REVISTA CHILENA
DE DERECHO Y TECNOLOGÍA

VOL. 12 (2023) • e71020 • DOI 10.5354/0719-2584.2023.71020
RECIBIDO: 13/6/2023 • APROBADO: 21/11/2023 • PUBLICADO: 31/12/2023

DOCTRINA

El derecho de acceso a los datos relativos a la salud después del fallecimiento del titular

The right of access to health data after the death of the data subject

Idoia Landa Reza
Universidad del País Vasco, España

RESUMEN El ejercicio del derecho de acceso a los datos relativos a la salud tras el fallecimiento del titular plantea incertidumbres. Se debe realizar una diferenciación entre el acceso a los datos personales del fallecido, y el acceso *postmortem* de cualquier contenido en formato digital de la persona fallecida. De la misma manera, es necesario identificar un instrumento jurídico adecuado ya existente que permita reflejar la voluntad del futuro ejercicio del derecho de acceso del interesado, ya que la normativa de protección de datos personales no lo incluye.

PALABRAS CLAVE Datos relativos a la salud, derecho de acceso, interesado, ejercicio, fallecido.

ABSTRACT The exercise of the right of access to health data after the death of the data subject raises uncertainties. A differentiation must be made between access to the deceased's personal data, and *postmortem* access to any content in digital format of the deceased person. In the same way, it is necessary to identify an appropriate legal instrument already in place to reflect the will of the future exercise of the data subject's right of access, as the personal data protection regulations do not include it.

KEYWORD Health data, right of access, data subject, exercise, deceased.

Introducción

Con el fin de hacer frente a los problemas que han surgido con los avances tecnológicos que se han producido en los últimos años, el legislador europeo ha creado nuevas herramientas para que los titulares puedan ejercer su derecho a la protección de datos personales relacionados con tratamientos realizados por terceros. Tras la entrada en vigor del Reglamento general de protección de datos (RGPD),[1] los derechos del interesado descritos en los artículos 15 y 21 de este reglamento se transformaron y pasaron de llamarse derechos ARCO (acceso, rectificación, cancelación y oposición) a derechos ARSLPO (acceso, rectificación, supresión, olvido, limitación del tratamiento, portabilidad y oposición).

El objetivo de este reforzamiento de los derechos es adaptarlos a la era digital. A su vez, con la entrada en vigor del citado reglamento, desapareció la cancelación y se sustituyó por el derecho de supresión o derecho al olvido. En el artículo 22 del RGPD, bajo el título «decisiones individuales automatizadas, incluida la elaboración de perfiles», se regula el derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles o *profiling* (tratamiento automatizado de datos personales que consiste en utilizarlos para evaluar ciertos aspectos del interesado y analizar o predecir sus intereses, comportamientos y otros atributos), que produzca efectos jurídicos en el interesado o le afecte significativamente de modo similar. No queda claro si se trata realmente de un derecho del interesado o de una prohibición que introduce la normativa para el responsable del tratamiento de datos. Es por ello que no queda plasmado entre los derechos ARSLPO.

La aplicación de los derechos del interesado sigue planteando dificultades debido a la escueta y poco ilustrativa redacción del RGPD. La normativa es general y no contempla cómo han de ser interpretados los derechos en ámbitos tan específicos como el sanitario. La problemática aumenta cuando se habla de la política de protección de datos de un documento sanitario o de la página oficial de un centro de salud porque dichas secciones suelen estar limitadas a reproducir lo dispuesto en el RGPD sin adecuarlo al sector sanitario lo que plantea problemas interpretativos que pueden perjudicar al interesado.

De cara al ejercicio *post mortem* de los derechos del interesado hay que diferenciar el contenido de los artículos 3 y 96 de la Ley Orgánica de Protección de Datos Personales (LOPDGDD)[2] que regulan el acceso a los datos personales del difunto y el ac-

1. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Disponible en https://bit.ly/4alztFB.

2. Ley Orgánica 3/2018, del 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Boletín Oficial del Estado 294, de 6 de diciembre de 2018. Disponible en https://bit.ly/41kSowl.

ceso póstumo a cualquier contenido del fallecido en formato digital respectivamente. Finalmente, es necesario identificar un instrumento jurídico que permita al interesado reflejar adecuadamente dicha voluntad para que en el futuro se respete su deseo.

¿Cómo interpretar los derechos del interesado en el ámbito sanitario?

El apartado de protección de datos de documentos sanitarios reproduce lo dispuesto en el RGPD sin adecuarlo al ámbito sanitario lo que crea problemas interpretativos. Existen siete derechos en materia de protección de datos personales: de acceso, rectificación, supresión, olvido, limitación del tratamiento, portabilidad y oposición. Aunque la interpretación relativa a esos derechos del ámbito sanitario es necesaria, nos centraremos en el derecho de acceso por tratarse de la base o «llave» que posibilita el ejercicio de los otros derechos, es difícil ejercer cualquier otro si no sabemos que se están tratando o manejando nuestros datos de salud.

Según el artículo 15 del RGPD el interesado tiene derecho a obtener confirmación del responsable del tratamiento de si se están tratando o no datos personales que le conciernen.[3] De ser así podrá solicitar el acceso a los datos personales y a una serie de informaciones adicionales como los fines del tratamiento, las categorías de datos personales de que se trate y los destinatarios o categorías de destinatarios a los que se comunican los datos personales.

El derecho de acceso es reconocido, además, en el artículo 8.2 de la Carta de los Derechos Fundamentales de la Unión Europea y, en el ámbito sanitario específicamente, en el artículo 18.1 de la Ley 41/2002, comúnmente conocida como Ley Básica reguladora de la Autonomía del Paciente (LBAP),[4] y en el artículo 12.1 del Decreto 38 sobre historia clínica del País Vasco.[5] El derecho de acceso permite al interesado saber si alguien maneja sus datos personales, para qué fines y cómo los trata, lo que facilita el ejercicio de los otros derechos reconocidos al interesado (rectificación, supresión y olvido, limitación del tratamiento, portabilidad y oposición). Por lo tanto, el derecho de acceso se constituye como instrumento necesario para ejercer el resto de los derechos del grupo ARSLPO y así lo ha reconocido también el Tribunal de Justicia de la Unión Europea.[6]

3. Sentencia del Tribunal de Justicia de la Unión Europea del 10 de diciembre de 2010, asunto C-620/19.

4. Ley 41/2002, del 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica. Boletín Oficial del Estado 274 del 15 de noviembre de 2022. Disponible en https://bit.ly/3v6ljIi.

