los derechos que confiere

el citado artículo 82 a los justiciables y, en particular, los criterios que permitan determinar la cuantía de la indemnización debida en este contexto, siempre que se respeten los principios de equivalencia y de efectividad [sentencias de 4 de mayo de 2023, C-300/21, EU:C:2023:370, apartado 54, y de 11 de abril de 2024, juris, C-741/21, EU:C:2024:288, apartado 58]".

En segundo lugar, que "el derecho a indemnización previsto en el artículo 82, apartado 1, del RGPD no cumple una función disuasoria o incluso punitiva. De ello resulta que la gravedad de la infracción de este Reglamento que haya causado los daños y perjuicios materiales o inmateriales en cuestión no puede influir en el importe de la indemnización concedida en virtud de dicha disposición y que ese importe no puede fijarse en una cuantía que exceda de la compensación completa de ese perjuicio [sentencias de 21 de diciembre de 2023, Krankenversicherung Nordrhein, C-667/21, EU:C:2023:1022, apartado 86, y de 11 de abril de 2024, juris, C-741/21, EU:C:2024:288, apartado 60]".

En tercer lugar, que la "indemnización pecuniaria debe considerarse 'total y efectiva' si permite compensar íntegramente los daños y perjuicios sufridos concretamente como consecuencia de la infracción de dicho Reglamento, sin que sea necesario, a efectos de tal compensación íntegra, imponer el pago de indemnizaciones de carácter punitivo [sentencias de 4 de mayo de 2023, Österreichische, C-300/21, EU:C:2023:370, apartados 57 y 58, y de 11 de abril de 2024, juris, C-741/21, EU:C:2024:288, apartado 61]".

Finalmente, que "habida cuenta de la diferente redacción y finalidad del artículo 82 del RGPD, interpretado a la luz del considerando 146 de este, y del artículo 83 del mismo Reglamento, interpretado a la luz de su considerando 148, no puede entenderse que los criterios de evaluación establecidos específicamente en dicho artículo 83 sean aplicables mutatis mutandis en el marco del citado artículo 82", ni "los criterios para la fijación del importe de las multas administrativas previstos en el artículo 83 de este Reglamento ni, por otra parte, atribuir a ese derecho a indemnización una función disuasoria (sentencia de 11 de abril de 2024, C-741/21, EU:C:2024:288, apartado 62)".

2. Casuística indemnizatoria.

Adentrándonos en la situación concreta en España, en cuanto a la reclamación indemnizatoria por la infracción de la normativa de protección de datos de salud, hasta la fecha, según se ha apuntado, ésta ha estado ligada a la invocación de la Ley Orgánica 1/1982 y operatividad de su art. 9.3, que presume la existencia de perjuicio y daño moral acreditada la intromisión ilegítima.

A ese respecto cabe citar, entre las más recientes, la STS de 25 de abril de 2023, n.º 617/2023, Rec. 4158/2022 (ECLI: ES:TS:2023:1674). En este caso la indemnización concedida ascendió a 3.000 euros y la vulneración se ligó al atentado contra la intimidad producido por el comunicado emitido por el sindicato demandado en el que se desvelaba la enfermedad del demandante (Covid-19) entre los miembros de los colectivos profesionales de Guardia Urbana y de Bomberos del Ayuntamiento de Barcelona. Se valoró tal intromisión y su carente justificación, toda vez que el demandante había adoptado las prevenciones médicas pertinentes para aislarse y participar en las reuniones por medios telemáticos. No se acogió como justificación, para la divulgación de la situación de enfermedad, la preocupación social por la pandemia provocada por el Covid-19, ni la necesidad de conocer quién portaba el virus para tomar las precauciones necesarias. Tampoco se aceptó que concurrieran circunstancias que permitieran entender que prevalecía la libertad de expresión cuando se relaciona con la libertad sindical.

Más ligada a la infracción del derecho a la protección de datos en el ámbito de la salud se encuentran las reclamaciones instadas contra la Administración Sanitaria Pública. La valoración de responsabilidad patrimonial por funcionamiento anormal de los servicios públicos e indemnización del daño moral se ha reconocido por la STSJ de Extremadura, de 25 de noviembre de 2002, n.º 1932/2002, Rec. 1621/1999, cuando ha quedado acreditado el acceso indebido a la historia clínica de un niño recién nacido con discapacidad sin la autorización de los padres, otorgándose una indemnización 6.010,12 euros; o por la STSJ del Principado de Asturias, de 30 de septiembre de 2008, n.º 1165/2008, Rec. 888/2005, ante la publicación de la enfermedad padecida por un menor y los datos de los progenitores en un artículo de la Revista Anales Españoles de Pediatría para el que no se prestó el consentimiento, cuantificándose el daño moral en 9.000 euros.

No se ha considerado que concurriera tal vulneración por la STSJ de Cataluña de 3 de marzo de 2014, n.º 166/2014, Rec. 99/2012, respecto a la publicación en el Diario Oficial de la Generalidad de Cataluña de la Resolución administrativa de otorgamiento de la medalla de oro con distintivo rojo, concedida a un agente de policía con motivo de la incapacidad permanente total derivada de accidente de trabajo, al valorar que no existía un daño antijurídico que debiera ser resarcido. Se daba la circunstancia de que era un hecho público que el reclamante era un miembro de la "Associació per a la Integració Laboral-Mossos d'Esquadra amb discapacitat (AIL-MED)", asociación que difunde su actividad, entre otras, a través de una página web, ostentando el galardonado un cargo directivo en ella.

