

Recibido: 30 julio 2021
Aceptado: 14 octubre 2021

La sucesión digital internacional y el Reglamento sucesorio europeo 650/2012

Antonio MERCHÁN MURILLO *

SUMARIO: I. Introducción. II. La sucesión digital: la huella digital y los activos digitales. III. La determinación del objeto de la sucesión digital. IV. El patrimonio digital: la propiedad de los datos. V. Los acuerdos contractuales a debate. VI. El Reglamento sucesorio europeo en la sucesión digital. 1. La repercusión transfronteriza de la sucesión. 2. La propiedad digital dentro del Reglamento sucesorio. 3. El certificado sucesorio europeo. VII. Conclusiones.

RESUMEN: Internet se ha convertido en una realidad omnipresente, tanto en nuestra vida personal como colectiva. No obstante, los riesgos que ofrece a la ciudadanía son evidentes. Uno de ellos es lo que pasa con el patrimonio tras la muerte, en relación con actividad desarrollada en Internet, a través de la huella y los activos digitales, que se almacenan en distintos servidores en la nube que, generalmente, se administran a través de cuentas protegidas con contraseña. En este sentido, pretendemos reflexionar sobre las cuestiones esenciales que se van a plantearse en una posible sucesión *mortis causa* digital e internacional, para posteriormente, analizar si el patrimonio digital entra dentro del Reglamento 650/2012, de 4 de julio de 2012 relativo a la competencia, la ley aplicable, el reconocimiento y la ejecución de las resoluciones, a la aceptación y la ejecución de los documentos públicos en materia de sucesiones *mortis causa* y a la creación de un certificado sucesorio europeo.

PALABRAS CLAVE: SUCESIÓN DIGITAL –INTERNACIONAL – HUELLA DIGITAL – ACTIVOS DIGITALES, PROPIEDAD DIGITAL – REGLAMENTO 650/2012.

The International Digital Succession and the European Successory Regulation 650/2012.

ABSTRACT: *The Internet has become an omnipresent reality, both in our personal and collective lives. However, the risks it offers to citizens are obvious. One of them is what happens to heritage after death, in relation to activity carried out on the Internet, through the fingerprint and digital assets, which are stored on different servers in the cloud that, generally, are managed through password protected accounts. In this sense, we intend to reflect on the essential questions that will arise in a possible digital and international succession mortis causa, to later analyze the application of the Regulation of 4 July 2012 on jurisdiction, applicable law, recognition and*

* Profesor ayudante doctor de Derecho Internacional Privado. Universidad Pablo de Olavide.

enforcement of decisions and acceptance and enforcement of authentic instruments in matters of succession and on the creation of a European Certificate of Succession.

KEYWORDS: INTERNATIONAL DIGITAL SUCCESSION, DIGITAL FOOTPRINT, DIGITAL ASSETS, DIGITAL PROPERTY, REGULATION 650/2012.

I. INTRODUCCIÓN

Cuando éramos más pequeños, las cosas que nos dejaban nuestros abuelos tenían un gran valor emocional y, en algunos casos, económico siendo fácilmente su transmisión *post mortem*, pensemos, por ejemplo, álbumes de fotos, diccionarios, libros en los que aparecían o en los que se hablaba de ellos, etc.; es decir, sobre estas cosas podíamos ejercer un derecho sobre los recuerdos. Sin embargo, hoy día, cuando se almacenan en la nube, parece que se olvida que tienen similitud a los de antaño. Los proveedores de servicios digitales no incluyen cláusulas sobre el impacto que la muerte del usuario pueda tener sobre las cosas digitales, aunque si contemplan explícitamente en sus acuerdos que la muerte del usuario implica la terminación de estos¹.

En relación con lo anterior, debe observarse que los recuerdos no son las únicas cosas que se digitalizan. Una persona podría tener un correo electrónico, una foto en la cuenta de almacenamiento de Dropbox (junto con una cuenta financiera, con contraseñas, y bitcoins), una cuenta de música, Apps de compras, cuentas de redes sociales y muchas otras cosas virtuales. En total, una persona podría tener un promedio de entre treinta o cuarenta cuentas en línea, todas pueden tener propiedades digitales y, por tanto, patrimonio de una misma persona. Este hecho nos lleva a pensar ¿Qué pasará con esta propiedad (digital) después de la muerte?

Los activos a los que hacemos referencia son intangibles y es fácil pasar por alto este tipo de propiedad al escribir un testamento, si es que se hace. Asimismo, sería difícil ver que estos activos tienen algún valor o puedan ser objeto de propiedad. No obstante, en nuestra opinión, si pueden ser objeto de propiedad y pueden tener valor económico. Por tanto, se debe hablar de ello tratando el objeto de la sucesión digital; pues, los activos digitales pueden tener algo más que un valor emocional, aunque esta cuestión está abierta a debate. En cualquier caso, se trata de mostrarse proactivo y reflexionar en torno a ello.

¹ Por ejemplo, en el caso de Apple [<http://www.apple.com/legal/icloud/en/terms.html> y Yahoo! [<http://info.yahoo.com/legal/us/yahoo/utos/utos-173.html>]] (fecha de consulta 29 de julio de 2021)

Asimismo, una vez determinado el objeto de la sucesión digital va a surgir la necesidad de plantear si el patrimonio digital y, por tanto, la sucesión digital tiene encaje en el marco del Reglamento 650/2012 del Parlamento Europeo y del Consejo, de 4 de julio de 2012, relativo a la competencia, la ley aplicable, el reconocimiento y la ejecución de las resoluciones, a la aceptación y la ejecución de los documentos públicos en materia de sucesiones *mortis causa* y a la creación de un certificado sucesorio europeo; pues, no será raro que pueda darse un elemento extranjero en la sucesión. En este contexto, pensemos que las cuestiones legales relacionadas en torno al acceso, control, propiedad y transmisión digital son complejas y, como decimos, todo está sujeto a discusión.