5. Decreto 38 del 13 de marzo de 2012, sobre historia clínica y derechos y obligaciones de pacientes y profesionales de la salud en materia de documentación clínica. Disponible en https://bit.ly/47YKyec.

6. Sentencia del 7 de mayo de 2009, asunto C-553/07.

Según la Ley Orgánica de Protección de Datos Personales[7] se reconoce, en el ámbito sanitario, el derecho de los interesados a acceder a los datos relativos a la salud. Este derecho entrega al usuario la facultad de conocer en un momento determinado el contenido de su historia clínica y de documentos que contengan sus datos personales (De Lorenzo Montero, 2003: 26). Bajo la rúbrica de «usos de la historia clínica», la Ley 41/2002 regula las diferentes finalidades o destinos de la documentación sanitaria y determina qué persona, en cumplimiento de cada una de esas finalidades, puede acceder a la historia clínica. El artículo 18 de esta ley regula el derecho de acceso utilizando el término «uso» como sinónimo de finalidad, utilidad u objetivo, y el término «acceso» en el sentido de conocer, de obtener información (Sáiz Ramos y Larios Risco, 2009). Sin embargo, la normativa no recoge un procedimiento específico para dicho acceso y le corresponde a los centros sanitarios la creación del procedimiento.[8] La ley establece en su artículo 15.2 que el interesado debe tener acceso a todo su historial clínico y debe obtener copia de los datos que contiene[9] en el plazo máximo de un mes.[10] Si los datos son inexactos o no están completos, el interesado puede utilizar su derecho de rectificación que se regula en los artículos 16 del RGPD y 14 de la LOPDGDD, y que refiere al derecho a solicitar al responsable que rectifique sus datos personales cuando estos sean inexactos o estén incompletos (respecto al o los objetivos del tratamiento de los datos). La LBAP no habla expresamente del derecho de rectificación, aunque en el artículo 15 se establece que la historia clínica incorporará la información que se considere trascendental para el conocimiento veraz y actualizado del estado de salud del paciente. En este sentido, si los datos que se encuentran en el historial clínico son incorrectos o inexactos el profesional sanitario no tendrá un conocimiento veraz y actualizado del estado de salud de su paciente como requiere la norma. El empleo de datos erróneos por parte de los profesionales sanitarios puede acarrear riesgos para la salud de los pacientes, puesto que se tomarían decisiones sobre la base de información no verídica.

7. Considerando 63 de la Ley Orgánica 3/2018, del 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Disponible en https://bit.ly/41kSowl.

8. Artículo 18.1 de la Ley 41/2002.

9. Sobre este tema véanse: resolución de la Agencia Española de Protección de Datos (AEPD) R/01773/2018 del 8 de enero de 2019, procedimiento TD/01234/2018; resolución de la AEPD R/01620/2018 del 5 de octubre de 2018, procedimiento TD/01026/2018; y resolución de la AEPD R/01463/2018 del 27 de agosto de 2018, procedimiento TD/01032/2018.

10. La resolución de la AEPD R/01583/2018 del 20 de septiembre de 2018, procedimiento TD/00946/2018, pone de manifiesto la importancia de cumplir con el plazo estipulado: «transcurrido el plazo establecido conforme a las normas antes señaladas, su solicitud no obtuvo la respuesta legalmente exigible».

Así, el paciente que compruebe que la información contenida en su historial clínico no es correcta o está incompleta tendrá el derecho de solicitar la rectificación[11] y corresponderá al profesional sanitario determinar si se debe o no rectificar el dato. A pesar de la importancia del derecho de rectificación en el ámbito de la salud, se pueden crear situaciones problemáticas como consecuencia de su ejercicio, por ejemplo, cuando los datos del historial clínico fueron ciertos en el pasado, pero no lo son en la actualidad. En ese caso se deberá analizar si la rectificación perjudicará la asistencia sanitaria del mismo interesado o de terceras personas para decidir si se realiza la rectificación.

Ahora, los siguientes dos derechos, el de supresión y al olvido, se aplican en ámbitos distintos. Al introducir entre paréntesis el derecho al olvido dentro del título del artículo 17 del RGPD, pareciera que se trata de una denominación común del derecho a la supresión. Sin embargo, las diferencias entre ambos son sustanciales.

El derecho de supresión es la versión renovada del antiguo derecho de cancelación. Al ejercer este derecho se obliga al responsable a que cese el tratamiento de los datos personales y los elimine. En el ámbito sanitario los pacientes tienen derecho a solicitar el borrado de sus datos de salud. No obstante, se limita el derecho a la supresión de datos de la historia clínica por motivos de asistencia o tratamiento sanitario, o por interés público ya que el médico y personal clínico no podrían atender adecuadamente al paciente si parte de su historial clínico puede ser borrado por solicitud de este. En este sentido, la normativa establece un plazo mínimo de conservación. El artículo 19.1 del Decreto 38/2012, al igual que el artículo 17.1 de la LBAP, obliga a los centros sanitarios a conservar la documentación clínica de los pacientes por un plazo mínimo de cinco años desde la fecha del alta de cada proceso asistencial.

El derecho al olvido es el ejercicio de los derechos de cancelación y oposición aplicados a los buscadores de Internet[12] y busca impedir la publicación de información personal en la red cuando no se cumplen los requisitos de adecuación y pertinencia previstos en la normativa. Incluye el derecho a limitar la difusión universal e indiscriminada de datos personales en los buscadores generales cuando la información es obsoleta o ya no tiene relevancia ni interés público, aunque la publicación original sea legítima (en el caso de boletines oficiales o informaciones amparadas por las libertades de expresión o de información).

11. Resoluciones de la AEPD: R/01422/2018 del 8 de octubre de 2018, procedimiento TD/01051/2018; R/00847/2018 del 18 de mayo de 2018, procedimiento TD/00297/2018; R/00858/2018 del 18 de mayo de 2018, procedimiento TD/00296/2018; y R/01455/2018 del 27 de agosto de 2017, procedimiento TD/00917/2018.