3. Información sobre la propia salud a familiares: ¿cabe la responsabilidad civil?

En el caso de la información de salud que se transmite por los profesionales a los familiares más cercanos del paciente, si éste se halla en una situación de

incapacidad física, el sistema individualista de protección absoluto del derecho a la protección de datos cede ante la necesidad de atención. De hecho, en España, el art. 9. 3.a) de la LBAP, en el caso de que el paciente mayor de edad no sea capaz de tomar decisiones cuando su estado físico o psíquico no le permite hacerse cargo de su situación, faculta que el consentimiento lo presten "las personas vinculadas a él por razones familiares o de hecho". Siendo ello así, difícilmente podrá considerarse que exista una vulneración de la protección de datos por parte del Centro médico que avise sobre tal situación cuando requieran adoptar decisiones médicas.

Esta misma idea cabe extraer del ordenamiento peruano. Aquí el Reglamento de la Ley nº 29414, norma que establece los derechos de las personas usuarias de los servicios de salud, por remisión de las previsiones del art. 18, in fine, que establece que "en caso de menores de edad o de personas cuyas condiciones particulares le impidan ejercer este derecho, el consentimiento a que se refiere el párrafo precedente, será expresado de acuerdo a lo establecido en el artículo 4° del presente Reglamento", traslada ese deber y representación, art. 4.b, "cuando la persona usuaria sea mayor de edad, capaz pero no pueda expresar su voluntad" a quien ejerza esa "conforme a lo estipulado por el Código Civil respecto al grado de consanguinidad o afinidad". De esta forma, cónyuge o concubino, padres, hijos mayores de edad o hermanos serán los que reciban la información sobre la salud del paciente y adopten las decisiones que estimen oportunas.

Hasta aquí, en apretada síntesis, el dibujo de algunas de las principales cuestiones a las que tiene que hacer frente el tratamiento de los datos personales de salud.

La ponderación de lo racional y humanamente justo en Derecho, base de toda prudente decisión, implica sentido común y trascender al individuo. En estos pilares se asienta la defensa de todo derecho fundamental. El interés personal no puede llevar a que quede orillado el bien común; máxime en un ámbito como es el de la salud, en el que todos estamos implicados y del que depende el sino de la humanidad.

BIBLIOGRAFÍA

Alkorta Idiakez, I.: *El espacio europeo de datos sanitarios: nuevos enfoques de la protección e intercambio de datos sanitarios*, Thomson-Reuters Aranzadi, 2022.

Brito Izquierdo, N.: "Recursos, responsabilidad y sanciones (arts. 77-84)" en López Calvo, J. (coord). *El nuevo marco regulatorio derivado del Reglamento Europeo de protección de datos*, Bosch, 2018.

De Miguel Sánchez, N.: *Tratamiento de datos personales en el ámbito sanitario: intimidad "versus" interés público"*, Tirant lo Blanch, Valencia, 2003.

Di Pizzo Chiacchio A.: *La expansión del derecho al olvido digital*, Atelier, 2018.

Egusquiza Balmaseda, M.A.: "Olvido oncológico protección de datos de salud y no discriminación", *Revista de Derecho, Empresa y Sociedad (REDS)*, 22-23, 2023, 24 y ss.

Egusquiza Balmaseda, M.A.: *Protección de datos: intimidad y salud*, Cuadernos de Aranzadi civil, Aranzadi-Thomson Reuters, 2009.

Etreros Huerta, J., Alonso Villar C., Marco Cuenca, G., Cabronero Fernández, M., Alfaro Latorre, M.: "El sistema de historia clínica digital del sistema nacional de salud: accesibilidad y protección de la información como elementos clave", *Derecho y Salud*, 18 (1), 2009, pp. 99-111.

García Goldar, M.: "Disposición adicional única", en Cañizares Laso A. (dir.), *Comentarios al Texto Refundido de la Ley de Consumidores y Usuarios*, Tirant lo Blanch, T. II., 2022.

Martín Faba, J. M.: "Novedades en materia de indemnización y protección de datos personales", *Revista Cesco de Derecho de Consumo*, núm. 49, 2004.

Navas Navarro, S.: *Datos sanitarios electrónicos. El espacio europeo de datos sanitarios,* Reus, 2023.

Nicolás Jiménez, P., Armaza, E.J., y Perin, A.: "Impact of the Directive 2011/24/UE on the application of patient`s rights in cross-border healthcare. A comparative analysis", *Revista de derecho y genoma humano: genética, biotecnología y medicina avanzada/Law and the human genomereview: genetics, biothechnology and advanced medice*, núm. 44, 2016.

Rubí Puig, A.: "Daños por infracciones del derecho a la protección de datos personales. El remedio indemnizatorio del artículo 82 RGPD, *Revista de Derecho Civil*, vol. 4, núm. 5, 2018.

Rubí Puig, A.: "Problemas de coordinación y compatibilidad entre la acción indemnizatoria del artículo 82 del reglamento general de protección de datos y otras acciones en Derecho Español", *Derecho Privado y Constitución*, núm. 34, 2018 (https://doi.org/10.18042/cepc/dpc.34.05)

Torrelles Torrea, E.: *El derecho al olvido oncológico*, Atelier, 2024.

Trujillo Machuca, V.: "La reclamación de daños y perjuicios en materia de protección de datos, *Actualidad Civil*, núm. 12, 2020.