II. LA SUCESIÓN DIGITAL: LA HUELLA DIGITAL Y LOS ACTIVOS DIGITALES

Internet se ha convertido en una realidad omnipresente, tanto en nuestra vida personal como colectiva. Una gran parte de nuestra actividad profesional, económica y privada se desarrolla en la Red y adquiere una importancia fundamental tanto para la comunicación humana como para el desarrollo de nuestra vida en sociedad. No obstante, los riesgos y oportunidades que ofrece a la ciudadanía son evidentes.

Uno de los problemas es la propiedad de los datos, esencial para determinar el objeto de la sucesión. El motivo de por qué no se ha prestado atención a la propiedad es porque se antoja relativamente reciente. En cualquier caso, debemos observar que los datos son una forma moderna de riqueza en el mundo digital, lo que presenta problemas relacionados con la propiedad². Pensemos que esta problemática se relaciona con algo que pocos parecen advertir, como el verdadero conflicto existente hoy en día, en un mundo cada vez más global: la soberanía de los datos y, con ello, la residencia de los datos.

Para hacernos a la idea de lo importante que son los datos, basta con fijarse en los servicios que lo necesitan: sectores de energía, transporte, banca, infraestructura de mercados financieros, salud, suministro y distribución de agua potable e infraestructura digital. Estos últimos incluyen puntos de intercambio de Internet (IXP) y sistemas de registro de nombres de dominio de primer nivel y los proveedores de servicios (DNS), etc. Además, deben observarse servicios digitales: motores de búsqueda, mercados en línea, computación en la nube, etc. Así como tecnologías como

² L. Edwards y E. Harbinja, "What happens to my Facebook profile when I die? Legal Issues Around Transmission of Digital Assets on Death", *CREATe Working Paper*, 5, 2013, pp. 1-25.

Blockchain, inteligencia artificial, etc.³ Todo lo referido anteriormente marca el debate de la propiedad de los datos, algo que se presenta crucial como presente y futuro.

Los desarrollos normativos actuales, en conexión con las nuevas tecnologías, como la inteligencia artificial, han desarrollado la protección de datos personales, comenzando con el derecho fundamental al respeto de la vida privada o sobre el derecho fundamental a la protección de datos personales. Sin embargo, no se pensó en la propiedad de los datos, y aún menos por supuesto en la propiedad de los datos personales, en tanto en cuanto no se presenta una línea divisible de lo que son los datos personales y no personales. La línea en este contexto es móvil, ya que los datos que ahora se consideran datos no personales pueden convertirse en datos personales (gracias a los avances analíticos y tecnológicos).

En cualquier caso, lo que parece evidente es que resulta necesario explorar los límites conceptuales de la propiedad de datos personales, para proceder a los debates sobre la propiedad de datos no personales. No obstante, debemos tener presente que los datos, sean personales o no, se reconocen como activos económicos clave⁴, y evitar preguntas sobre su propiedad es, por tanto, retrasar la protección de los usuarios⁵.

En relación con la propiedad, debemos hablar de la huella digital creada por la propia actividad desarrollada en Internet, que se almacena en distintos servidores de proveedores de servicios digitales en la nube que, generalmente, se administran a través de cuentas protegidas con contraseña. De esta forma, mientras estamos vivos, la huella digital está, aparentemente, bajo nuestro control exclusivo, mediante el acceso personal proporcionado por el proveedor de servicios digitales. Sin embargo, si fallecemos perdemos, por motivos evidentes, el control. En primer lugar, cuando un usuario fallece, su huella digital permanece en la red si no se hace nada al respecto o si el causante no lo previó consecuentemente y, al mismo tiempo, herederos, amigos, etc. a menudo encuentran imposible o difícil administrar los archivos que componen la huella digital del primero, en términos de sucesión digital.

En el contexto en el que hablamos, debemos dejar claro que cuando hablamos de huella digital nos referimos a los registros que están en la nube,

³ A. McEwen y H. Cassimally, *Internet de las cosas. La tecnología revolucionaria que todo lo conecta*, Madrid, Anaya Multimedia, 2014, p. 57.

⁴ C. Bartolini, C. Santos y C. Ullrich, "Property and the cloud", *Computer Law & Security Review*, n.º 2, abril, 2018, pp. 358-390.

⁵ Osborne Clarke LLP, *Legal study on ownership and access to data (European Commission 2016)*. Puede consultarse en [<https://bookshop.europa.eu/en/legal-study-on-ownership-and-access-to-data-pbKK0416811/>>] (fecha de consulta 21 de julio de 2021).

creados a través de comunicaciones, transacciones, actos realizados en redes sociales, almacenamiento, fotos o videos, libros, música, etc. Actos que se realizan y que, en suma, forman parte de la identidad digital y que los proveedores de servicios digitales, en muchos casos a través de cuentas virtuales o electrónicas, usan como parte de su negocio a través de la nube⁶.

El contenido de los archivos, que componen la huella digital, puede diferir en naturaleza y valor⁷, para conformar los activos digitales. Algunos de estos registros pueden contener datos protegidos por diferentes derechos, algunos fundamentales, como la libertad de expresión o los datos personales, derechos de imagen y el derecho al honor personal y familiar, etc. Otros pueden contener creaciones originales protegidas por derechos de propiedad intelectual (es decir, documentos o fotografías). Además, algunos pueden tener un valor económico, en mayor o menor grado, pensando con ello en los bitcoins. Otros, mientras tanto, pueden ser, sólo o adicionalmente, de valor sentimental para el usuario o su círculo personal o familiar.

Es más, obvio resulta que, en muchos casos, se da un sorprendente grado de confianza a las muchas empresas que actúan en Internet, por ejemplo, a Facebook y Google o iCloud (de Apple), asumiendo que estas compañías tienen intenciones positivas al usar los datos de los usuarios. Ahora bien, pocos parecen observar que los productos que nos ofrecen de manera personalizada, es fruto de la mercantilización de nuestros propios datos, en principio anonimizados, lo que, en nuestra opinión, podría suponer ignorar posibles violaciones de la privacidad, si examinamos caso a caso. Interesante nos resulta traer a colación una noticia publicada en el New York Times, en 2013, en el que una empresa, llamada *Evidon*, dedicada al análisis web y privacidad, descubrió que las 20 aplicaciones sobre salud más descargadas transmiten información a una red de casi 70 compañías⁸.