12. Sentencia del Tribunal de Justicia de la Unión Europea, Gran Sala, del 24 de septiembre de 2019. Asunto C136/17.

Cuando el paciente quiera borrar sus datos personales se ejercerá, como norma general, el derecho de supresión y no el derecho al olvido porque los datos de salud de los pacientes no se encuentran a disposición de los ciudadanos en Internet. No obstante, se pueden crear situaciones en las que el paciente podrá ejercer el derecho al olvido en este ámbito, un ejemplo es la solicitud de eliminar las imágenes del «antes y después». Es decir, si un paciente con acné autoriza la publicación de sus fotografías antes y después del tratamiento recibido en una clínica dermatológica y luego cambia de opinión respecto a la publicación de dichas imágenes, puede solicitar que se eliminen del sitio web. Según la definición del artículo 4.1 del RGPD estas imágenes serían datos personales porque muestran la cara del paciente y permiten establecer su identidad. De la misma manera, indican que la persona padece, o padecía, una enfermedad cutánea, es decir, un dato sobre la salud que pertenece a la categoría especial de datos personales.

Gracias al derecho a la limitación del manejo de datos regulado en el artículo 18 del RGPD el interesado podrá solicitar al responsable la limitación temporal del manejo de sus datos personales. Para eso se solicita que el responsable aplique medidas sobre algunos datos personales para evitar su modificación o, en su caso, su borrado o supresión, otorgando al interesado mayor control sobre sus datos personales.

Cuando exista un conflicto entre un paciente y un centro sanitario el paciente podrá ejercer el derecho a limitar el manejo de datos, esto significa que podrá solicitar que su información personal no sea utilizada mientras el centro decide sobre la exactitud de los datos: cuando el paciente desea que los datos se conserven, incluso si el tratamiento puede ser ilícito o innecesario; cuando el responsable del tratamiento ya no necesita los datos, pero el paciente los necesita para llevar a cabo reclamaciones o defenderse de ellas; y mientras el centro decide si el derecho de oposición es aplicable (APDCAT, 2022: 19).

El artículo 20 del RGPD agregó el derecho a la portabilidad de datos. Gracias a esto el interesado puede recibir en un formato estructurado, de uso común y lectura mecánica, los datos que proporcionó al responsable y transmitirlos a otro sin impedimentos. Se trata de una experiencia sin fronteras donde las personas pueden moverse fácilmente entre servicios de red, reutilizar los datos que proporcionan mientras controlan su privacidad y respetan la privacidad de los demás (Van Der Auwermeulen, 2017: 18). Este derecho se puede definir como la facultad que tiene el interesado de exigir que el responsable del tratamiento le devuelva sus datos personales. Tras dicha «devolución» el interesado tendrá la opción de transmitir los mismos a otro responsable. También se permite la transmisión directa en que los datos personales se envían del primer responsable al segundo sin pasar por las manos del interesado.

El derecho a la portabilidad es muy importante para el paciente porque le permite acudir a otro centro sanitario. Si bien este derecho no puede ser ejercido en la salud pública, porque la atención sanitaria prestada por los centros y servicios de la red de

salud pública no se basa en el consentimiento de los pacientes o en la ejecución de un contrato, sí se puede solicitar a los responsables (mutuas privadas, médicos en ejercicio privado, etcétera) que tratan los datos de forma automatizada y de acuerdo con una decisión previa del paciente que contrató la prestación. Si la clínica privada está obligada a conservar los datos en el plazo estipulado por la LBAP los suprimirá cuando se cumpla el plazo. Esto no implica la supresión automática de los datos en los sistemas informáticos del antiguo responsable. Como no es únicamente aplicable a nivel estatal, se identifica como una ventaja para la actual sociedad globalizada.

El derecho de oposición[13] permite al interesado oponerse en cualquier momento, por motivos relacionados con su situación particular, al tratamiento de sus datos personales cuando: a) se basa en el cumplimiento de una misión de interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, pero también si el tratamiento es necesario para la satisfacción de intereses legítimos del responsable o de un tercero; b) los datos personales son tratados con fines de mercadotecnia directa (cualquier acción, como el envío de correos electrónicos, que realice una empresa para enviar publicidad a particulares);[14] o c) cuando el tratamiento de datos personales tenga fines de investigación científica o histórica o fines estadísticos. En palabras del Tribunal Constitucional «es la facultad de exigir a quien corresponda que ponga fin a la posesión y al uso de los datos personales».[15]

Si el centro sanitario demuestra que hay razones legítimas imperiosas que deben prevalecer, por ejemplo, si pone en peligro la asistencia sanitaria que recibe el paciente o el buen funcionamiento del sistema de salud, este derecho podrá ser limitado (APDCAT, 2022: 16). El ejercicio de este derecho no implica necesariamente la supresión de los datos, dado que el centro puede tener la obligación de conservar la información durante un periodo determinado.

13. Artículo 21 del Reglamento General de Protección de Datos y 18 de la Ley Orgánica de Protección de Datos (LOPDGDD).

14. La Agencia Española de Protección de Datos (AEPD) sobre la base de RGPD y al artículo 21 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI), resolvió en su Informe jurídico 2018-0173 del 11 de diciembre de 2018 que no se podrá enviar publicidad mediante correo electrónico si el interesado no ha otorgado el consentimiento o si no existe una relación contractual previa. En cuanto a la comunicación postal o telefónica la AEPD, en su informe jurídico 2018-0164 del 11 de diciembre de 2018, indicó que la LSSI no será de aplicación y se podrán enviar comunicaciones comerciales sin necesidad de recabar el consentimiento, con base al interés legítimo del responsable y siempre que la publicidad se refiera a productos o servicios similares contratados por el cliente.

15. Sentencia del Tribunal Constitucional 290/2000 del 30 de noviembre de 2000.

El ejercicio post mortem del derecho de acceso en el ámbito sanitario

La normativa de protección de datos no se aplica al manejo de datos personales de personas fallecidas.[16] Esta exclusión se basa en el artículo 32 del Código Civil que establece que el fallecimiento de una persona determina la extinción de su personalidad civil. Sin perjuicio de que el RGPD establezca que la normativa de protección de datos no se aplique al manejo de datos personales de personas fallecidas, los Estados miembros son competentes para establecer normas relativas al tratamiento de esos datos personales. Por ende, el legislador europeo ha renunciado a armonizar la regulación sobre el tratamiento de los datos de las personas fallecidas. Una de las razones de dicha elección puede ser la gran diversidad de normas de derecho sucesorio que coexisten en los Estados miembros y su gran arraigo con la tradición jurídica nacional (Díaz Alabart, 2021).

