CAPÍTULO NOVENO.
TRANSPARENCIA, PROTECCIÓN Y CONTROL DE LOS DATOS DE SALUD EN LA SANIDAD DIGITAL[1]

Inmaculada Vivas Tesón
Catedrática de Derecho civil
Universidad de Sevilla

SUMARIO. 1. CONSIDERACIONES PREVIAS. 2. EL MARCO NORMATIVO DE LOS DATOS PERSONALES EN EL ÁMBITO SANITARIO: UN ANÁLISIS CRÍTICO. 3. CUESTIONES DE INTERÉS PRÁCTICO EN TORNO A LA HISTORIA CLÍNICA ELECTRÓNICA. 3.1. La relevancia asistencial y legal de la historia clínica. 3.2. El alcance del derecho de acceso: en concreto, la trazabilidad de los accesos no autorizados a la historia clínica.

1. CONSIDERACIONES PREVIAS

Nuestro sistema de salud debe afrontar, en la actualidad, grandes e innumerables retos, entre los cuales podemos mencionar el progresivo envejecimiento de la población; la implantación de una historia clínica digital e interoperable entre los distintos ámbitos asistenciales y entre las Comunidades autónomas, lo que es muy necesario a la vista de los continuos desplazamientos geográficos de las personas por motivos diversos (labo-

[1] El presente trabajo se enmarca dentro del Grupo de Investigación "Nuevas Dinámicas del Derecho Privado Español y Comparado" (SEJ-617) y del Grupo de investigación consolidado "Discapacidad, Enfermedad Crónica y Accesibilidad a los Derechos" (DECADE) de la Universidad de Alcalá, así como del Proyecto I+D+i "Discriminación a las personas con discapacidad en el ejercicio de la capacidad jurídica en las situaciones internacionales e interregionales (PID2021-127361NB-I00), Ayudas a Proyectos de generación de conocimiento en el marco del Programa Estatal para Impulsar la Investigación Científico-Técnica y su Transferencia, del Plan Estatal de Investigación Científica, Técnica y de Innovación 2021-2023, del que es investigadora responsable la Profª. Goñi Urriza.

rales, ocio, etc.) en el territorio nacional[2]; la absoluta desconexión entre las bases de datos de los servicios públicos de sanidad y las de los seguros y mutuas privadas, lo que impide compartir los datos sanitarios de sus pacientes; la vertiginosa digitalización de procesos, productos y servicios, la llamada *e-Health*, la cual requiere considerables esfuerzos para cerrar por completo las brechas digitales con el fin de que toda la ciudadanía sin excepción pueda aprovechar las bondades de las tecnologías de la información y comunicación (las TICs); la prestación de servicios médicos personalizados, preventivos, predictivos y participativos; la mejora de la transparencia y buen gobierno en la sanidad; la búsqueda constante de la eficacia, eficiencia y calidad en todas y cada una de las actuaciones y procesos y, a la vez, de la optimización del gasto sanitario; la aportación del sector al desarrollo sostenible en cumplimiento de los Objetivos de Desarrollo Sostenible de la Agenda 2030[3] de las Naciones Unidas; la máxima seguridad en la conservación, uso y circulación de los datos clínicos del paciente; y la aplicación de herramientas de Inteligencia Artificial (en adelante, IA) en la toma de decisiones y en la ejecución de las mismas.

Es evidente que la sanidad debe adaptarse a las nuevas realidades y la nueva realidad, ahora, es la era tecnológica.

La perspectiva *Tech* (pensemos en *Big Data, Cloud Computing*, la *MHealth* o el *Internet of Medical Things –IoMT–*) hace del ámbito sanitario un sector estratégico por sus múltiples implicaciones y oportunidades, pero también por sus riesgos presentes y futuros.

La sanidad electrónica y algorítmica tiene, sin duda alguna, un gran impacto en los derechos fundamentales de la persona, así como en el derecho a la protección de su salud (repárese en que no se trata del "derecho a estar sano", el cual, como tal, no puede ser garantizado al ciudadano de ninguna ma-

---

[2] CRAVIOTTO VALLE, P.: *Responsabilidad por el tratamiento indebido de los datos personales de salud: la histórica clínica como eje vertebrador*, Reus, Madrid, 2023, p. 112, expone el complejo escenario que vivimos en España como consecuencia de la descentralización de la gestión sanitaria y la consiguiente legitimidad regulatoria de las diecisiete Comunidades Autónomas con sus respectivos sistemas sanitarios, lo que genera desigualdad e inseguridad jurídica.

Ello llama especialmente la atención porque la Ley 11/2020, de 30 de diciembre, de Presupuestos Generales del Estado para el año 2021, en su Disposición adicional centésima cuadragésima octava, contempló la creación de una Tarjeta Sanitaria Interoperable que, de manera automática, permitiera el intercambio de información de salud de cualquier paciente, con independencia de la Comunidad de residencia del mismo. En enero de 2023, fecha de cierre del presente trabajo, aún no se ha dado cumplimiento a dicha previsión normativa.

[3] En concreto, destaca el ODS 3, Salud y Bienestar (Garantizar una vida sana y promover el bienestar en todas las edades es esencial para el desarrollo sostenible), pero también son importantes para el sector, entre otros, el 9 (Industria, Innovación e Infraestructura), el 12 (Producción y Consumo Responsables) y el 13 (Acción por el Clima).

nera), que, aunque pueda resultar extraño, no goza, en nuestra Carta Magna, de la misma naturaleza de aquéllos al encontrarse ubicado en su art. 43, esto es, entre los principios rectores de la política social y económica. Se trata, por consiguiente, de un derecho social. Ello explica que sea desarrollado por la legislación ordinaria, que carezca de contenido constitucionalmente esencial[4] y que no goce de la tutela reforzada prevista en el art. 53.1º y 2º de la Norma Suprema.

Conforme a ello, no es susceptible de recurso de amparo, a pesar de lo cual el Tribunal Constitucional suele ponerlo en conexión con los derechos fundamentales a la vida y a la integridad física y moral consagrados por el art. 15, así como con la libertad religiosa del art. 16[5], lo que es tremendamente lógico y muy atinado.

Además, los datos relativos al estado de salud son datos de carácter personal, de modo que el tratamiento indebido de dicha información puede vulnerar otro derecho fundamental, el reconocido por el art. 18.4 de nuestra Carta Magna, de indiscutible naturaleza autónoma respecto al derecho a la intimidad del art. 18.1, del que es tan afín, pero del que difiere en su función, objeto y contenido[6].

Si en las sociedades contemporáneas basadas en la datacracia (por tanto, en el control y vigilancia de la ciudadanía está fuera de duda que los datos personales lo son todo, hasta el punto que podría decirse que vivimos permanentemente sumergidos en un tsunami de datos, es en el campo sanitario donde lo comprobamos con mayor claridad, pues aquéllos son los recursos necesarios para proteger la salud. En éste, como en ningún otro ámbito de la sociedad, los datos evidencian su extraordinaria potencialidad. Sin paciente y sin sus datos no puede ponerse en marcha el ecosistema sanitario. Los datos de los pacientes son la llave de la actividad asistencial, pero también de la prosperidad colectiva, por ello debemos ser conscientes del valor de nuestros datos personales, de lo que está en juego.

Y en el contexto de los cuidados médicos no se trata, únicamente, de proteger los datos clínicos del paciente y respetar su intimidad, sino que promover su dignidad y libertad en la toma de decisiones debe ser, en todo momento, una prioridad absoluta. La dignidad de la persona es un derecho inviolable que es exigible con mayor intensidad si cabe cuanto más frágil o vulnerable se encuentre por causa de la enfermedad, la desnudez, el dolor, el sufrimiento o la llegada de la muerte. En realidad, la dignidad del profesional (si se trata de un robot, evidentemente, la cosa cambia, si bien, en última instancia, siempre debe existir

4 Vid. STC 139/2016, de 21 de julio.

5 Entre otras, la STC 62/2007, de 27 marzo y STC 37/2011, de 28 marzo.

6 Vid. FJ 5º 6º y 7º de la STC 292/2000, de 30 de noviembre.

la acción de un ser humano) se mide por su respeto a la del paciente. Respetar al prójimo es respetarse a uno mismo.