Ahora bien, si se observa bien lo comentado anteriormente, hablamos de activos digitales, que podemos dividirlos en relación con su valor económico puro y el valor personal o no económico. Por ejemplo, los nombres de dominio tienen un valor económico mientras que las fotos son de muy poco valor para cualquiera que no sean familiares o amigos inmediatos del titular de la cuenta, pero tienen un valor. No obstante, la huella digital está

⁶ A. Cerrillo I Martinez, "How do we provide the digital footprint with eternal rest? Some criteria for legislation regulating digital wills", *Computer Law & Security Review*, vol. 34, nº 5, 2018, pp. 1119-1130.

⁷ F. Watkins, "Digital Properties and Death: What Will Y ties and Death: What Will Your Heirs Ha our Heirs Have Access to after You Die?", *Buff. L. Rev.*, vol. 62, 2014, pp. 193-235.

⁸ A.G. Sulzberger, "How the Times Thinks About Privacy", *New York Times*, 2019. Puede consultarse en. [<https://www.nytimes.com/2019/04/10/opinion/sulzberger-new-york-times-privacy.html>] (fecha consulta 22 de julio de 2021).

controlada por proveedores de servicios digitales a través de sus acuerdos, que forman parte de los términos del servicio y de las políticas que rigen la prestación, de la mayoría de los servicios digitales que establecen, generalmente, el uso que se puede hacer con los registros creados por las actividades realizadas por los usuarios.

III. LA DETERMINACIÓN DEL OBJETO DE LA SUCESIÓN DIGITAL

En cualquiera de los casos, debemos explorar los límites conceptuales de la propiedad de datos para proceder a los debates sobre la propiedad de datos no personales. Teniendo presente que los datos, sean personales o no, se van a reconocer, como trataremos de demostrar más adelante, como activos económicos clave. Por ello, evitar preguntas sobre su propiedad es, por tanto, retrasar la protección de los usuarios.

Dicho lo anterior, partimos del art. 4.1º Reglamento 2016/679, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD)⁹, que define los “datos personales” como “toda información sobre una persona física identificada o identificable”. Esta definición debemos ponerla en conexión con el considerando 68 que infiere la necesidad de reforzar el control sobre los datos propios de una persona, cuando el tratamiento de los datos personales se efectúe por medios automatizados. Con esto, parece referirse la propiedad de los datos, por parte de los interesados. No obstante, los datos personales aparecen en la definición del Reglamento como “información”, en este caso, información personal, relacionada con una persona física¹⁰, al igual que nuestra Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDyDD)¹¹. Ahora bien, debe observarse que existe una distinción conceptual clara entre los datos y la información, que tiene implicaciones cruciales para determinar la propiedad de los datos¹².

Los datos y la información son dos conceptos distintos¹³, por razones obvias, no hay información sin datos; es decir, no debemos comprender la

⁹ DO L 1119 de 4.5.2016.

¹⁰ J.E.J. Prins, “The propertization of personal data and identities”, *Electronic. J. Comp. L.*, nº8, 2004, pp. 3-25.

¹¹ BOE 6.12. 2018.

¹² A. Garriga Domínguez, *Nuevos retos para la protección de datos personales en la era de las big data y de la computación ubicua*, Madrid, Dykinson, 2016, p. 106.

¹³ A. Aziz y R. Telang, “What Is a Digital Cookie Worth?”, *SSRN*, marzo, 2016, pp. 3-37.

información como cualquier forma transmitir datos, ni la forma de tratar los datos como un activo del que se puede extraer información valiosa de futuro.

De esta forma, puede verse como el RGPD define los datos personales a la inversa, puesto que los datos son la fuente de información¹⁴. De esta forma, el choque entre la privacidad y la propiedad defendida parece un problema en que no se sabe bien cuál debe ser el primero en solucionarse; pues, si hablamos de que lo importante es la información, todo nos va a llevar a priorizar la personal, pero si nos centramos en la propiedad todo conduce a los datos, en su conjunto y debe ser objeto de análisis detallado, puesto que la información no puede ser objeto de propiedad.

El motivo está en que el debate europeo se centró sobre la protección de la privacidad; es decir, desde una perspectiva de los derechos humanos, no desde una perspectiva comercial, que podría conllevar el concepto de propiedad¹⁵. Ahora bien, este argumento también podría funcionar al revés, en un sentido puro, la idea de los derechos humanos tiene que ver con el empoderamiento y, por ello, podría argumentarse que negarle a cualquier individuo un derecho de propiedad de sus datos y así su privacidad viola sus derechos fundamentales.

En cualquier caso, va a resultar esencial, para determinar la propiedad de los datos conocer¹⁶: quién recopila la información, quién la analiza, quién la difunde y a quién, la naturaleza de la información, las relaciones entre las distintas partes, e incluso mayores circunstancias institucionales y sociales.

Lo anterior, nos lleva al estudio del objeto de la sucesión digital. Concretamente, por un lado, se pretende distinguir entre distinguir entre la identidad digital (el sujeto)¹⁷ y el patrimonio digital (el objeto)¹⁸, surgiendo aquí la necesidad de realizar una diferenciación, que en nuestra opinión, se antoja fundamental entre: los datos personales que te identifican o te hacen identificable y la posible mercantilización de los datos (que podrían ser datos no personales), puesto que a menudo se habla de "contenidos digitales" ("los datos producidos y suministrados en formato digital", según el art. 2.1º de la Directiva 2019/770, de 20 de mayo de 2019, relativa a

¹⁴ V. Janeček, "Ownership of personal data in the Internet of Things", *Computer Law & Security Review*, nº 34, 2018, pp. 1039-1052.

¹⁵ E. Fosch Villaronga, P. Kieseberg y T. Li, "Humans forget, machines remember: Artificial intelligence and the Right to Be Forgotten", *Computer Law & Security Review*, vol. 34, nº 2, 2018, pp. 304-313.

¹⁶ A. Cerrillo I Martínez, "How do we provide...", *loc. cit.*

¹⁷ A. Madrid Parra, "La identificación electrónica", *Revista de la Contratación Electrónica*, nº 15, 2001, pp. 5-61.