En lo que respecta a la normativa española, el artículo 2.2 de la Ley Orgánica 3/2018 dice que esta ley no es aplicable a los tratamientos de datos de personas fallecidas. No obstante, la LOPDGDD regula el acceso a los datos personales y los contenidos del fallecido gestionados por prestadores de servicios de la sociedad de la información en los artículos 3 y 96 respectivamente. El artículo 3 regula el acceso a los datos personales del fallecido y el artículo 96 se refiere al acceso *post mortem* de cualquier contenido en formato digital de la persona fallecida. Al tratarse de accesos tan distintos, es necesaria una labor interpretativa para comprender el alcance de cada artículo.

En el artículo 3 se recoge que las personas vinculadas a la persona fallecida por razones familiares o de hecho, así como sus herederos, podrán dirigirse al responsable o encargado para solicitar el acceso a los datos personales y, en su caso, su rectificación o supresión siempre que la persona fallecida no lo hubiese prohibido expresamente o así lo establezca una ley. En consecuencia, esta normativa parte de la regla de acceso y solo se prohíbe por la negativa del fallecido o cuando lo establezca la ley. Como crítica se podría afirmar que legitimar, salvo la prohibición expresa del fallecido o de una ley, a las personas que tengan un vínculo con la persona fallecida (por razones familiares o de hecho) es excesivo. Tampoco se determina cuál es el grado de parentesco que se debe cumplir, si las razones de hecho solo se refieren a las parejas de hecho o si deben estar registradas.

Según lo establece el artículo 3.3 las personas o instituciones que el fallecido hubiese designado expresamente para eso también podrán solicitar, de acuerdo a las instrucciones recibidas, el acceso a los datos personales, su rectificación o supresión. En el caso del fallecimiento de personas con discapacidad, *estas facultades también* se podrán ejercer por quienes hayan sido designados para el ejercicio de funciones

16. Considerando 27, 158 y 160 del RGPD y artículo 2.b) de la LOPDGDD.

de apoyo, si tales facultades se entendieran comprendidas en las medidas de apoyo prestadas por el designado. Este apartado es realmente curioso, habla de medidas de apoyo y al momento de su redacción quedaban tres años para la entrada en vigor de la Ley 8/2021.

En el caso de que se hayan establecido medidas de apoyo voluntarias que recojan la actuación del prestador de apoyo en el área de protección de datos personales, tras el fallecimiento del interesado el prestador de apoyo podrá ejercer estas facultades. Respecto a las medidas judiciales, la persona que otorgaba el apoyo podrá ejercer los derechos del interesado siempre que en las medidas de apoyo judiciales se comprendan estas facultades. El problema interpretativo surge cuando la medida de apoyo es informal, sin embargo, como el guardador de hecho generalmente es un familiar del interesado el caso podría entrar dentro del apartado 1 del artículo 3 de la LOPDGDD, «las personas vinculadas al fallecido por razones familiares o de hecho».

Según el artículo 12.5 del RGPD cuando las leyes aplicables a determinados tratamientos establezcan un régimen especial que afecte al ejercicio de los derechos, se realizará lo que ellas disponen. En el caso del ámbito sanitario, el artículo 18.4 de la Ley Básica de Autonomía del Paciente (LBAP) establece que los centros sanitarios y facultativos de ejercicio individual solo facilitarán el acceso a la historia clínica del paciente fallecido a las personas vinculadas por razones familiares o de hecho, salvo que el fallecido lo hubiese prohibido expresamente y así se acredite. Esta prohibición puede constar en el historial clínico del paciente o en el documento de voluntades anticipadas (Craviotto Valle, 2023). 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 la intimidad del fallecido ni las anotaciones subjetivas de los profesionales, ni que perjudique a terceros.[17]

El artículo 14.3 del Decreto 38/2012 establece que se podrá producir el acceso a la documentación[18] de la historia clínica de las personas fallecidas por terceras personas que acrediten su vinculación por razones familiares o de hecho,[19] siempre que se justifiquen motivos por un riesgo para la propia salud de la persona solicitante y salvo que la persona fallecida lo hubiese prohibido expresamente y así se acredite. Este acceso se limitará a los datos pertinentes y no se facilitará información que afecte a la intimidad de la persona fallecida, o las anotaciones subjetivas de los profesionales

17. Resolución de la Agencia Española de Protección de Datos (AEPD) R01237/2018 del 5 de julio de 2018 y dictamen de la Autoridad Catalana de Protección de Datos (APDCAT) CNS 8/2019 del 18 de febrero de 2019.

18. 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 (Boletín Oficial del País Vasco 65 del 29 de marzo de 2012). Disponible en https://bit.ly/47YKyec.

19. Agencia Vasca de Protección de Datos. Dictamen D09-051 del 26 de octubre de 2009.

que intervinieron, o información que perjudique a terceras personas. La legitimación automática que otorgan la LBAP y el Decreto 38/2012 a los familiares del fallecido se podría considerar excesiva y sería más adecuado que las bases legitimadoras fuesen la justificación de un interés propio o la designación expresa del fallecido.

La duda surge al determinar el grado que deben tener los familiares que podrán solicitar el acceso o la rectificación y supresión de los datos de salud del historial clínico del fallecido, puesto que ni la LBAP ni el Decreto 38/2012 definen el grado de parentesco, tampoco precisan si las parejas de hecho deben estar inscritas en el registro de parejas o si es suficiente con acreditar la convivencia. En este sentido, se considerarán familiares los cónyuges, hijos, padres y hermanos, y la relación de hecho deberá estar acreditada en el correspondiente registro o con la inscripción en el padrón municipal. Respecto de los terceros, son aquellas personas que no están vinculadas al paciente por razones familiares o de hecho, y solo pueden acceder a la historia clínica cuando exista un grave riesgo para su salud y solo tendrán acceso a los datos pertinentes (Troncoso Reigada, 2010).

La Agencia Española de Protección de Datos (AEPD) en su Informe 171/2008 del 4 de agosto de 2008 indica que el ejercicio del derecho de acceso a la historia clínica del fallecido corresponde a su cónyuge o persona vinculada por una relación de hecho similar, a los ascendientes y a los descendientes. Los hermanos no se mencionan en el informe, pero se podría indicar que este vacío es un mero error, un olvido de la AEPD, puesto que el texto se basa en el artículo 4 de la Ley Orgánica 1/1982 que sí que los contempla entre los legitimados.[20]

La redacción confusa del artículo 14.3 del Decreto 38/2012 puede crear problemas interpretativos, y es que de la lectura de la frase «terceras personas que acrediten su vinculación con aquéllas por razones familiares o de hecho», se puede deducir que las terceras personas serán aquellas que tengan una relación familiar o de hecho directa con el fallecido. El citado artículo indica que este acceso se permitirá «siempre que se justifiquen motivos por un riesgo para la propia salud de la persona solicitante». Entonces, se podría comprender que la normativa solo permite el acceso a la historia clínica del fallecido a terceras personas que acrediten su relación familiar o de hecho con el difunto y justifiquen un motivo de riesgo para su salud, debiendo cumplirse las dos condiciones.