Desde la óptica constitucional se trata, aunque cueste mucho entenderlo pues sin salud no hay nada, de un derecho social. De un derecho social peculiar, pues tiene una dimensión individual y otra colectiva, como ha evidenciado, de manera cristalina, la pandemia mundial del Covid-19, durante la cual hemos sido testigos directos de la recopilación masiva de los datos del estado de salud de los ciudadanos, quienes parecen cada vez estar más concienciados en cuanto al alto valor de su información personal y de los riesgos a los que, continuamente, los expone el mundo digital y, en consecuencia, van ensanchando poco a poco su empoderamiento al respecto, con excepción de aquéllos que, asombrosamente, prefieren sacrificar su privacidad a cambio de míseras ofertas y promociones e, incluso, de forma gratuita.

Conforme a dicha doble y simultánea perspectiva, individual y social, desde la cual han de ser contemplados y regulados, los datos clínicos se caracterizan por la tensión entre, de un lado, su máxima confidencialidad basada en la confianza depositada en el secreto profesional y, de otro, su circulación (aunque circunscrita a la adecuada, pertinente y necesaria para los fines para los que son tratados conforme al principio de minimización) para la protección de la salud pública y el avance de la investigación científica sobre nuevas formas de terapia, nuevas tecnologías de tratamiento y nuevos medicamentos. Si nos paramos a pensar, una auténtica paradoja, pues son datos que no deberían conocer personas ajenas al paciente y a los profesionales que le proveen la atención sanitaria sin mediar su consentimiento informado, pero, al mismo tiempo y preservando adecuadamente la privacidad de su titular, deben circular porque encierran una información vital para predecir escenarios sanitarios futuros, de ahí su enorme transcendencia y valor. En definitiva, son datos íntimos de la persona que, contradictoriamente, van más allá de su propia individualidad.

Las *smarts tecnologies* o herramientas inteligentes desempeñan un papel crucial en la atención sanitaria actual, tanto en el ámbito del diagnóstico y tratamiento como en el de los procesos de gestión y organizativos. La materia prima de la que se alimentan no es otra que los datos clínicos de las personas, los cuales son altamente delicados o sensibles porque expresan la esencia más auténtica de nuestro yo físico y psíquico y, por tanto, son susceptibles de exponer al individuo y a su vulnerabilidad (temporal o permanente) a las más mezquinas etiquetas y discriminaciones (pensemos en la contratación laboral, bancaria y de seguros[7]), de ahí el comprensible temor por las injerencias

[7] Acerca de dicha problemática, vid. VIVAS TESÓN, I., "El Derecho contractual antidiscriminatorio: *Drittwirkung* y libertad negocial", en *Cuadernos de Derecho Transnacional*, vol. 13, nº 1, 2021, pp. 672-692.

indebidas, los riesgos de alteración de la información, así como por los eventuales ciberataques a las infraestructuras informáticas con el fin de lucrarse a costa de nuestros datos.

Es innegable que los procesos relacionados con la salud, sobre todo, aquéllos que pueden facilmente mecanizarse por su carácter repetitivo, están transformándose al ritmo vertiginoso que marcan los imparables avances tecnológicos y, en consecuencia, deben ser reformulados a medida que aquéllos van sucediéndose, si bien, por cuanto ahora nos ocupa, un principio que sigue siendo clave y permanece invariable en nuestros días es el de garantizar la seguridad y privacidad de los datos de salud del paciente, tanto para fines de diagnóstico y terapia como de investigación.

Las entidades y personas involucradas en este sector son muchas: los pacientes y sus familiares, los hospitales y centros de salud (públicos y privados), el personal sanitario[8] y de administración de servicios, las empresas farmacéuticas, los proveedores de servicios de la sociedad de la información, los docentes y estudiantes universitarios, etc. Por si fuera poco, a ellos se suman las "máquinas inteligentes" o agentes artificiales, los cuales se nutren de cantidades ingentes de datos personales para realizar el aprendizaje automático (*machine learning*) y extraer decisiones algorítmicas (verdades construidas por un *software*), que, lejos de ser neutrales (ni técnica ni éticamente) y exentas de sesgos como ingenuamente pudiera pensarse, pueden llegar a ser dañinas para el paciente.

Uno de los problemas frecuentes en la práctica está ligado a la falta de concienciación tanto de los pacientes como de los operadores acerca de las implicaciones que conlleva la cesión y control de datos de carácter personal, pues ello se percibe por unos y otros como un mero trámite burocrático que se limita a la entrega de documentación y marcado de una casilla y no como un derecho fundamental a la protección de la información relativa a nosotros mismos. Los distintos profesionales que gestionan las historias clínicas de los

[8] Entre los operadores sanitarios que ejercen una actividad asistencial podemos citar, sin ánimo de exhaustividad: médicos, farmacéuticos; odontólogos; veterinarios; psicólogos; enfermeros; fisioterapeutas; óptico-optometristas; y profesionales de la nutrición humana y dietética.

Para mayor detalle, vid. la Ley 44/2003, de 21 de noviembre, de Ordenación de las Profesiones Sanitarias.

No puede olvidarse que los datos de salud también son tratados en ámbitos distintos al sanitario, como las clínicas de estética y centros de piercings, micropigmentación y tatuajes, que no tienen la consideración de operadores sanitarios pero que han de cumplir la correspondiente reglamentación administrativa en cuanto a las condiciones técnicas e higiénico-sanitarias que han de observar los establecimientos y los profesionales de dichas actividades. Asimismo, los datos de salud son proporcionados a clubs deportivos, centros educativos y a aseguradoras.

Así las cosas, los datos de salud no se circunscriben únicamente el sector médico-sanitario.

pacientes deben conocer las consecuencias que puede acarrear fisgar en las mismas.

La irrupción de las tecnologías en la práctica sanitaria ha supuesto un auténtico cambio de paradigma, el cual ha tenido un impulso acelerado a raíz de la pandemia mundial del Covid-19. Son muchas las herramientas digitales de salud: videoconsultas, acceso de imágenes *online*, informes médicos digitalizados, *chatbots*, dispositivos electrónicos con sensores para medir parámetros fisiológicos (como la frecuencia cardíaca, el nivel de glucosa en sangre, la saturación de oxígeno o la presión arterial) y monitorizar las condiciones de salud para diagnosticar enfermedades de forma más ágil y precisa, prescripciones electrónicas, prótesis artificiales conectadas y *Apps* móviles sanitarias (sobre éstas, ha de tenerse en cuenta que no todas las aplicaciones sobre nutrición, deporte y estilos de vida saludables que instalamos en nuestros *smartphones* y *tablets* son productos sanitarios a los efectos del Reglamento UE 2017/745, del Parlamento Europeo y del Consejo de 5 de abril de 2017[9], si bien todas recopilan datos clínicos de sus usuarios –vgr. alergias, intolerancias alimentarias, índice de masa corporal, etc.-). Nuestra salud está en línea y nuestros datos sensibles se albergan en servidores o circulan por y entre redes informáticas con suma facilidad. Las amenazas y peligros aumentan a la par que el número de dispositivos e infraestructuras sanitarias conectadas.

El escenario es, indudablemente, harto complejo, pero debe ser exactamente igual de garantista con los derechos y libertades fundamentales de la persona como lo viene siendo hasta ahora. Las reglas del juego deben seguir siendo las mismas, también en el campo de la IA aplicada a la salud y a los cuidados, en el que se plantean problemáticas jurídicas novedosas, como la relativa a la responsabilidad médico-sanitaria por los daños causados por máquinas supuestamente inteligentes pero, en cuanto a la que ahora nos ocupa, la concerniente a la protección de los datos médicos, nada cambia. Los algoritmos no están por encima de la ley.

Revelar una información de salud no puede ser fruto de la elección de otros, sino una decisión consciente y consentida de su titular. Tampoco puede depender de un error en la comunicación de resultados a persona distinta de su destinatario o de ciberataques como consecuencia de las deficiencias técnicas de los sistemas informáticos. La máxima seguridad en el uso y circulación de los datos personales en la prestación de un servicio en el ámbito sanitario ha de constituir un objetivo prioritario al margen de cuál sea el concreto es-

[9] Vid. art. 2.1 del Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo de 5 de abril de 2017 sobre los productos sanitarios, por el que se modifican la Directiva 2001/83/CE, el Reglamento (CE) n.º 178/2002 y el Reglamento (CE) n.º 1223/2009 y por el que se derogan las Directivas 90/385/CEE y 93/42/CEE del Consejo, aplicable desde el 26 de mayo de 2021.

tado de la tecnología (el actual y el que esté por venir) y de sus particulares especificidades.