¹⁸ C. Bartolini; C. Santos y C. Ullrich, "Property...", *loc. cit.*

determinados aspectos de los contratos de suministro de contenidos y servicios digitales¹⁹), en términos generales, pero realmente puede que estemos hablando de nuestros datos. Por este motivo, es posible detectar:

Una vertiente personal: datos personales, intimidad, etc. Que en suma van a constituir la identidad digital de una persona.

Una vertiente patrimonial: activos digitales, que pueden tener un alto valor de mercado, por ejemplo, los datos no personales. En este apartado también podría incluirse, en algún caso, lo anterior siempre que los datos de los usuarios sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados (art. 5.1º.c RGPD).

Dicho de otro modo, hablamos de: identidad digital (el sujeto, en tanto que los datos personales te identifican o te hacen identificable) y lo que podría considerarse como patrimonio digital (el objeto, la posible mercantilización de los datos)²⁰, puesto que a menudo se habla de “contenidos digitales”, en términos generales, cuando realmente puede que estemos hablando de nuestros datos. Motivo por el que es posible detectar una vertiente personal (datos personales, intimidad e identidad digital) y una vertiente patrimonial (todo tipo de “activos digitales” pueda tener un alto valor de mercado, en el que podrían incluirse en algún caso lo anterior y, además, los datos no personales. Todos ellos como activos).

Con lo anterior, debemos hacer una reflexión: un hecho no discutible es que la identidad es muy valiosa, especialmente, si nos movemos en un espacio on-line²¹. Los detalles de uno mismo aumentan a medida que uno navega por internet y se van vinculando datos que son intrínsecos a uno mismo y aunque se identifiquen como datos no personales lo van a ser²². De esta forma, surge el consabido temor en el que las técnicas de vinculación de datos, anexo a la identidad y/o a la identificación de una persona, alimentan los temores de que se explote la identidad de alguien. En este sentido, podría decirse que la propiedad de dichos datos implicaría conceptualmente la propiedad de las identidades de las personas, con

¹⁹ DO L 136 de 22.5.2019.

²⁰ S. Cámara Lapuente, *La sucesión mortis causa en el patrimonio digital: una aproximación, conferencia dictada en el colegio notarial de Madrid*, salón académico, el 24 de enero de 2019, puede consultarse en [<http://www.elnotario.es/index.php/academia-matritense-del-notariado/9279-la-sucesion-mortis-causa-en-el-patrimonio-digital-una-aproximacion>] (fecha de consulta 24 de julio de 2021).

²¹ A. Madrid Parra, “Aspectos jurídicos de la identificación en el comercio electrónico”, en *Derecho del comercio electrónico. (primeras Jornadas celebradas en la Universidad Carlos III de Madrid)* (coord. I. Ramos Herranz y R. Illescas Ortiz (dir.), La Ley, 2001, pp. 225–257.

²² S. Mason, “Validating identity for the electronic environment”, *Computer Law & Security Review*, nº 3, 2004, pp.164–170.

independencia de que los datos sean personales o no personales. Por ello, debemos tener presente que las personas dependen del uso de sus datos²³. Por ejemplo, pensemos que el ADN de una persona puede ser lo que los datos son en internet de un individuo cualquiera (que son datos personales como ha reconocido el TEDH).

En este contexto, en relación con la vertiente personal, como datos propios de la persona que nos lleva a los atributos de identidad que permiten identificarla, ante necesidad de vincular la información a una determinada persona, sin olvidar que la identidad electrónica o digital es un conjunto de informaciones y datos relevantes para una persona, física o jurídica, que se almacenan y se transmiten a través de los sistemas electrónicos y se utiliza con el fin de identificar a una persona²⁴. Por otro lado, en relación con la vertiente patrimonial, con el proceso de verificación de la afirmación que se hace relativa a la identidad o al atributo perteneciente a dicha identidad, que va a formar parte de la transacción o de lo que se hace en la nube.

En definitiva, podríamos hablar de un entorno intrínsecamente personal, es decir datos que son y pertenecen únicamente a la esfera privada de la persona, y un entorno que no es intrínsecamente personal²⁵. Los primeros son los que estaría o serían objeto de protección por la propia normativa de protección de datos y los segundo son los que serían objetos del derecho a la propiedad de los datos.

IV. EL PATRIMONIO DIGITAL: LA PROPIEDAD DE LOS DATOS

Cuando se configura una cuenta en línea, la mayoría de las veces se acepta un conjunto de términos de servicio, que se configuran a través de un simple “clic”. Este acuerdo crea un contrato con el proveedor de servicios de la cuenta, que en principio va a tener cláusulas que van a ser relevantes en caso de muerte, lo que veremos más adelante. Dentro de ese contrato, la distinción importante en la que nos debemos situar, en primer lugar, es en la propiedad “en” la nube y propiedad “de” la nube. Sin bien la propiedad digital se puede definir como la propiedad y gestión y derechos relacionados con una cuenta digital y activo digital. Una cuenta digital la podríamos contextualizar como un sistema electrónico para crear, generar, enviar, recibir, almacenar, mostrar

²³ J.E.J. Prins, “The propertization of...”, *loc. cit.*

²⁴ A. Merchán Murillo, *Firma electrónica: Funciones y problemática: especial referencia al Reglamento (UE) nº 910/2014, relativo a la identificación electrónica por la que se deroga la Directiva 1999/93/CE de firma electrónica*, Aranzadi, 2016, p. 256.

²⁵ V. Janeček, “Ownership of...”, *loc. cit.*

o procesar información que proporciona acceso a un activo digital o servicio digital, en otras palabras, una cuenta digital es el método por cuál se llega a los correos electrónicos, música y otros recursos digitales, siendo por tanto el activo digital los archivos, ya sean correos electrónicos, archivos JPEG o cualquier otra cosa, almacenado en una cuenta digital.

En nuestra opinión, dado que la gran mayoría de los activos digitales se encuentran dentro de una cuenta digital, las dos tienden a mezclarse en discusión, al difuminarse la propiedad de la nube con la propiedad en la nube. Esta distinción es relevante porque los activos digitales son, normalmente, creación del usuario, mientras que las cuentas digitales son creación del proveedor.