Sin perjuicio de lo anterior, la Agencia Vasca de Protección de Datos (AVPD) en su dictamen D19-008 del 30 de mayo de 2019 concluyó que estarán legitimados para acceder a la historia clínica del fallecido, salvo oposición expresa del mismo debidamente acreditado, su cónyuge o pareja de hecho, ascendientes, descendientes

20. Ley Orgánica 1/1982, del 5 de mayo reguladora de la protección civil de los derechos fundamentales al honor, a la intimidad personal y familiar y a la propia imagen. Boletín Oficial del Estado 115 del 14 de mayo de 1982. Disponible en https://bit.ly/477sFcc.

y hermanos. Se considerarán terceros a quienes no demuestren ese parentesco o el vínculo de hecho, y al igual que los familiares afectados por la oposición expresa del fallecido, únicamente accederán a la historia clínica cuando exista un riesgo para su salud, y exclusivamente a los datos clínicos necesarios para proteger ese bien jurídico, salvo que fuesen designados en el testamento para el ejercicio de las acciones de la Ley Orgánica 1/1982 o herederos.

Según la interpretación de la AVPD, las personas que acrediten una relación familiar o de hecho del difunto estarán siempre legitimadas para acceder a la historia clínica del fallecido salvo que este lo hubiese prohibido, y al igual que ocurre con las terceras personas, solo podrán acceder a la historia clínica de la persona fallecida si existe un riesgo para su propia salud, debiendo delimitarse el acceso a los datos clínicos necesarios. En la recomendación que la Defensoría del pueblo del País Vasco realizó al servicio vasco de salud (Osakidetza) se recoge que las peticiones de acceso de familiares de personas fallecidas se deben resolver previa comprobación de su condición de familiares y de la inexistencia de una prohibición expresa de la persona fallecida para el acceso, y que la falta de acreditación de justificación de un riesgo para la propia salud de la persona solicitante no puede ser interpretada como causa de denegación en estos procedimientos de acceso.[21]

Por su parte, el artículo 96 de la LOPDGDD, a diferencia del analizado artículo 3 del mismo cuerpo legal, regula el acceso a contenidos gestionados por prestadores de servicios de la sociedad de la información sobre personas fallecidas. Por el uso de las palabras «testamento» y «digital» se podría llegar a entender erróneamente que el legislador se refiere al formato utilizado para realizar el acto jurídico, siendo necesario diferenciarlo del testamento online. En el testamento digital se recoge la voluntad de una persona sobre su contenido digital para el caso de su fallecimiento, y el testamento online es el que se realiza en línea, formato que no se contempla expresamente en el Código Civil español aunque existan empresas que lo ofrecen (Llopis Benlloch, 2016).

El artículo 96 se refiere a la gestión de los contenidos digitales tras el fallecimiento del interesado (Martínez Martínez, 2019: 178-207). Estos contenidos digitales no solo son bienes en su sentido clásico, la huella que deja la actividad del interesado en la red puede tener carácter patrimonial y no patrimonial. Pese a que no existe una descripción en la normativa, el término contenido digital se puede utilizar para describir sitios web, dominios, criptomonedas, cuentas electrónicas (banca online o servicios de pago), cuentas de correo electrónico o cuentas de redes sociales (Connor, 2010: 548). Si bien las cuentas están catalogadas dentro de la definición de contenido digital, en realidad son relaciones obligatorias de naturaleza contractual en cuya virtud un prestador de servicios de internet ofrece al usuario determinados servicios digita-

21. Recomendación General 9/2013 del 5 de noviembre de 2013.

les. Puede que exista una intransmisibilidad establecida en el contrato celebrado por el usuario y el prestador de servicios cuando no haya derecho de propiedad sino una licencia de uso sobre el bien, por ejemplo, música, videos o libros digitales (Santos Morón, 2018: 416-422).

En cuanto a los archivos la norma habla de contenidos digitales gestionados por prestadores de servicios de la sociedad de la información, por lo que se entiende que los archivos deben de estar en la nube y no en un soporte físico como el disco duro del ordenador o en un *pendrive* (Moralejo Imbernón, 2020: 255). El mundo digital está en constante evolución y no es fácil identificar cuándo estamos realmente ante un activo digital (Toygar, Taipe y Zhu, 2013: 118), y puede que por esa razón el legislador estatal ha preferido no realizar un listado de dichos contenidos digitales en la normativa, aunque esta opción pueda crear problemas interpretativos en el futuro.

Tienen legitimación para acceder a contenidos digitales de la persona fallecida las personas vinculadas por razones familiares o de hecho y sus herederos; el albacea testamentario así como aquella persona o institución a la que el fallecido hubiese designado expresamente para ello; en el caso de los menores sus representantes legales o, en el marco de sus competencias, el Ministerio Fiscal; y, en el caso de que el fallecido fuese una persona con discapacidad, el designado para el ejercicio de funciones de apoyo si tales facultades se entendieran comprendidas en las medidas de apoyo que prestase.

Ante esta realidad se ha manifestado que la amplia legitimación que otorga la normativa por defecto es inadecuada, y sería preferible que la legitimación para ejercer esas facultades provenga del difunto (Cámara Lapuente, 2019: 421-422). Siguiendo esta línea, se afirma que permitir la intervención concurrente de tantas personas legitimadas *ex lege* e identificadas de manera tan imprecisa e indeterminada, basta solo un vínculo con el fallecido por razones familiares o de hecho salvo prohibición expresa, y con facultades tan amplias resulta excesivo. Por eso, sería preferible la regla del no acceso salvo que se haya manifestado lo contrario (Ginebra Molins, 2020: 233-234).