Vivimos en el milenio dominado por la omnipotencia del dato y por las TICs, cuyas ventajas, a estas alturas, son indiscutibles, pero también los riesgos que encierran en cuanto a la vulneración de los derechos fundamentales de la persona. Así las cosas, debe seguir apostándose por las tecnologías emergentes, pero velando por la protección de los derechos y libertades de los ciudadanos y, más concretamente, reforzando los protocolos de privacidad y seguridad en el tratamiento automatizado de los datos clínicos mediante la adopción de medidas técnicas y organizativas eficaces. En el sistema sanitario contemporáneo ha de tratarse de alcanzar una equilibrada integración entre la dimensión humana y el avance tecnológico en salud. El mensaje es claro: debemos avanzar en las tecnologías pero sin deshumanizar un ápice el entorno sanitario.

2. EL MARCO NORMATIVO DE LOS DATOS PERSONALES EN EL ÁMBITO SANITARIO: UN ANÁLISIS CRÍTICO

El escenario regulatorio de los datos de carácter personal ha encontrado un decisivo impulso en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en adelante, RGPD), el cual ha pretendido ponerse al mismo nivel que el irrefrenable progreso técnico, lo que, seamos realistas, resulta imposible. Al momento de publicarse la norma comunitaria, su obsolescencia estaba ya más que asegurada. La sociedad algorítmica se asienta sobre unos parámetros específicos que difieren, considerablemente, de los de la sociedad de la información.

La definición de datos relativos a la salud la encontramos en su art. 4.15), según el cual son 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[10].

Su Considerando 35, de forma más pormenorizada, establece 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

[10] Para un detenido estudio, vid. BELTRÁN AGUIRRE, J. L., "Tratamiento de datos personales de salud: Incidencia del reglamento general de protección de datos", en *Salud electrónica: Perspectiva y realidad*, PÉREZ GÁLVEZ (dir.), Tirant lo Blanch, Valencia, 2017, pp. 86-123.

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; 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".

Tales datos se incluyen en la categoría más amplia de datos sujetos a tratamiento especial contemplados por el art. 9 del RGPD, ya que son capaces de revelar detalles muy íntimos de la persona, razón por la cual son objeto de protección reforzada.

Dicho precepto establece una prohibición general sobre el tratamiento de datos relativos a la salud que el propio legislador comunitario levanta cuando concurra una de las circunstancias contempladas en su apartado 2º, algunas de las cuales se refieren específicamente a los datos de salud mientras que otras los comprenden al no hacer distinción en cuanto a concretos tipos de datos:

- Consentimiento explícito del interesado;
- Resulte necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social;
- Resulte necesario para proteger intereses vitales del interesado, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento;
- Es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical;
- Se refiere a datos personales que el interesado ha hecho manifiestamente públicos;

- Es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial;
- Es necesario por razones de un interés público esencial;
- 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, cuando su tratamiento sea realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad;
- Es necesario por razones de interés público en el ámbito de la salud pública[11], 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;
- Es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos.

El art. 9, en su apartado 4º, deja a los Estados miembros la posibilidad de "mantener o introducir nuevas condiciones, incluidas limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud", lo que puede entorpecer la deseable armonización del tratamiento de tales categorías de datos en la Unión Europea al permitirse que los Derechos nacionales adopten medidas diferentes. De ello es consciente el legislador comunitario, a la vista de lo que afirma en el Considerando 53 del RGPD: "el presente Reglamento debe establecer condiciones armonizadas para el tratamiento de categorías especiales de datos personales relativos a la salud, en relación con necesidades específicas, en particular si el tratamiento

[11] Según el Considerando 54 del RGPD, "el tratamiento de categorías especiales de datos personales, sin el consentimiento del interesado, puede ser necesario por razones de interés público en el ámbito de la salud pública. Ese tratamiento debe estar sujeto a medidas adecuadas y específicas a fin de proteger los derechos y libertades de las personas físicas. En ese contexto, «salud pública» debe interpretarse en la definición del Reglamento (CE) n.º 1338/2008 del Parlamento Europeo y del Consejo (1), es decir, todos los elementos relacionados con la salud, concretamente el estado de salud, con inclusión de la morbilidad y la discapacidad, los determinantes que influyen en dicho estado de salud, las necesidades de asistencia sanitaria, los recursos asignados a la asistencia sanitaria, la puesta a disposición de asistencia sanitaria y el acceso universal a ella, así como los gastos y la financiación de la asistencia sanitaria, y las causas de mortalidad. Este tratamiento de datos relativos a la salud por razones de interés público no debe dar lugar a que terceros, como empresarios, compañías de seguros o entidades bancarias, traten los datos personales con otros fines".

de esos datos lo realizan, con fines relacionados con la salud, personas sujetas a la obligación legal de secreto profesional. El Derecho de la Unión o de los Estados miembros debe establecer medidas específicas y adecuadas para proteger los derechos fundamentales y los datos personales de las personas físicas. Los Estados miembros deben estar facultados para mantener o introducir otras condiciones, incluidas limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud". Y añade en el inciso final: "No obstante, esto no ha de suponer un obstáculo para la libre circulación de datos personales dentro de la Unión cuando tales condiciones se apliquen al tratamiento transfronterizo de esos datos".

Por su parte, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), en su art. 9.2, dispone que "los tratamientos de datos contemplados en las letras g), h) e i) del artículo 9.2 del Reglamento (UE) 2016/679 fundados en el Derecho español deberán estar amparados en una norma con rango de ley, que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad. En particular, dicha norma podrá amparar el tratamiento de datos en el ámbito de la salud cuando así lo exija la gestión de los sistemas y servicios de asistencia sanitaria y social, pública y privada, o la ejecución de un contrato de seguro del que el afectado sea parte".

Repárese en que dicha previsión normativa hace descansar en una "norma con rango de ley" el tratamiento de datos en el ámbito de la salud en los supuestos contemplados, esto es, puede no ser una ley orgánica, cuyo carácter es expresamente exigido por el art. 81.1 de nuestra Constitución para la regulación de los derechos fundamentales y libertades públicas. Con tal reserva de ley cumplen las normas citadas por el apartado 1º de la Disposición Adicional 17ª de la LOPDGDD[12], a la cual confiere carácter orgánico en su Disposición Final 1ª.

[12] Según el aptdo. 1º de la DA 17ª de la LOPDGDD, "se encuentran amparados en las letras g), h), i) y j) del artículo 9.2 del Reglamento (UE) 2016/679 los tratamientos de datos relacionados con la salud y de datos genéticos que estén regulados en las siguientes leyes y sus disposiciones de desarrollo:

a) La Ley 14/1986, de 25 de abril, General de Sanidad.

b) La Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales.

c) 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.

d) La Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud.

e) La Ley 44/2003, de 21 de noviembre, de ordenación de las profesiones sanitarias.

f) La Ley 14/2007, de 3 de julio, de Investigación biomédica.

g) La Ley 33/2011, de 4 de octubre, General de Salud Pública.

h) La Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras.

Junto a la norma comunitaria y a la LOPDGDD, el *corpus* normativo regulador de los datos clínicos está integrado también por legislación sectorial en el campo de la salud y, en particular, por 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 (en adelante, LAP), la cual, sorprendentemente, no ha sido modificada por la Ley 8/2021, de 2 de junio, por la que se reforma la legislación civil y procesal para el apoyo a las personas con discapacidad en el ejercicio de su capacidad jurídica, lo que está provocando no pocos problemas interpretativos en la práctica.

Pues bien, la dificultad estriba en que, en materia de tratamiento de datos de salud, deben aplicarse, de manera conjunta y complementaria, el RGPD, la LOPDGDD y la LAP, así como las correspondientes legislaciones autonómicas dictadas en virtud de la competencia sobre sanidad e higiene reconocida por el art. 148.1.21ª de la Constitución española. Así las cosas, el panorama actual se caracteriza por una enorme disparidad y complejidad normativa. Por ello, se echa muy en falta una ley específica sobre los datos de salud y el tratamiento de los mismos, la cual logre, en aras de una mayor seguridad jurídica, la ansiada homogeneidad jurídica.

Debemos mencionar, por su transcendencia, que la Comisión Europea presentó el 3 de mayo de 2022 una propuesta de Reglamento para crear el Espacio Europeo de Datos Sanitarios[13]. Según dicha propuesta, el Espacio Europeo de Datos Sanitarios es un ecosistema específico para la salud formado por reglas, normas y prácticas comunes, infraestructuras y un marco de gobernanza cuyo objetivo es:

- empoderar a las personas con el fin de que puedan tener un mayor control y acceso digital a sus datos sanitarios personales electrónicos, tanto a escala nacional como de la UE, así como apoyar su libre circulación, fomentando un auténtico mercado único para los sistemas de historiales médicos electrónicos, los productos sanitarios pertinentes y los sistemas de IA de alto riesgo (uso primario de los datos);

- ofrecer un marco coherente, fiable y eficiente para el uso de datos sanitarios en actividades de investigación, innovación, formulación de políticas y reglamentación (uso secundario de los datos).