De esta forma, la distinción entre los activos y las cuentas digitales es importante, ya que deben tener un tratamiento diferenciado bajo la Ley, por ejemplo, obsérvese el art. 96 LOPDyDD cuando se habla sobre el “acceso a contenidos gestionados por prestadores de servicios” y “decidir acerca del mantenimiento o eliminación de los perfiles”²⁶. De esta forma, mientras que un heredero puede tener un derecho a un activo digital, él o ella no necesariamente tendría el derecho a la cuenta digital, que es donde se almacena el activo. La razón de esta diferencia de trato es que las cuentas digitales pueden ser intransferibles según los términos del servicio, momento en el que el derecho a la cuenta expira con la muerte del usuario. Ahora bien, el contenido, sin embargo, pertenece al patrimonio del difunto, motivo por el que se le debe permitir el acceso.

En este contexto, van a ser importantes las cláusulas sobre la disposición que se establezca en el ordenamiento de Estado del foro; pues de ser aplicable la *lex fori*, por ejemplo, los usuarios de Facebook aceptan que cualquier “reclamación se debe resolver en un tribunal competente en la República de Irlanda y que las leyes de ese país regirán estas Condiciones”, lo que supone una cuestión extremadamente importante ya que este tipo cláusulas tienen la posibilidad de anular la aplicabilidad de la ley de otro Estado, es decir, no importaría si se aplicará la Ley española en relación a la transferencia de activos digitales, porque ésta no regiría, regiría la Ley irlandesa. En relación con la propiedad de los datos deben observarse dos perspectivas bajo las cuales se puede analizar la propiedad, y mezclarlas puede generar confusión. Por un lado, encontramos la propiedad “de” la nube, compuesta de un hardware y un software²⁷, que constituyen los activos comerciales del

²⁶ S. Cámara Lapuente, “La sucesión *mortis causa* en el patrimonio digital: una aproximación”, *El Notario del Siglo XXI*, nº 84, marzo-abril de 2019), pp. 138-144.

²⁷ J. A. Cuerva De Cañas, “La propiedad intelectual en el mundo digital”, en *Sociedad Digital y Derecho* (Tomás de la Quadra-Salcedo y Fernández del Castillo (dir.), J.L. Piñar Mañas (aut.), Ministerio de Industria, Comercio y Turismo, 2018, pp. 719-740.

proveedor del servicio; por otro lado, la propiedad “en” la nube, ante la necesidad de garantizar la protección de los datos de los usuarios. En este contexto, surgen cuestiones de propiedad intelectual planteadas a raíz de modificaciones de datos de los clientes y derechos de propiedad sobre los datos procesados en la nube, por ejemplo, metadatos²⁸.

De esta forma, como decimos, la propiedad “de” la nube se estructura básicamente en dos componentes: hardware y software, los cuales constituyen los activos comerciales del proveedor del servicio. El primero consiste en un conjunto de bienes materiales, sujetos a las reglas de propiedad comunes, y cuya circulación depende de las leyes estatales. La del software es una situación más complicada, debido a que está sujeto al complejo marco de las normas de propiedad intelectual. Por otro lado, la propiedad “en” la nube, que consiste en la necesidad definida, a nivel global, de garantizar que los usuarios retengan el control sobre sus propios datos. Estos datos, por ejemplo, pueden ser escritos u otras obras de arte (incluidas fotografías que no pueden considerarse datos personales), notas, documentos utilizados para nuestro trabajo, documentos privados, copias de seguridad, materiales electrónicos comprados, como libros, música o películas, software, etc. Todos estos datos plantean preguntas muy importantes sobre su propiedad²⁹. Además, estos datos pueden estar sujetos a protección de acuerdo con su contenido (por ejemplo, protección de datos, derechos de autor, secretos comerciales y similares, etc.), lo que complica su régimen legal aplicable.

La ley otorga protección a ambas partes desde diferentes y variadas perspectivas, obteniéndose como resultado una compleja combinación de regímenes entrelazados, cuya complicación viene de la naturaleza intrínsecamente internacional de la Computación en nube, que planteará la más que posible problemática de la Ley aplicable³⁰.

En cualquier caso, centrándonos en este segundo aspecto, pensemos que los usuarios pueden tener acceso a una cantidad sin precedentes de servicios personalizados, lo que conllevará aparejado que el entorno mismo (Internet) pueda adquirir información sobre los usuarios de manera automática, pudiendo encontrarnos con perfiles invasivos e inferenciales

²⁸ J. Pabón Cadavid, “Protección legal a los metadatos y la gestión digital de los derechos de autor”, *Ius et Praxis*, vol. 26, nº 1, 2020, pp. 57-76; y P.A. De Miguel Asensio, “Mercado único digital y propiedad intelectual: las Directivas 2019/789 y 2019/790”, *La Ley: Unión Europea*, nº 71, 2019.

²⁹ CNUDMI/UNCITRAL: *Aspectos jurídicos de los contratos inteligentes y la inteligencia artificial: documento presentado por Chequia*, Nueva York, 25 de junio a 13 de julio de 2018.

³⁰ A-L. Calvo Caravaca y J. Carrascosa González, *Derecho internacional privado*, vol. II, 18ª ed., Granada, Comares, 2018, p. 1363.

resultado del intercambio de datos, en particular cuando múltiples dispositivos, por ejemplo, de Internet de las Cosas, que proporcionan datos que están vinculados a una sola identidad (virtual) de usuario.

Existen al menos tres formas posibles de monitoreo y creación de perfiles, que ofrecen motivos para la discriminación en los sistemas de IoT³¹: a) recopilación de datos, que conduce a inferencias sobre la persona (por ejemplo, comportamiento de navegación en Internet); b) creación de perfiles en general mediante la vinculación de conjuntos de datos IoT (a veces denominado “fusión de sensores”); c) perfil que se produce cuando los datos se comparten con terceros que combinan datos con otros conjuntos de datos (por ejemplo, empleadores, aseguradores).