El caso francés y catalán

En el derecho foráneo podemos citar el caso de la legislación francesa. El artículo 40.1 de la Ley 78-17[22] recoge que los derechos del interesado se extinguen con su muerte. No obstante, la normativa permite que el titular de los datos pueda definir directrices relativas al almacenamiento, supresión y comunicación de sus datos personales para

22. Ley 78-17 del 6 enero de 1978 relativa a la Informática, archivos y libertades añadido por el artículo 63.2 de la Ley 2016-1321 del 7 octubre de 2016 para una república digital (*Loi 2016-1321 du 7 octobre 2016 pour une République numérique*). Disponible en https://bit.ly/47XUtRh.

el caso de su fallecimiento, nombrando un responsable para que lleve a cabo dichas instrucciones. El legislador francés utiliza el término de directrices, no habla de voluntades digitales como la normativa catalana que se indicará más adelante.

Las directrices pueden ser generales o específicas. Las primeras se refieren a todos los datos personales del titular, mientras que las segundas solo contemplan determinados tipos de datos personales que están registrados ante proveedores de servicios particulares (Ordelin Font y Oro Boff, 2020: 121). Las directrices generales atañen al conjunto de los datos personales del titular y pueden ser registradas ante un tercero digital de confianza certificado por la Comisión Nacional de la Informática y Libertades (CNIL), la autoridad de protección de datos en Francia, en un registro único cuyos términos y condiciones se fijan por decreto en el Consejo de Estado, previo dictamen motivado y publicado de la CNIL.

Las directrices particulares son instrucciones que el interesado otorga directamente a los proveedores de servicios para los datos que manejan. Es decir, son instrucciones que se otorgan a prestadores específicos de servicios de Internet sobre los datos de los cuales son responsables. Estas instrucciones no pueden ser el resultado de la mera aceptación de los términos y condiciones generales, el interesado debe tener libertad para expresar su voluntad.

La persona que otorga las directrices puede designar a una tercera persona para que ejecute las instrucciones. En el caso de que el titular de los datos no hubiese designado a una persona para la ejecución de las directrices, tanto generales como particulares, los herederos podrán ejercer los derechos mencionados en la medida necesaria para la liquidación y partición de la herencia. A su vez, los herederos pueden recibir información sobre activos digitales, hacer que se cierren las cuentas de usuario del difunto, oponerse a la continuación del procesamiento de sus datos personales o hacer que se actualicen. El problema es que la normativa francesa solo se refiere a los datos personales, a diferencia de la Ley Orgánica de Protección de Datos que diferencia los datos personales de los contenidos digitales del fallecido, lo cual podría dejar datos no personales fuera de la aplicación de la normativa francesa.

A diferencia del ya mencionado artículo 3, el artículo 96 de la misma normativa introduce el concepto del albacea, lo cual es un claro ejemplo del sentido sucesorio que le ha querido otorgar el legislador estatal al presente artículo. No obstante, se puede cuestionar la adecuación del uso este término, dado que el albacea es nombrado por el testador, y si el testamento digital no es realmente un testamento, no habrá albaceas. A su vez, es cuestionable que la identidad digital que tenía el fallecido en las redes sociales sea transmisible aunque el artículo 96.2 permite expresamente decidir acerca del mantenimiento o eliminación de los perfiles personales en redes sociales de las personas fallecidas.[23] Aunque el artículo 96 utilice el término «testamento», el

23. El Tribunal Federal de Justicia de Alemania en su sentencia ZR 183/17 del 12 de julio de 2018 re-

contenido va más allá de la definición que otorga el Código Civil en su artículo 667 al concepto tradicional del testamento, siendo más adecuado nombrarlo como la voluntad digital del fallecido tal y como lo hace la Ley 10/2017.[24]

Se entiende por «voluntades digitales en caso de muerte» a las disposiciones establecidas por una persona para que, después de su muerte, el heredero, el albacea universal o la persona designada para ejecutarlas, actúe ante los prestadores de servicios digitales con quienes el causante tuviese cuentas activas. Sobre la base de lo dispuesto en el preámbulo de la citada ley para gestionar la huella en los entornos digitales cuando la persona muere y para evitar daños en otros derechos o intereses, tanto de la propia persona como de terceros, las personas pueden manifestar sus voluntades digitales para que el heredero, el legatario, el albacea, el administrador o la persona designada para su ejecución actúen ante los prestadores de servicios digitales después de su muerte. Uno de los mayores problemas que surge en este punto es que, debido a la falta de una normativa homogeneizada a nivel internacional, los prestadores de servicios digitales pueden tener diferentes políticas sobre lo que le sucede con la identidad digital y activos digitales al morir el interesado (Conway y Grattan, 2017).

Mediante estas voluntades digitales las personas pueden ordenar las acciones que consideren más adecuadas para facilitar que la desaparición física y la pérdida de personalidad que supone la muerte se extiendan a los entornos digitales y que eso contribuya a reducir el dolor de las personas que les sobrevivan y con las que tengan vínculos familiares, de afecto o amistad, o bien que se perpetúe la memoria con la conservación de los elementos que ellas determinen en los entornos digitales o con cualquier otra solución que consideren pertinente en ejercicio de la libertad civil que les corresponde en vida.

La persona a quien se encarga la ejecución de las voluntades digitales no tiene un cometido mínimo o esencial, la ley permite diversas posibilidades: comunicar la muerte a los prestadores de los servicios digitales, solicitarles la cancelación de cuentas, y solicitarles que ejecuten lo previsto contractualmente para el caso de muerte del titular, incluida la posibilidad de obtener una copia de los archivos correspondientes. La ley no obliga a que en todos los casos se borre la presencia del difunto en Internet, sino que su cometido podría ser todo lo contrario, en tal caso se debe asegurar que dicha presencia no desaparezca (Ruda González, 2017).

---

solvió que los padres de una menor fallecida en el metro de Berlín en circunstancias que hacían pensar que podría tratarse de un suicidio, estaban legitimados para acceder a su cuenta de Facebook para indagar sobre su muerte al haberse transmitido el contrato que firmó la fallecida con la plataforma a su herederos, en este caso, sus padres. Se consideró que la posición contractual de la hija era transmisible a los padres.

24. Ley 10/2017 del 27 de junio, de las voluntades digitales y de modificación de los libros segundo y cuarto del Código Civil de Cataluña. Boletín Oficial del Estado 173, del 21 de julio de 2017. Disponible en https://bit.ly/3RobqNJ.