---

i) El texto refundido de la Ley de garantías y uso racional de los 105 medicamentos y productos sanitarios, aprobado por Real Decreto Legislativo 1/2015, de 24 de julio.

j) El texto refundido de la Ley General de derechos de las personas con discapacidad y de su inclusión social, aprobado por Real Decreto Legislativo 1/2013 de 29 de noviembre".

[13] Proposal for a regulation - The European Health Data Space, COM(2022) 197/2.

De este modo, el Espacio Europeo de Datos Sanitarios sería el primer espacio común de datos de la UE en un ámbito específico, convirtiéndose en un pilar clave de la sólida UE de la salud.

3. CUESTIONES DE INTERÉS PRÁCTICO EN TORNO A LA HISTORIA CLÍNICA ELECTRÓNICA

3.1. La relevancia asistencial y legal de la historia clínica

Según el art. 4.1 de la LAP[14], el paciente tiene derecho a conocer su información asistencial.

Pues bien, una de las cuestiones más controvertidas en la práctica sanitaria es la relativa a los usos y accesos a la historia clínica.

Conforme al art. 15.2 de la LAP, "la historia clínica tendrá como fin principal facilitar la asistencia sanitaria, dejando constancia de todos aquellos datos que, bajo criterio médico, permitan el conocimiento veraz y actualizado del estado de salud", lo que pone de manifiesto el valor probatorio del contenido de la historia clínica ante una eventual reclamación de responsabilidad por una concreta actuación sanitaria, a la vista de su capacidad para reflejar la asistencia recibida por el paciente y su sujeción o no a parámetros legales y deontológicos. En definitiva, es un instrumento de carácter médico y también legal, de ahí su enorme relevancia.

Según el FJ. 4º de la SAP de Pontevedra (Sección 6ª) de 23 de julio de 2010, "la historia clínica es un documento fundamental en el que se plasma la relación entre médico y paciente; participa de las características de una reseña biográfica, si se toma en consideración la perspectiva del paciente, y supone, desde la del médico, una elaboración científica integrada, fundamentalmente, por apreciaciones, valoraciones y hallazgos clínicos. Sirve de memoria al propio médico y, a la vez, es fuente de información para otros profesionales y, en ocasiones, para los tribunales.

La naturaleza de la historia clínica desde una perspectiva jurídica que permita atribuir facultades de gobierno, control o disposición, sobre ella, y, por ende, de su custodia, encierra cierta complejidad y no es tarea fácil; de ahí la diversi-

[14] Art. 4.1 de la LAP: "1. Los pacientes tienen derecho a conocer, con motivo de cualquier actuación en el ámbito de su salud, toda la información disponible sobre la misma, salvando los supuestos exceptuados por la Ley. Además, toda persona tiene derecho a que se respete su voluntad de no ser informada. La información, que como regla general se proporcionará verbalmente dejando constancia en la historia clínica, comprende, como mínimo, la finalidad y la naturaleza de cada intervención, sus riesgos y sus consecuencias".

dad de opiniones, de signo diverso. Esa complejidad es debida a que convergen en ella intereses diversos, y siempre habrá una tendencia a atribuir a los titulares o portadores de esos intereses una suerte de titularidad preeminente sobre la historia clínica, según la perspectiva que se adopte".

No hay duda de que la información referida a la historia clínica debe ser considerada datos de salud *ex* art. 4.15) del RGPD y, por tanto, se incluye dentro de las categorías especiales de datos cuyo tratamiento prohíbe el apartado 1º de su art. 9, si bien constituye uno de los supuestos excepcionales que se recogen en su apartado 2º y, en concreto, el contemplado por su letra h), el cual, según el art. 9.2 de la LOPDGDD, está amparado por la LAP, citada explícitamente por el apartado 1º, letra c), de su Disposición Adicional 17ª.

En España, la historia clínica en papel pasó hace ya algún tiempo a digitalizarse. La historia clínica electrónica o digital es un registro informatizado formado por todos aquellos datos clínicos relevantes para la atención sanitaria de un paciente. Cada Comunidad autónoma está realizando esfuerzos para implantarla, mientras que el Gobierno central está tomando medidas para solucionar su principal problema, la interoperabilidad de la que denomina "Historia de Salud Digital"[15], la cual deberá alcanzarse en el cuarto trimestre de 2023 en todas las Comunidades autónomas entre distintos ámbitos asistenciales, al menos, entre atención primaria y atención hospitalaria. Como aspectos destacables a reseñar, de un lado, tales medidas excluyen a los servicios sanitarios privados y, de otro, se propone que la historia clínica digital vaya más de los datos de salud del paciente y en ella se incluyan condicionantes sociales y de contexto familiar para un "abordaje biopsicosocial" en la consulta, de manera que los equipos profesionales pueden conocer y tener en cuenta las condiciones de vida de la persona a la hora de hacer un diagnóstico, una recomendación, un seguimiento o una propuesta de manejo o de cuidados. Si bien tales condicionantes deberán ser definidos por un grupo de trabajo específico, a primera vista, parece apuntar al lugar de origen del paciente, sus antecedentes familiares, su estilo de vida e, incluso, su situación económica, lo que nos inquieta y mucho.

3.2. El alcance del derecho de acceso: en concreto, la trazabilidad de los accesos no autorizados a la historia clínica

El tratamiento de los datos de las personas físicas, titulares de las historias clínicas de las que dispone un centro sanitario, se encuentra sometido a los principios y garantías de la normativa de protección de datos personales, entre

[15] Vid. Plan de Acción de Atención Primaria y Comunitaria 2022-2023, aprobado por el Consejo Interterritorial del Sistema Nacional de Salud el 15 de diciembre de 2021.

los que se encuentra el principio de licitud, lealtad y transparencia, así como de integridad y confidencialidad *ex* art. 5.1 del RGPD.

Conforme al art. 15 del RGPD (al que se remite el art. 13 de la LOPDGDD), el interesado tendrá derecho de acceso a sus datos personales y a exigir al responsable del tratamiento la siguiente información:

- Copia de los datos personales objeto de tratamiento (si se pide más de una copia, el responsable podrá cobrar por ella);
- Los fines del tratamiento;
- Las categorías de datos personales de que se trate;
- Los destinatarios[16] o las categorías de destinatarios a los que se comunicaron o se comunicarán los datos personales, en particular, destinatarios en terceros u organizaciones internacionales;
- De ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo;
- La existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento;
- El derecho a presentar una reclamación ante una autoridad de control;
- Cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen;
- La existencia de decisiones automatizadas, incluida la elaboración de perfiles, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado;

[16] Según el art. 4.9) del RGPD, "destinatario" es "la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento".

- Cuando se transfieran datos personales a un tercer país o a una organización internacional, el interesado tendrá derecho a ser informado de las garantías adecuadas relativas a la transferencia.

El art. 12.5 de la LOPDGDD dispone que cuando las leyes aplicables a determinados tratamientos establezcan un régimen especial que afecte al ejercicio de los derechos previstos en el Capítulo III del Reglamento (UE) 2016/679, se estará a lo dispuesto en aquéllas. Por consiguiente, debemos acudir a la LAP, la cual, en su art. 3, define la historia clínica como el conjunto de documentos que contienen los datos, valoraciones e informaciones de cualquier índole sobre la situación y la evolución clínica de un paciente a lo largo del proceso asistencial.

De ella se ocupa, con detenimiento, en sus arts. 14 y ss.[17].

Según su art. 18, el paciente tiene derecho de acceso a la documentación (en papel o electrónica) de su historia clínica y a obtener copia de los datos que figuran en ella, si bien dicho derecho no puede ejercitarse en perjuicio del de terceras personas a la confidencialidad de los datos que constan en ella recogidos en interés terapéutico del paciente, ni en perjuicio del de los profesionales participantes en su elaboración, los cuales pueden oponer al derecho de acceso la reserva de sus anotaciones subjetivas[18].

---

[17] Vid. art. 19 del Código de Deontología Médica.