Las tecnologías de identificación permiten precisamente este tipo de vinculación. Al enlazar múltiples dispositivos o equipos y los datos que producen a una única identidad de usuario, el uso de un dispositivo o servicio puede personalizarse, basándose en comportamientos y preferencias del pasado, y deducciones extraídas de estos datos.

Los riesgos de privacidad de la vinculación entre conjuntos de datos se vuelven particularmente graves cuando los sistemas de autenticación o los almacenes de identidad tienen acceso a los datos que generan los dispositivos autenticados. Aunque ofrece una mejor experiencia de usuario, el enlace y la personalización entre múltiples dispositivos y servicios de presentan riesgos, para la privacidad del usuario.

En este contexto, observemos que las tecnologías de identificación de IoT permiten vincular los perfiles de usuario, a través de Blockchain o de la propia inteligencia artificial³², que pueden desconocer el alcance y potencial de ellos, así como en qué medida sus datos son accesibles a terceros fuera del contexto o propósito para el que fueron creados.

Pensemos en los datos de las aplicaciones de salud o de aparatos como Fitbit que podrían, por ejemplo, ser relevantes para empresas al inferirse hábitos de ejercicio, comportamiento alimentario o sueño. La falta de sueño, que Fitbit rastrea, no cabe duda de que se puede relacionar con el bienestar: problemas de salud, bajo rendimiento cognitivo, emociones negativas como depresión, la tristeza, etc. Aparentemente, podría hablarse de datos aparentemente no personales, creados a través de la denominada anonimización. No obstante, las deficiencias de la anonimización deben ser tenidas muy en cuenta; pues, existe una preocupación especial de que los

³¹ C. Sullivan, “Protecting digital identity in the cloud: Regulating cross border data disclosure”, *Computer Law & Security Review*, vol. 30, n° 2, 2017, pp. 137-152.

³² C. Sullivan, “Digital identity. From emergent legal concept to new reality”, *Computer Law & Security Review*, vol. 34, n° 4, 2018, pp. 723-731.

datos vinculados a una determinada información pueden ser utilizados para predecir el comportamiento futuro. Asimismo, estos datos son susceptibles de abrirse a la reidentificación e ingeniería inversa de identidad, pensemos que la tecnología de la información permite a través de nodos y metadatos (*big data*) se vincule a un determinado dispositivo.

Como puede observarse, se da una falta de claridad legislativa de lo que debe o debería ser objeto de la sucesión y de lo que es propiedad digital y, como resultado, los proveedores de servicios se han decantado por el lado de intimidad y la protección de los datos personales, quizá por interés³³. No obstante, a medida que avanza el siglo XXI³⁴, debe considerarse si la privacidad debiera ser realmente el principal objetivo en relación con las propiedades digitales del difunto.

Parece esencial, en cualquier contexto, en el que hablamos de la propiedad de los datos conocer: quién recopila la información, quién la analiza, quién la difunde y a quién, la naturaleza de la información, las relaciones entre las distintas partes, e incluso mayores circunstancias institucionales y sociales. Pensemos en los servicios en línea “gratis”, por ejemplo, los servicios de Wifi gratuitos en espacios públicos, por ejemplo, en aeropuertos, en hoteles, estaciones de tren, etc. Que obligan a los usuarios a aceptar cookies y rastreadores y a dar su dirección de correo electrónico si quieren navegar por internet; es decir, si desean tener un servicio gratuito de Internet, deben revelar al proveedor determinados datos, relacionados con la autenticación de la identidad, como los sitios web visitados, datos de ubicación, etc. y, por lo tanto, crean un perfil personal. Otro ejemplo, podemos encontrarlo para las redes sociales, que en el fondo son servicios de computación en nube, que crean perfiles a través de sistemas de inteligencia artificial, al crear un perfil social y autorizar el acceso de Facebook a sus datos de perfil.

Estos servicios gratuitos pagados con datos, que deberán ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados (“minimización de datos”) (art. 5.1º.c RGPD), van en contra de la posibilidad de establecer un derecho a la propiedad de los datos, puesto que en un sistema normativo como el nuestro, en el que todo se ha centrado en la información, parece que la discusión sobre mecanismos adecuados para la protección de datos personales se traslada a los modelos estadísticos, perfiles y algoritmos que se utilizan para generar conocimiento sobre nuestro comportamiento individual, social.

³³ A. Garriga Domínguez, *Nuevos retos para...*, *op. cit.*

³⁴ S. Cámara Lapuente, “La sucesión *mortis causa* en el patrimonio digital”, *Anales de la Academia Matritense del Notariado*, 2019, pp. 375–432.

De esta forma, parece que la mercantilización de nuestras identidades y comportamientos se han centrado no en la necesidad de establecer un debate sobre los derechos de propiedad con respecto a los datos personales, sino más bien en un debate sobre la necesidad de proporcionar instrumentos jurídicos necesarios proteger y controlar la forma en que se procesan nuestras identidades.

Los datos y la información son dos conceptos distintos³⁵, por razones obvias, no hay información sin datos; es decir, no debemos comprender la información como cualquier forma transmitir datos, ni la forma de tratar los datos como un activo del que se puede extraer información valiosa de futuro.

La raíz de este problema está en que la legislación de la UE define los datos personales a la inversa, puesto que los datos son la fuente de información³⁶. De esta forma, el choque entre la privacidad y la propiedad defendida parece un problema en que no se sabe bien cuál debe ser el primero en solucionarse; pues, si hablamos de que lo importante es la información, todo nos va a llevar a priorizar la personal, pero si nos centramos en la propiedad todo conduce a los datos, en su conjunto y debe ser objeto de análisis detallado, puesto que la información no puede ser objeto de propiedad.

V. LOS ACUERDOS CONTRACTUALES A DEBATE

No hay duda de que los tokens, saldo bancario de cuenta online, sea de PayPal o cualquier otra entidad, tienen un valor económico y patrimonial, por lo que van a formar parte de la herencia. No obstante, la música, fotos, email, documentos almacenados en la nube, entre otros, en principio, se habla, como hemos dicho, de su gran valor emocional y, además, que el causante no es propietario del archivo o contenido digital, sino un derecho a usarlo de acuerdo con las condiciones estipuladas en el contrato.