La normativa también contempla en su artículo 1, que modifica el artículo 222-2 del Código civil de Cataluña, la posibilidad de otorgar un poder mediante el cual el interesado podrá establecer la gestión de sus voluntades digitales y su alcance para que, en caso de pérdida sobrevenida de la capacidad, el apoderado actúe ante los prestadores de servicios digitales con quienes el interesado tenga cuentas activas a fin de gestionarlas y, si procede, solicitar su cancelación. Al adecuar este apartado a la Ley 8/2021, una persona podrá otorgar un poder en previsión o apreciación de circunstancias que puedan dificultarle el ejercicio de su capacidad jurídica para que el apoderado gestione su voluntad en el mundo digital. El problema es que la aplicabilidad de este artículo está limitada a la vida de la persona con discapacidad y no se refiere en ningún momento al caso en que fallezca el usuario. El titular de la cuenta estará vivo cuando el apoderado tenga que ejecutar las voluntades digitales del primero.

El concepto de «voluntades digitales en caso de muerte» que regula la legislación catalana puede tener un contenido sucesorio y/o no sucesorio. La persona tiene la posibilidad de ordenar el destino de sus bienes digitales en caso de muerte como puede gestionar el destino del resto de su patrimonio analógico (Ginebra Molins, 2020). Junto a estas disposiciones sucesorias el causante puede prever otras disposiciones no sucesorias, a modo de instrucciones a ciertas personas para que actúen sobre el rastro o resto digital (Morse y Birnhack, 2022) que deja tras de sí, lo que cobra especial relevancia para la gestión de las redes sociales.

Ante esta regulación, en el voto particular que formula la Magistrada Roca Trías a la sentencia dictada en el recurso de inconstitucionalidad 4751-2017 del 17 de enero de 2019, se pone de manifiesto que el documento de voluntades digitales no es un testamento, el formato digital de ciertos contenidos en archivos o el lugar donde se encuentran ubicados no los distingue del resto de bienes que puedan integrar la masa hereditaria. Al fallecimiento del otorgante del documento de voluntades digitales, su herencia comprenderá todos los bienes, derechos y obligaciones que no se hayan extinguido por su fallecimiento y su transmisión se producirá, en cualquier caso, por la voluntad que este haya manifestado en testamento y, a falta del mismo, por disposición de la ley.

El documento de voluntades no contiene una verdadera ordenación de la sucesión, ni siquiera de los materiales o archivos digitales del causante, que con independencia del soporte digital en el que se encuentran forman parte del caudal hereditario y son objeto de la sucesión. Lo que recoge realmente el documento es la voluntad del fallecido respecto a la realización de actividades concretas relacionadas con el ejercicio de derechos personalísimos de carácter no patrimonial no transmisibles *mortis causa*, como las de comunicar a los prestadores de servicios digitales su defunción; solicitar la cancelación de las cuentas activas o que ejecuten las cláusulas contractuales o que se activen las políticas establecidas para los casos de defunción y, si procede, que liberen una copia de los archivos digitales que estén en sus servidores.

Instrumento jurídico válido para reflejar la voluntad del interesado

En el artículo 3.2 de la Ley Orgánica de Protección de Datos se indica que mediante real decreto se establecerán los requisitos y condiciones para acreditar la validez y vigencia de estos mandatos e instrucciones y, en su caso, el registro de los mismos. Sin embargo, años después de la entrada en vigor de la norma nacional de protección de datos personales, aún no existe ningún real decreto que cree una herramienta jurídicamente vinculante que permita al interesado reflejar su voluntad relativa al ejercicio póstumo de sus derechos. De la misma manera, no se ha creado un registro que permita inscribir dichos documentos. Por tanto, hasta que no se cree un instrumento con dicho fin, se deberá de utilizar una herramienta válida ya existente.

En este sentido, dentro del ámbito sanitario identificamos al documento de instrucciones previas o voluntades anticipadas, regulado a nivel nacional en el artículo 11 de la Ley Básica de Autonomía del Paciente y en la Ley 7/2002,[25] que fue ideado para que una persona pudiese reflejar su voluntad sobre el cuidado, tratamiento y destino de su cuerpo o partes del mismo anticipadamente.

Aunque principalmente sea aplicable durante la vida de la persona, el párrafo 6 de los motivos de la Ley 7/2002 del País Vasco indica que se optó por un modelo de voluntades anticipadas cuyo contenido sea el más amplio posible y permita abarcar desde la manifestación de los propios objetivos vitales y valores personales, hasta instrucciones sobre los tratamientos que se desean o se rechazan, así como otras previsiones relacionadas con el final de la vida. Al permitir instrucciones relacionadas, entre otras, con la donación de los órganos, se entiende que su aplicabilidad no se limita a la vida de la persona.

Tomando dicha realidad como ejemplo, se podría defender la creación de unas voluntades anticipadas más amplias que también recojan la voluntad del interesado respecto al acceso de sus datos de salud tras su fallecimiento.

Conclusiones

Aunque el objetivo del legislador nacional era crear un instrumento jurídico para que el interesado pueda indicar tras su fallecimiento quién puede acceder a sus datos personales, y en lo que nos respecta, a sus datos de la salud, sigue sin existir dicha herramienta.

Como el testamento digital del artículo 96 de la Ley Orgánica de Protección de Datos Personales se refiere al acceso a los contenidos gestionados por prestadores de servicios de la sociedad de la información, el interesado no podrá utilizar esta vía

25. Ley 7/2002, de 12 de diciembre, de las voluntades anticipadas en el ámbito de la sanidad del País Vasco (BOVP núm. 248, de 30 de diciembre de 2002). Disponible en https://bit.ly/3TqlMzj.

para determinar su voluntad relativa al acceso, rectificación o supresión de sus datos de salud. En este sentido, sería interesante recoger todas las voluntades sanitarias en un único documento, separando los respectivos tratamientos (médicos y de los datos de salud).

Aunque la creación del documento de instrucciones previas o voluntades anticipadas fue ideado para que una persona pueda reflejar anticipadamente su voluntad en cuanto al cuidado, tratamiento y destino de su cuerpo o partes del mismo, el párrafo 6 de los motivos de la Ley 7/2002 del País Vasco indica que se ha optado por un modelo de voluntades anticipadas cuyo contenido sea el más amplio posible y que permita abarcar desde la manifestación de los propios objetivos vitales y valores personales, hasta instrucciones sobre los tratamientos que se desean o rechazan, así como otras previsiones relacionadas con el fin de la vida.