[18] La LAP no aclara qué ha de entenderse por "anotaciones subjetivas", como sí hacen, en cambio, algunas normas autonómicas, como el art. 21.1. del Decreto 29/2009, de 5 de febrero, por el que se regula el uso y acceso a la historia clínica electrónica de Galicia ("se entiende por anotaciones subjetivas las valoraciones personales, sustentadas o no en los datos clínicos de que se disponga en ese momento, que no formando parte de la historia clínica actual del/de la paciente o usuario/a, puedan influir en el diagnóstico y futuro tratamiento médico una vez constatadas") y el art. 7.4 del Decreto 38/2012, de 13 de marzo, sobre historia clínica y derechos y obligaciones de pacientes y profesionales de la salud en materia de documentación clínica del País Vasco ("se entenderán por anotaciones subjetivas las impresiones o valoraciones personales de las y los profesionales sanitarios no sustentadas directamente en datos objetivos o pruebas complementarias y que, en su criterio, resulten de interés para la atención sanitaria de la persona paciente").

Por su regulación más detallada, traemos a colación el art. 64.4. de la Ley foral 17/2010, de 8 de noviembre, de derechos y deberes de las personas en materia de salud en la Comunidad foral de Navarra, el cual dispone que "a los efectos de lo dispuesto en la presente Ley Foral, se entenderán por anotaciones subjetivas las impresiones o valoraciones personales de los profesionales sanitarios no sustentadas directamente en datos objetivos o pruebas complementarias y que, en su criterio, resulten de interés para la atención sanitaria del paciente. Se considerarán anotaciones subjetivas únicamente aquellas que puedan encuadrarse en algunos de los siguientes apartados:

Valoraciones sobre hipótesis diagnósticas no demostradas.

Sospechas acerca de incumplimientos terapéuticos.

Sospechas de tratamientos no declarados.

Sospechas de hábitos no reconocidos.

Los centros sanitarios y los facultativos de ejercicio individual sólo facilitarán el acceso a la historia clínica de los pacientes fallecidos a las personas vinculadas a él, por razones familiares o de hecho, salvo que el fallecido lo hubiese prohibido expresamente y así se acredite. En cualquier caso el acceso de un tercero a la historia clínica motivado por un riesgo para su salud se limitará a los datos pertinentes. No se facilitará información que afecte a la intimidad del fallecido ni a las anotaciones subjetivas de los profesionales, ni que perjudique a terceros.

Por consiguiente, el derecho de acceso a la historia clínica por el propio paciente (o sus representantes legales[19]), esto es, a su propia información personal, no es absoluto, pues está sujeto a las limitaciones legalmente establecidas. En el caso de pacientes fallecidos, el acceso a la historia clínica por personas con vínculo familiar o de hecho puede ser vetado expresamente por el propio paciente en vida.

Sin embargo, la problemática se plantea, mayormente, ante los accesos indebidos a la historia clínica por terceros que no son ni el paciente ni sus allegados, esto es, profesionales sanitarios que no intervienen en la atención al paciente, personal de administración, gestión o inspección del centro sanitario o bien personas ajenas al ámbito asistencial. La trazabilidad de tales accesos no autorizados a la historia clínica del paciente requiere algunas reflexiones jurídicas.

Vayamos por partes.

El art. 7.1 de la LAP dispone que "toda persona tiene derecho a que se respete el carácter confidencial de los datos referentes a su salud, y a que nadie pueda acceder a ellos sin previa autorización amparada por la Ley".

Pues bien, una de las cuestiones controvertidas que se plantea en relación a dicho principio de preservación de la privacidad de los datos de salud de las

---

Sospechas de haber sido víctima de malos tratos.

Comportamientos insólitos.

Los profesionales sanitarios deberán abstenerse de incluir expresiones, comentarios o datos que no tengan relación con la asistencia sanitaria del paciente o que carezcan de valor sanitario".

Acerca de la materia, vid. SEOANE RODRÍGUEZ, J. A., "Historia clínica y derechos fundamentales: una reflexión sobre las anotaciones subjetivas", en *Datospersonales.org: La revista de la Agencia de Protección de Datos de la Comunidad de Madrid*, nº 21, 2006.

[19] Una cuestión no resuelta a día de hoy de manera satisfactoria es la consulta de la historia clínica del menor de edad por parte de sus representantes legales, sobre todo, cuando el hijo tiene 16 años, mayoría de edad sanitaria. De ello tuvimos ocasión de ocuparnos en VIVAS TESÓN, I., "Autodeterminación informativa, validez del consentimiento y protección de datos sensibles: críticas al nuevo marco normativo", en *Revista de Derecho y genoma humano: genética, biotecnología y medicina avanzada*, nº 1, 2019, pp. 233-271.

personas y la correlativa obligación de confidencialidad de los centros y profesionales sanitarios es si el paciente tiene derecho a ser informado acerca de la existencia de accesos no autorizados a su historia clínica para fines distintos a los asistenciales (para utilizar en un proceso de divorcio, por tratarse de un personaje famoso, etc.) y, en su caso, a conocer la identidad de la persona que consulta indebidamente dicha información reservada, conducta que, además de infringir el correspondiente código deontológico y ser susceptible de sanción disciplinaria, es constitutiva de delito, en concreto, el de descubrimiento y revelación de secretos (art. 197 del Código penal), por ello que sobre la materia encontremos pronunciamientos de nuestros tribunales, como, entre otros, la Sentencia de 25 de septiembre de 2020 de la Sala de lo penal del Tribunal Supremo, que ventila el caso del acceso de dos enfermeros a la historia clínica de un compañero que se encontraba en situación de baja laboral sin su consentimiento ni conocimiento y sin que mediara relación asistencial que pudiera justificar el acceso. Presentada la correspondiente denuncia, los dos enfermeros fueron condenados penalmente, así como al pago de una indemnización por los perjuicios causados. El procedimiento giró, concretamente, en torno a la licitud o no de la prueba obtenida, de manera irregular, por el denunciante para conocer quién había accedido a su historia clínica ("pantallazos" que le proporcionó un médico) y, en su caso, si con ello habían sido conculcados los derechos de los acusados en el proceso[20].

[20] El Supremo, al realizar el correspondiente juicio de ponderación, toma en consideración lo siguiente:

a) En cuanto a la entidad o naturaleza de la ilicitud en la obtención de pruebas, el hecho de conocer o identificar a las personas que han consultado una historia clínica no supone lesión alguna del derecho a la protección de datos.

Según declara la STC 292/2000, de 30 de noviembre, el derecho reconocido en el art. 18.4 CE "[...] contiene, en los términos de la STC 254/1993, un instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los restantes derechos de los ciudadanos que, además, es en sí mismo "un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama la informática", lo que se ha dado en llamar "libertad informática" (FJ 6, reiterado luego en las SSTC 143/1994, FJ 7, 11/1998, FJ 4, 94/1998, FJ 6, 202/1999, FJ 2). La garantía de la vida privada de la persona y de su reputación poseen hoy una dimensión positiva que excede el ámbito propio del derecho fundamental a la intimidad (art. 18.1 CE), y que se traduce en un derecho de control sobre los datos relativos a la propia persona. La llamada "libertad informática" es así derecho a controlar el uso de los mismos datos insertos en un programa informático (*"habeas data"*) [...]".

Difícilmente puede invocar ese derecho quien, como el recurrente, accede a un sistema informático violentando las normas de acceso para conocer información reservada de otra persona y cuando, además, su conducta es constitutiva de delito.

Es cierto que el denunciante también accedió a la información del sistema al margen de las vías previstas legal o reglamentariamente, pero esa irregularidad no es comparable y, desde luego, carece de relevancia constitucional. El denunciante accedió a sus propios datos personales, que figuraban en la base de datos por disposición legal y a cuyo conocimiento tenía derecho. La

Según el art. 15.2 de la LAP, el contenido mínimo de la historia clínica es el siguiente:

a) La documentación relativa a la hoja clínico-estadística.

b) La autorización de ingreso.

c) El informe de urgencia.

d) La anamnesis y la exploración física.

e) La evolución.

f) Las órdenes médicas.

g) La hoja de interconsulta.

h) Los informes de exploraciones complementarias.

i) El consentimiento informado.

j) El informe de anestesia.

k) El informe de quirófano o de registro del parto.

l) El informe de anatomía patológica.

m) La evolución y planificación de cuidados de enfermería.

n) La aplicación terapéutica de enfermería.