Por ello, resulta relevante tratar los acuerdos contractuales, para la sucesión digital, ya que van a tener incidencia en la aplicación del Reglamento sucesorio, al poder plantear la posible intransmisibilidad de lo digital, en virtud de lo firmado en el propio contrato por el propio usuario.

En este sentido, perfiles de redes sociales, por ejemplo, en Facebook, Twitter, Google + o LinkedIn o en los perfiles de los juegos de las Apps, parece que se olvida que tienen similitud a los de antaño. Sin embargo, los

³⁵ Osborne Clarke LLP, *Legal study on ownership...*, *op. cit.*

³⁶ J.E.J., Prins, "The propertization of...", *loc. cit.*

proveedores de servicios digitales no incluyen cláusulas sobre el impacto que la muerte del usuario pueda tener sobre las cosas digitales, aunque si contemplan explícitamente en sus acuerdos que la muerte del usuario implica la terminación de estos.

En este punto, la pregunta clave sería la siguiente: hasta qué punto los activos digitales encajan en el contexto normativo actual y si se necesita una nueva ley, ya que, en primer lugar, los activos sólo entran en el patrimonio de un difunto si son propiedad de éste, pero no todas las cosas que podemos querer, o creemos que poseemos, son propiedad, por ejemplo, algunas licencias de uso como, por ejemplo, iTunes, o libros electrónicos descargados que, en principio, se venden en relación con la música o propiedad intelectual³⁷, en general; es decir, se proporcionan explícitamente sólo para un período de tiempo, lo que puede significar que expiran al morir (o antes) y, por lo tanto, no forman parte del patrimonio del fallecido, es famoso el caso de Bruce Willys, que no tuvo suerte, aunque recientemente se ha dado algún caso en el que se permite el acceso a la cuenta, como veremos.

Por otro lado, debe tenerse presente que, desde el punto de vista de la protección de datos, cuando una persona fallece, no tiene derecho a proteger sus datos personales. Así se establece claramente en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de dichos datos, y derogando Directiva 95/46 / CE que reconoce que “no se aplica a los datos personales de personas fallecidas” (considerando 27). Ahora bien, países como Francia o España han hecho alguna excepción. Concretamente, nuestro país lo ha hecho entorno al art. 96 y 3 de la LOPDyDD, haciéndose eco de que, el Reglamento también establece que “los Estados miembros pueden establecer normas sobre el procesamiento de datos personales de personas fallecidas”, lo que nos va a llevar al problema relacionado con la jurisdicción, ley aplicable y activos digitales, ya que si la legislación no está armonizada podrá otorgar diferentes poderes a herederos e interesados.

En cualquier caso, debe tenerse en cuenta que la referencia que se hace en los arts. 3 y 96 LOPDyDD es a los derechos ARCO (acceso, rectificación, cancelación y oposición) de los datos personales que se hallen recogidos en los ficheros³⁸, en coherencia con lo dicho por el Tribunal Constitucional, en

³⁷ J. Díaz-Noci, “Intellectual property and transmedia informative products: A comparative, transnational legal analysis”, *Hipertext.net: Revista Académica sobre Documentación Digital y Comunicación Interactiva*, nº 20, 2020.

³⁸ N. Moralejo Imbernón, “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”, *ADC*, t. LXXIII, 2020, fasc. I, pp. 241–281.

su Sentencia 292/2000, de 30 de noviembre, en relación con el objeto de protección del derecho fundamental (Fundamento Jurídico 6º) y la AEPD en su memoria de 2002³⁹.

Ahora bien, debemos hacer una diferenciación en este aspecto, el valor que tienen las fotos impresas en álbumes de fotos y las fotos digitales de las redes, mientras se piensa que es emocional, también se puede pensar que es económico. La mercantilización de las identidades digitales es una realidad emergente en la economía basada en datos. Lo problemático es que las personas no son conscientes del valor monetario de sus datos personales y tienden a subestimar su poder económico dentro del mercado de datos y a sucumbir pasivamente a la mercantilización de su identidad digital.

La privacidad y la protección de datos personales a menudo se han rechazado como una defensa pasiva de las personas frente a la recopilación, el uso y la reutilización de sus datos. Sin embargo, en la era del big data, esto puede ser poco realista e ineficaz, porque la limitación del acceso y el uso de los datos es difícil de aplicar y limita las oportunidades que ofrece el big data. En cambio, un enfoque más realista y eficaz hacia la protección efectiva de los intereses de los interesados sería un empoderamiento activo de las personas en la gestión de sus datos personales. Dicho de otro modo, puede observarse como el enfoque tradicional ha sido la protección de manera pasiva de la privacidad de la información, sólo se observa en la legislación existente la protección de los datos según su valor personal y emocional (cualitativo). Para reducir la asimetría de la información en la era de los macrodatos y hacer que las personas sean actores más fuertes en esta economía impulsada por los datos, lo que se necesita es proporcionar cada vez más información sobre el valor monetario (cuantitativo), cuánto valen sus datos.

Aquí es donde aparecen los aspectos contractuales, que pueden provocar la posible intransmisibilidad establecida en el contrato celebrado por el usuario y el prestador de servicios. Que el derecho del causante sea de carácter obligatorio y consista en una licencia de uso no es obstáculo para que sea transmisible *mortis causa*, pero el problema viene dado por los "términos de uso"; esto es, las condiciones generales establecidas por el proveedor del servicio o suministrador del contenido digital determinan la intransmisibilidad del derecho adquirido por el usuario o su extinción con la muerte de este⁴⁰. Estas cláusulas, en principio, como comenta la Prof. Moralejo Imbernón serán válidas una cláusula que establezca el carácter

³⁹ Puede consultarse en [<https://www.aepd.es/media/memorias/memoria-AEPD-2002.pdf>] (Fecha de consulta 25 de julio de 2021).

⁴⁰ M. J. Santos Morón, "La denominada "herencia digital": ¿necesidad de regulación? estudio de derecho español y comparado", *CDT*, vol. 10, nº 1, 2018, pp. 413-438.

temporal de un derecho de crédito a menos que pueda considerarse abusiva a la vista del conjunto de derechos y obligaciones de las partes⁴¹.