Sobre la base de ese modelo amplio se puede decir que el documento de las voluntades anticipadas es un instrumento jurídico adecuado para que el interesado pueda plasmar su voluntad en cuanto al acceso, rectificación o supresión de sus datos de salud tras su fallecimiento, quedando todas sus pretensiones sanitarias juntas en un único documento. Tras la entrada en vigor de la Ley 8/2021 las personas mayores con discapacidad también podrán, con el apoyo que precisen, indicar en el documento de voluntades anticipadas cuál es su voluntad en cuanto al tratamiento de sus datos de salud que pueda realizarse tras su muerte.

Referencias

Agencia Española de Protección de Datos (2019). «Guía para pacientes y usuarios de la sanidad». Disponible en https://bit.ly/3NoQJAb.

Autoridad Catalana de Protección de Datos (2022). «Guia de protecció de dades per a pacients i usuaris dels serveis de salud». Disponible en https://bit.ly/3toXxqv.

Cámara Lapuente, Sergio (2019). «La sucesión mortis causa en el patrimonio digital». *El notario del siglo XXI: revista del Colegio Notarial de Madrid*, 84: 138-144. Disponible en https://bit.ly/3thOOq6.

Connor, John (2010). «Digital life after death: The issue of planning for a person's digital assets after death». *Texas Tech Law School Research Paper*, 2: 1-23. Disponible en https://bit.ly/47Xf9Jg.

Conway, Heather y Sheena Grattan (2017). «The New Property: Dealing with Digital Assets on Death». *Modern Studies in Property Law*, 9: 99-115. Disponible en https://bit.ly/3GJsUiB.

Craviotto Valle, Patricia (2023), *Responsabilidad por el tratamiento indebido de los datos personales de salud: La historia clínica como eje vertebrador*. Madrid: Reus.

De Lorenzo Montero, Ricardo (2003). *Derechos y obligaciones de los pacientes: Análisis de la Ley 41/2002, de 14 de noviembre básica reguladora de autonomía de los pacientes y de los derechos de información y documentación clínica*. Madrid: Colex.

Díaz Alabart, Silvia (2021). *La protección de los datos y contenidos digitales de las personas fallecidas*. Madrid: Reus.

Ginebra Molins, Maria Esperança (2020). «Voluntades digitales: Disposiciones Mortis Causa». En Ester Arroyo y Sergio Cámara (directores), *El derecho privado en el nuevo paradigma digital*. Madrid: Marcial Pons. Disponible en https://bit.ly/3voQ4Pb.

Llopis Benlloch, José (2016). «Con la muerte digital no se juega: El testamento online no existe». En Ricardo Oliva León y Sonsoles Valero Barceló (coordinadores), *Testamento ¿Digital?* (pp. 45-52). Madrid: Colección Desafíos legales. Disponible en https://bit.ly/3tfkwV7.

Martínez Martínez, Nuria (2019). «Reflexiones en torno a la protección post mortem de los datos personales y la gestión de la transmisión mortis causa del patrimonio digital tras la aprobación de la LOPDGDD». *Derecho Privado y Constitución*, 35: 169-212. Disponible en https://bit.ly/48hwZGv.

Moralejo Imbernón, Nieves (2020). «El testamento digital en la nueva Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales». *Anuario de derecho civil*, 73 (1): 241-281. Disponible en https://bit.ly/3Txbld8.

Morse, Tal y Michael Birnhack (2022). «The posthumous privacy paradox: Privacy preferences and behavior regarding digital remains». *New Media & Society*, 24 (6): 1-20. Disponible en https://bit.ly/47XWcGf.

Ordelin Font, Jorge Luís y Salete Oro Boff (2020). «Bienes digitales personales y sucesión mortis causa: la regulación del testamento digital en el ordenamiento jurídico español». *Revista de derecho*, 33 (1): 119-139. Disponible en https://bit.ly/3Rimax8.

Ruda González, Albert (2017). «Vida más allá de la muerte (digital). La protección de las voluntades digitales en la reforma del derecho catalán». En Anglès Juanpere, Joan Balcells Padullés, Rosa Borge Bravo, Ana María Delgado García, Mirela Fiori, Maria Julià Barceló, Alessandro Mantelero, Clara Marsan Raventós, María José Pifarré de Moner y Mònica Vilasau Solana, *Managing risk in the digital society*. Barcelona: Huygens.

Sáiz Ramos, Macarena y David Larios Risco (2009). «El derecho de acceso a la historia clínica por el paciente: propuesta para la reserva de anotaciones subjetivas». *Derecho y salud*, 18 (1): 21-41. Disponible en https://bit.ly/3RJITUq.

Santos Morón, María José (2018). «La denominada herencia digital: ¿necesidad de regulación? Estudio de Derecho español y comparado». *Cuadernos de Derecho transnacional*, 10 (1): 413-438. Disponible en https://bit.ly/3RJ5Wi8.

Toygar, Alp, C.E. Taipe, Jake Zhu (2013). «A new asset type: digital assets». *Journal of International Technology and Information Management*, 22 (4): 113-120. Disponible en https://bit.ly/3tsmFg2.

Troncoso Reigada, Antonio (2010). *La protección de datos personales. En busca del equilibrio*. Valencia: Tirant lo Blanch.

Van Der Auwermeulen, Barbara (2017). «How to attribute the right to data portability in Europe: A comparative analysis of legislations». *Computer Law & Security Review*, 33: 57-72. Disponible en https://bit.ly/48l7Gnd.

Sobre la autora

Idoia Landa es doctora en Derecho y profesora de Derecho Civil de la Universidad del País Vasco. Su correo es idoia.landa@ehu.eus. https://orcid.org/0000-0002-8345-4117.

REVISTA CHILENA DE DERECHO Y TECNOLOGÍA

La *Revista de Chilena de Derecho y Tecnología* es una publicación académica semestral del Centro de Estudios en Derecho Informático de la Facultad de Derecho de la Universidad de Chile, que tiene por objeto difundir en la comunidad jurídica los elementos necesarios para analizar y comprender los alcances y efectos que el desarrollo tecnológico y cultural han producido en la sociedad, especialmente su impacto en la ciencia jurídica.

DIRECTOR

Daniel Álvarez Valenzuela

(dalvarez@derecho.uchile.cl)

SITIO WEB

rchdt.uchile.cl

CORREO ELECTRÓNICO

rchdt@derecho.uchile.cl

La edición de textos, el diseño editorial
y la conversión a formatos electrónicos de este artículo
estuvieron a cargo de Tipográfica
(www.tipografica.io).