ñ) El gráfico de constantes.

o) El informe clínico de alta[21].

irregularidad de su conducta se limitó a no haber utilizado el cauce reglamentariamente previsto. En cambio, los condenados accedieron al sistema no sólo al margen de los cauces previstos legamente, sino para conocer una información ajena, que no les era permitido conocer, cometiendo un delito. Las conductas descritas no son equiparables y en el caso de los recurrentes no hubo lesión alguna de su derecho a la protección de datos. La ausencia de lesión constitucional bastaría por sí para rechazar la nulidad de las pruebas que se interesa en el recurso.

b) Por otra parte y desde una perspectiva interna, en relación con el proceso al que las pruebas se aportaron, la actuación del denunciante no parece que estuviera orientada a obtener pruebas al margen de los cauces constitucionalmente exigibles, sino simplemente a obtener información. Además, la actuación del denunciante no tuvo ningún tipo de conexión instrumental, objetiva o subjetiva, con las actuaciones investigadoras de las autoridades o funcionarios españolas. Fue previa al inicio de las investigaciones policiales, y absolutamente desconectada de éstas.

c) Y, por último, desde el punto de vista externo, tampoco apreciamos la existencia de un riesgo cierto de propiciar, con la admisión de la prueba controvertida, prácticas que comprometan pro futuro la efectividad del derecho fundamental en juego en el ordenamiento jurídico español" (FJ. 1º).

En consecuencia, la petición de nulidad de las pruebas de cargo no es acogida favorablemente.

[21] Los párrafos b), c), i), j), k), l), ñ) y o) sólo serán exigibles en la cumplimentación de la historia clínica cuando se trate de procesos de hospitalización o así se disponga.

Como puede fácilmente inferirse del tenor literal del precepto, se trata de un "contenido de mínimos" y, dado que la LAP es una norma estatal básica, si una autonómica contemplara un contenido adicional de la historia clínica, deberá estarse a lo en ella dispuesto, en concreto, por cuanto ahora nos incumbe, si prevé que el contenido del derecho de acceso a la historia clínica comprende, también, conocer quién ha accedido a la misma, tal y como hacen, entre otras, el art. 35.3 de Ley 3/2005, de 8 de julio de información sanitaria y autonomía del paciente de Extremadura y el art. 31.1 de la Ley foral 17/2010, de 8 de noviembre, de derechos y deberes de las personas en materia de salud en la Comunidad foral de Navarra, según los cuales el paciente tiene derecho "a conocer en todo caso quién ha accedido a sus datos sanitarios, el motivo del acceso y el uso que se ha hecho de ellos, salvo en caso del uso codificado de los mismos". En similares términos, el art. 22.2 del Decreto 51/2019, de 21 de junio, por el que se regulan la historia clínica y otra documentación clínica del Principado de Asturias dispone que "el paciente tiene derecho a conocer en todo caso quién ha accedido a sus datos sanitarios y el motivo del acceso".

La Agencia Española de Protección de Datos (AEPD) ha sostenido, en reiteradas ocasiones[22], que el derecho de acceso del paciente a su historia clínica no incluye conocer la identidad de las personas que dentro del ámbito de organización del responsable del fichero han podido tener acceso a la información contenida en el mismo, salvo que en la normativa autonómica aplicable o en otras normas se prevea expresamente dicha posibilidad. El argumento esgrimido para fundar su postura es que los datos de la persona que accede al fichero son datos de carácter personal protegidos bajo el deber de confidencialidad y, por consiguiente, su revelación al paciente supone una "cesión o comunicación de datos" que requiere el consentimiento de su titular.

La postura de la AEPD requiere una atenta reflexión: si la persona que accede indebidamente a la historia clínica pertenece al mismo ámbito de control y gestión del responsable del tratamiento[23], tal vez no estemos ante una cesión de datos personales a los efectos de la normativa aplicable a los mismos. Dicho de otro modo, la regulación de la protección de datos personales, a nuestro juicio, no impide comunicar al paciente la información relativa a la trazabilidad del personal (asistencial, de administración, de inspección, etc.)

[22] Informes jurídicos 165/2005 y 165/2005, 171/2008 y 0003/2021 (en el que analiza, nuevamente, la problemática pero desde la perspectiva del RGPD y la LOPDGDD, reafirmándose en su postura), así como las Resoluciones R/00948/2011, R/00945/2013 y R/02488/2015.

[23] El art. 4.7) del RGPD define "responsable del tratamiento" o "responsable", como "la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros".

que presta servicios o está bajo la dependencia del propio responsable del tratamiento, el cual tiene la obligación de adoptar las medidas técnicas y organizativas necesarias apropiadas para garantizar la seguridad de los datos personales tratados, incluida la protección contra el tratamiento no autorizado o ilícito [arts. 5.1.f) y 24 del RGPD].

Por otra parte, el derecho de acceso es una de las facultades esenciales que integran el derecho fundamental a la protección de datos personales, mediante la cual el titular puede conocer qué datos sobre su persona son objeto de tratamiento. Además, dicha facultad es la base del ejercicio de otras reconocidas legalmente tales como las de rectificación, supresión, limitación, portabilidad u oposición. Conforme a ello, las limitaciones del derecho de acceso deben ser las mínimas, dado que mediante su ejercicio se garantiza la efectividad del derecho fundamental a la protección de datos personales.

A mayor abundamiento, si conforme a lo previsto en el art. 15.1.c)[24] y f) del RGPD, el interesado tiene derecho a conocer los destinatarios a los que se hayan comunicado los datos personales y a formular una denuncia por falta de seguridad del sistema, parece lógico que, si se producen accesos no autorizados, se le informe de ello, si así lo solicita, para poder formular la pertinente denuncia. Ante la negativa de proporcionarle los datos identificativos de los autores de tales consultas indebidas a su historia clínica, lo único que le queda al paciente afectado es solicitar dicha información, como prueba, en el seno de un procedimiento judicial.

Ante ello, el interrogante que nos surge es claro: ¿debe mantenerse, hoy día, una interpretación tan restrictiva del "derecho de acceso a los accesos no autorizados de la historia clínica" del paciente, obligándole a acudir a los tribunales para obtener la información sobre la trazabilidad de aquéllos?

Creemos que no. El paciente debe ver garantizado plenamente su derecho al control de sus datos de salud, conforme al cual tiene un interés legítimo en conocer, de manera nominal, los accesos a su historia clínica que se han producido para comprobar si se ha dado o no cumplimento a las correspondientes previsiones normativas y, en caso de corroborar sus sospechas de accesos indebidos

[24] Según el Considerando 63 del RGPD, "los interesados deben tener derecho a acceder a los datos personales recogidos que le conciernan y a ejercer dicho derecho con facilidad y a intervalos razonables, con el fin de conocer y verificar la licitud del tratamiento. Ello incluye el derecho de los interesados a acceder a datos relativos a la salud, por ejemplo los datos de sus historias clínicas que contengan información como diagnósticos, resultados de exámenes, evaluaciones de facultativos y cualesquiera tratamientos o intervenciones practicadas. Todo interesado debe, por tanto, tener el derecho a conocer y a que se le comuniquen, en particular, los fines para los que se tratan los datos personales, su plazo de tratamiento, sus destinatarios, la lógica implícita en todo tratamiento automático de datos personales y, por lo menos cuando se base en la elaboración de perfiles, las consecuencias de dicho tratamiento".

y constatar eventuales irregularidades en cuanto a las medidas legalmente exigibles al responsable del tratamiento en relación a la gestión de su historia clínica, decidir si presentar una reclamación (art. 77 del RGPD) o interponer una acción judicial para defender sus derechos e intereses. Para ello, resulta imprescindible conocer la identidad de quienes, con fines distintos a los autorizados, acceden a su historia clínica, pues, de lo contrario, además de una innecesaria e indeseada judicialización de este tipo de conflictos, se estarían fomentando tales prácticas ilícitas.

Acerca de la interpretación de la redacción literal del art. 15.1.c) del RGPD se ha pronunciado la reciente Sentencia del Tribunal de Justicia de la Unión Europea (Sala Primera) de 12 de enero de 2023 (C-154/2021: caso RW contra *Österreichische Post*), la cual resuelve la cuestión prejudicial planteada, con arreglo al art. 267 TFUE, por el *Oberster Gerichtshof*, el Tribunal Supremo de lo civil y penal de Austria.

Los antecedentes del litigio principal son los que siguen: el 15 de enero de 2019, RW solicitó a *Österreichische Post AG*, el principal operador austríaco de servicios postales y logísticos, en virtud del art. 15 del RGPD, acceso a los datos personales que le concernían que éste conservaba o había conservado en el pasado, así como, en caso de que los datos se hubieran comunicado a terceros, la identidad de esos destinatarios. En respuesta a dicha solicitud, *Österreichische Post* se limitó a señalar que utilizaba los datos, dentro de los límites legales, en el ejercicio de su actividad como editorial de guías telefónicas y que ofrecía estos datos personales a clientes comerciales con fines de marketing. Asimismo, se remitió a un sitio de Internet que ofrecía más información, también relativa a otros fines del tratamiento de datos. *Österreichische Post* no comunicó a RW la identidad de los destinatarios concretos de los datos.

RW demandó a *Österreichische Post* ante los tribunales austríacos, solicitando que le se ordenase que le facilitase, en particular, la identidad del destinatario o de los destinatarios a los que se habían comunicado sus datos personales. Durante el procedimiento judicial, *Österreichische Post* informó a RW de que sus datos personales habían sido tratados con fines de marketing y transmitidos a clientes, entre los que se encontraban anunciantes del sector de la venta por correspondencia y del comercio físico, empresas informáticas, editores de directorios y asociaciones como organizaciones caritativas, organizaciones no gubernamentales (ONG) o partidos políticos.

Los tribunales de primera instancia y de apelación desestimaron el recurso de RW por considerar que el art. 15, apartado 1º, letra c) del RGPD, en la medida en que se refiere a "los destinatarios o las categorías de destinatarios", concede al responsable del tratamiento la posibilidad de indicar al interesado

únicamente las categorías de destinatarios sin tener que facilitar los nombres de los destinatarios concretos a quienes son transmitidos los datos personales.

RW interpuso recurso de casación ante el *Oberster Gerichtshof*, el cual se pregunta sobre la interpretación del art. 15, apartado 1º, letra c) del RGPD, por cuanto el tenor de dicha disposición no permite saber claramente si concede al responsable del tratamiento la libertad de elegir si comunica la identidad concreta de los destinatarios o sólo las categorías de destinatarios, o si ofrece al interesado el derecho a conocer su identidad concreta.

Dicho órgano jurisdiccional señala que la *ratio legis* de la mencionada disposición aboga a favor de la interpretación según la cual el interesado es quien tiene la opción de solicitar información relativa a las categorías de destinatarios o a los destinatarios concretos de sus datos personales. A su juicio, cualquier interpretación contraria menoscabaría gravemente la efectividad de las vías de recurso de que dispone el interesado para proteger sus datos. En su opinión, si se diera a los responsables la posibilidad de optar entre indicar a los interesados los destinatarios concretos o indicar únicamente las categorías de destinatarios, es de temer que, en la práctica, casi ninguno de ellos facilitaría la información relativa a los destinatarios concretos. Además, en su entender, a diferencia de los arts. 13, apartado 1º, letra e) y 14, apartado 1º, letra e) del RGPD, que obligan al responsable del tratamiento a facilitar la información a que hacen referencia, el art. 15, apartado 1º hace hincapié en el alcance del derecho de acceso del interesado, lo que también parece indicar, según dicho órgano jurisdiccional, que el interesado tiene derecho a elegir entre solicitar información sobre los destinatarios concretos o sobre las categorías de destinatarios. Por último, el Tribunal Supremo austríaco añade que el derecho de acceso establecido en el art. 15, apartado 1º del RGPD no se refiere únicamente a los datos personales tratados en el presente, sino también a todos los datos tratados en el pasado[25].

En estas circunstancias, el *Oberster Gerichtshof* decidió suspender el procedimiento y plantear al Tribunal de Justicia europeo la siguiente cuestión prejudicial: "¿Debe interpretarse el art. 15, apartado 1º, letra c) del RGPD en el sentido de que, en el caso de comunicaciones previstas respecto de las que aún no se hayan determinado los destinatarios concretos, el derecho de acceso se limita a la información sobre las categorías de destinatarios, mientras que, en el caso de que los datos ya hayan sido comunicados, el derecho de acceso debe

[25] A este respecto, señala que las consideraciones expuestas en su Sentencia de 7 de mayo de 2009, Rijkeboer (C-553/07), basadas en la finalidad del derecho de acceso establecido en la Directiva 95/46, pueden transponerse al derecho de acceso contemplado en el art. 15 del RGPD, máxime cuando de los Considerandos 9º y 10º de este Reglamento puede deducirse que el legislador de la Unión no pretendió reducir el nivel de protección en relación con la citada Directiva.

extenderse necesariamente también a la información sobre los destinatarios de esas comunicaciones?".

En su Sentencia, el TJUE realiza las siguientes consideraciones:

Con carácter preliminar, recuerda que, según reiterada jurisprudencia, la interpretación de una disposición del Derecho de la Unión requiere tener en cuenta no sólo su tenor, sino también el contexto en el que se inscribe, así como los objetivos y la finalidad que persigue el acto del que forma parte[26]. Además, cuando pueda ser objeto de varias interpretaciones, deberá darse prioridad a la que permita garantizar su eficacia[27].

En cuanto a la redacción del art. 15, apartado 1, letra c) del RGPD, señala que los términos "destinatarios" y "categorías de destinatarios" se utilizan sucesivamente, sin que sea posible deducir un orden de prioridad entre uno y otro. Dicho tenor no permite determinar, de manera unívoca, si el interesado tiene, en el supuesto de que hayan sido o vayan a ser comunicados datos personales que le conciernen, derecho a ser informado de la identidad concreta de los destinatarios de estos datos.

Por lo que respecta al contexto en el que se inscribe el art. 15, apartado 1, letra c) del RGPD, recuerda que el Considerando 63 del Reglamento establece que el interesado debe tener derecho a conocer y a que se le comunique, en particular, la identidad de los destinatarios de esos datos personales y no precisa que ese derecho pueda limitarse únicamente a las categorías de destinatarios. Asimismo recuerda que, para dar cumplimiento al derecho de acceso, todo tratamiento de datos personales de las personas físicas debe ser conforme con los principios enunciados en el art. 5 del RGPD, entre los cuales figura el de transparencia, que implica, como resulta del Considerando 39, que el interesado de que se trate disponga de información sobre la forma en la que son tratados sus datos personales y que esa información sea fácilmente accesible y comprensible.

Señala que, a diferencia de los arts. 13 y 14 del RGPD, que obligan al responsable del tratamiento a facilitar al interesado la información relativa a las categorías de destinatarios o a los destinatarios concretos de los datos personales que le conciernen, en función de si estos datos se han obtenido o no del interesado, el art. 15 establece un verdadero derecho de acceso en favor del interesado, de modo que éste debe tener la posibilidad de elegir entre obtener información sobre los destinatarios específicos a los que los mencionados datos hayan sido o vayan a ser comunicados, cuando sea posible, y obtener información sobre las categorías de destinatarios.

---

26 Sentencia de 15 de marzo de 2022, Autorité des marchés financiers, C-302/20.

27 Sentencia de 7 de marzo de 2018, Cristal Union, C-31/17.

Recuerda que en una ocasión anterior ha declarado[28] que el ejercicio de este derecho de acceso debe permitir al interesado comprobar no sólo que los datos personales que le conciernen son exactos, sino también que son tratados lícitamente, en concreto, que son comunicados a los destinatarios autorizados[29]. En particular, este derecho de acceso es necesario para permitir al interesado ejercer, en su caso, su derecho de rectificación, su derecho de supresión ("derecho al olvido") y su derecho a la limitación del tratamiento, reconocidos, respectivamente, en los arts. 16, 17 y 18 del RGPD, así como su derecho de oposición al tratamiento de sus datos personales, contemplado en el art. 21 del RGPD, y su derecho a recurrir por los daños sufridos, previsto en los arts. 79 y 82 del RGPD. Así, pues, para garantizar la efectividad de todos sus derechos, el interesado debe tener, en particular, derecho a ser informado de la identidad de los destinatarios concretos cuando sus datos personales ya hayan sido comunicados.

Esta interpretación se ve confirmada por la lectura del art. 19 del RGPD, que establece, en su primera frase, que el responsable del tratamiento comunicará, en principio, a cada uno de los destinatarios a los que se hayan comunicado los datos personales, cualquier rectificación o supresión de datos personales o limitación del tratamiento y, en su segunda frase, que este responsable informará al interesado acerca de dichos destinatarios, si este así lo solicita. De este modo, el art. 19, segunda frase, confiere expresamente al interesado el derecho a ser informado acerca de los destinatarios concretos de los datos que le conciernen por el responsable del tratamiento en el marco de la obligación que éste tiene de informar a todos los destinatarios del ejercicio de los derechos de que ese interesado dispone en virtud de los arts. 16, 17.1 y 18 del RGPD.

Del análisis contextual que precede, el Tribunal concluye que el art. 15, apartado 1º, letra c) del RGPD constituye una de las disposiciones que tienen por objeto garantizar, en favor del interesado, la transparencia de los modos de tratamiento de los datos personales, que le permite ejercer las prerrogativas previstas, en particular, en los arts. 16 a 19, 21, 79 y 82 del RGPD. Por consiguiente, cabe considerar que la información facilitada al interesado en virtud del derecho de acceso establecido en el art. 15, apartado 1º, letra c) del RGPD debe ser la más exacta posible. En particular, este derecho de acceso implica la posibilidad de que el interesado obtenga del responsable del tratamiento la información sobre los destinatarios concretos a los que se comunicaron o serán comunicados los datos o que, alternativamente, opte por limitarse a solicitar información relativa a las categorías de destinatarios.

---

[28] Vid., por analogía, las Sentencias de 17 de julio de 2014, YS y otros, C-141/12 y C-372/12, y de 20 de diciembre de 2017, Nowak, C-434/16.

[29] Vid., por analogía, la Sentencia de 7 de mayo de 2009, Rijkeboer, C-553/07.

Por último, por lo que respecta a la finalidad que persigue el RGPD, el Tribunal europeo señala que tiene por objeto, en particular, tal y como se desprende de su Considerando 10, garantizar un nivel elevado de protección de las personas físicas dentro de la Unión[30], conforme a las exigencias derivadas del derecho fundamental a la protección de los datos personales consagrado en el art. 8 de la Carta de los derechos fundamentales de la Unión Europea. En ello encuentra respaldo el Tribunal encuentra para sostener la interpretación del art. 15, apartado 1º, letra c) que realiza en la sentencia, esto es, que el interesado tiene derecho a obtener del responsable del tratamiento información sobre los destinatarios concretos a los que hayan sido o vayan a ser comunicados los datos personales que le conciernen.

Por último, el Tribunal subraya que, como resulta del Considerando 4 del RGPD, el derecho a la protección de los datos personales no es un derecho absoluto, pues debe considerarse según su función en la sociedad y ponderarse con otros derechos fundamentales, de conformidad con el principio de proporcionalidad[31]. Por tanto, cabe admitir que, en determinadas circunstancias, no sea posible facilitar información sobre destinatarios concretos. En consecuencia, el derecho de acceso podrá limitarse a la información sobre las categorías de destinatarios cuando no sea posible comunicar la identidad de los destinatarios concretos, en particular, cuando estos aún no se conozcan.

Además, recuerda que, en virtud del art. 12, apartado 5º, letra b) del RGPD, el responsable del tratamiento (en el caso de autos, el *Österreichische Post*) puede, de conformidad con el principio de responsabilidad contemplado en el art. 5, apartado 2º, y en su Considerando 74, negarse a actuar respecto de las solicitudes del interesado cuando éstas sean manifiestamente infundadas o excesivas, si bien soporta la carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud.

En conclusión, el TJUE, respondiendo a la cuestión prejudicial planteada, señala que el art. 15, apartado 1º, letra c) del RGPD "debe interpretarse en el sentido de que el derecho de acceso del interesado a los datos personales que le conciernen, establecido en dicha disposición, implica, cuando esos datos hayan sido o vayan a ser comunicados a destinatarios, la obligación del responsable del tratamiento de facilitar a ese interesado la identidad de esos destinatarios, a menos que no sea posible identificarlos o que dicho responsable del tratamiento demuestre que las solicitudes de acceso del interesado son manifiestamente infundadas o excesivas en el sentido del art. 12, apartado 5º del RGPD, en cuyo caso éste podrá indicar al interesado únicamente las categorías de destinatarios de que se trate".

---

30 Vid. Sentencia de 6 de octubre de 2020, La Quadrature du Net y otros, C-511/18, C-512/18 y C-520/18.

31 Vid. Sentencia de 16 de julio de 2020, Facebook Ireland y Schrems, C-311/18.

Así las cosas, conforme al espíritu tuitivo y garantista del RGPD y, en particular, a los principios que recoge en su art. 5[32] y, en concreto, al de transparencia, el paciente tiene derecho a conocer la identificación del usuario que ha accedido a su historia clínica. Sólo así puede generarse confianza en los ciudadanos en las nuevas tecnologías y en que sus datos personales y, en especial, los relativos a su salud, están a buen recaudo. En la *e-Health*, cuantos más datos sobre nuestra salud, mayor control de los mismos por el paciente y mayor responsabilidad por parte del responsable de su tratamiento.

La pregunta, entonces, es: ¿qué datos personales del autor de la consulta han de facilitársele? En cumplimiento del principio de minimización de datos *ex* art. 5.1.c) del RGPD, creemos que la información a proporcionar al paciente debe limitarse a los datos estrictamente necesarios para alcanzar la finalidad pretendida (conocer las personas que han consultado su historia clínica), esto es, identidad, cargo o categoría profesional, fecha y hora del acceso, lugar y motivo. Otros datos personales como el número del Documento Nacional de Identidad, el domicilio o el teléfono no son, a nuestro juicio, pertinentes.

Proporcionar al paciente los datos identificativos de quienes han accedido indebidamente a su historia clínica encuentra amparo normativo, siempre que se trate de un centro sanitario público o privado proveedor de servicios públicos, en la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno[33]. Conforme a su art. 15 y a la ponderación razonada entre el derecho de acceso del solicitante y el derecho a la protección de datos de las personas afectadas en él prevista[34], merece mayor tutela el derecho de la persona reclamante a conocer la identidad de las que han accedido a su historia clínica y, así, poder saber si se han producido accesos inadecuados o improcedentes a sus datos de salud, que el derecho de quienes han accedido a la historia clínica de la persona reclamante a proteger su identidad, ya que en este caso el perjuicio que puede causarles el acceso solicitado se proyecta únicamente en el seguimiento de su actividad profesional[35].

---

[32] Vid. Considerando 39 del RGPD.

[33] A ello apunta la Agencia Catalana de Protección de Datos en sus Resoluciones núm. PT 140/2021, PT 141/2021 y PT 9/2022, así como, entre otros, en su Dictamen 48/2021.

[34] Antes de realizarla habría que cumplir con el trámite de audiencia previsto por el art. 19.3 de la Ley 19/2013, según el cual "si la información solicitada pudiera afectar a derechos o intereses de terceros, debidamente identificados, se les concederá un plazo de quince días para que puedan realizar las alegaciones que estimen oportunas. El solicitante deberá ser informado de esta circunstancia, así como de la suspensión del plazo para dictar resolución hasta que se hayan recibido las alegaciones o haya transcurrido el plazo para su presentación".

Es preciso señalar que en el caso de que los afectados manifiesten su oposición, ésta no tiene carácter vinculante para la Administración a la hora de resolver la solicitud.

[35] En este sentido se pronuncia la Comisión de Garantía del Derecho de Acceso a la Información Pública de la Generalitat de Catalunya (GAIP) en su Resolución 0265/2022, de 31 de

Es cierto que el personal del centro sanitario ha de tener garantizada su privacidad en el desarrollo de las tareas y funciones que tiene asignadas en relación con la prestación de asistencia sanitaria al paciente, pero no cuando utiliza los recursos y herramientas del centro para finalidades distintas o bien para acceder a información de otros usuarios (familiares del paciente, compañeros de trabajo, su propio cónyuge o pareja de hecho, etc.). En tales casos no parece que pueda invocarse el derecho a la confidencialidad de los datos personales de los autores de los accesos indebidos para justificar que al paciente se le impida conocer la identidad de aquéllos. El contrapeso de la balanza, a nuestro entender, se inclina hacia el lado del paciente.

En último lugar, nos resulta importante destacar que quien debe examinar y concluir si los accesos a su información personal clínica son debidos o indebidos es el paciente, es decir, al centro sanitario no le incumbe realizar una valoración previa de los accesos producidos a la historia clínica del paciente que reclama la información, determinar qué accesos considera debidos y cuáles podrían ser indebidos y, en su caso, indicar al paciente que no se han detectado accesos indebidos. Ésta es la postura mantenida por la Autoridad Catalana de Protección de Datos[36], la cual compartimos.

marzo (la cual ha sido impugnada ante el TSJC), que declara el derecho de la persona reclamante a acceder a los datos de carácter personal que hay en su historia clínica, incluida la información sobre el origen de los datos, cesionarios y personas que la han consultado, usos y finalidades para las cuales se almacenaron en un determinado periodo de tiempo.

[36] Vid. Dictámenes CNS 48/2021 y 10/2022.