En este contexto, podríamos encontrarnos en situaciones en las que las partes intervienen en desigualdad de condiciones, las leyes aplicables sobre contratos suelen establecer que el contrato en cuestión es un contrato de adhesión. Los proveedores de servicios suelen estar familiarizados con un número limitado de leyes locales y especialmente con las leyes locales que gobiernan los contratos y el derecho a la privacidad⁴². Por esa razón procederán a elegir una ley aplicable que establezca los requisitos relativos a la protección de la información que el proveedor de servicios en cuestión pueda o esté dispuesto a cumplir, lo cual ofrece reglas para la elaboración de contratos que son predecibles y aceptables para sus fines.

Estas cuestiones pueden obligar al usuario a asumir ciertas responsabilidades frente a sus usuarios finales en relación con la determinación de la Ley aplicable tipo, pudiendo ser ésta abusiva. Ante esto, como indica la STJUE 28 de julio de 2018, asunto C-191/15, al apreciar el carácter abusivo de una determinada cláusula contractual en el marco de una acción de cesación, del art. 6, ap. 2, del Reglamento Roma I, resulta que la elección de la ley aplicable se hace sin perjuicio de la aplicación de las disposiciones imperativas previstas por la ley del país en el que residen los consumidores cuyos intereses son defendidos mediante esa acción. Entre tales disposiciones pueden figurar las que transponen la Directiva 93/13, siempre que garanticen un nivel de protección más elevado para el consumidor⁴³. En este punto, el principal riesgo de índole jurídica que se plantea esta no poder evaluar plenamente los riesgos vinculados con el contrato, con los datos y su valor, que en ningún momento se indica si tienen valor monetario o no. Sólo se protege la información.

En este aspecto conviene recordar la Sentencia del Tribunal Federal de Alemania que declaró transmisible la posición contractual de la fallecida y consideró que las condiciones generales que excluían esa relación de la herencia eran abusivas por no superar el control de contenido del § 307.1 y 2 BGB⁴⁴, que vienen a indicar que los términos y condiciones generales son

⁴¹ N. Moralejo Imbernón, "El testamento digital en...", *loc. cit.*,

⁴² CNUDMI/UNCITRAL: *Propuesta del Gobierno del Canadá: posible labor futura en materia de comercio electrónico: cuestiones jurídicas que afectan a la informática "en la nube"*, Nueva York, 7 a 18 de julio de 2014, p. 2.

⁴³ STJUE 28 de julio de 2018, *Verein für Konsumenteninformation contra Amazon EU Sàrl*, as. 191/15 (ECLI:EU:C:2016:612), apartado 59.

⁴⁴ El precepto § 307 Inhaltskontrolle indica que: "(1) Bestimmungen in Allgemeinen Geschäftsbedingungen sind unwirksam, wenn sie den Vertragspartner des Verwenders entgegen den Geboten von Treu und Glauben unangemessen benachteiligen. Eine unangemessene Benachteiligung kann sich auch daraus ergeben, dass die Bestimmung nicht klar und

ineficaces si perjudican injustificadamente al socio contractual del usuario en contra de los requisitos de buena fe. Por ello, condenó a la plataforma digital indicando que el contenido que en ella se alojaba formaba parte de la herencia de su titular y, por tanto, en transmisible a los herederos.

Por tanto, no sería descabellado plantear la monetización de los datos personales como una realidad en casi todos los campos del mercado digital. La Comisión Europea ha destacado que el mercado de los datos de los consumidores está creciendo rápidamente y los modelos de negocio basados en la monetización de los datos se vuelven predominantes⁴⁵. En este sentido, se puede decir que la información general sobre una persona tiene valor económico desconocido y no expresado en los contratos tales como la edad, el sexo y la ubicación que valen, según la calculadora creada por Financial Times, apenas 0,05 centavos. Las personas que están comprando un automóvil, un producto financiero o unas vacaciones son más valiosas para las empresas que desean vender esos productos. Por ejemplo, los datos personales de los compradores de automóviles valen alrededor de 0,21 centavos por persona⁴⁶. Los datos personales que contienen condiciones de salud específicas o información necesaria que mezclada tienen un valor indudable y, además, en principio, los datos se pueden vender y revender muchas veces. A lo anterior, hay que destacar una encuesta de McAfee que estableció que el promedio de valor de los datos personales que, conformarían activos digitales, valen alrededor de \$ 55,000.12⁴⁷.

verständlich ist. (2) Eine unangemessene Benachteiligung ist im Zweifel anzunehmen, wenn eine Bestimmung 1. mit wesentlichen Grundgedanken der gesetzlichen Regelung, von der abgewichen wird, nicht zu vereinbaren ist oder; 2. wesentliche Rechte oder Pflichten, die sich aus der Natur des Vertrags ergeben, so einschränkt, dass die Erreichung des Vertragszwecks gefährdet ist. (3) Die Absätze 1 und 2 sowie die §§ 308 und 309 gelten nur für Bestimmungen in Allgemeinen Geschäftsbedingungen, durch die von Rechtsvorschriften abweichende oder diese ergänzende Regelungen vereinbart werden. Andere Bestimmungen können nach Absatz 1 Satz 2 in Verbindung mit Absatz 1 Satz 1 unwirksam sein.

⁴⁵ Vid. la identificación monetaria que se hace de los datos en la Propuesta de Directiva relativa a determinados aspectos de los contratos de suministro de contenidos digitales, COM (2015) 634 final 2015/0287 (COD), 9 de diciembre de 2015, que desaparece de la Directiva relativa a determinados aspectos de los contratos de suministro de contenidos y servicios digitales.

⁴⁶ E. Steel, C. Locke y E. Cadman, "How much is your personal data worth?", *Financial Times*, 2017. Puede consultarse en [https://ig.ft.com/how-much-is-your-personal-data-worth/?ft_site=falcon#axzz4dMtRpoZd] (fecha de consulta 15 de julio de 2021).

⁴⁷ McAfee encuestó a 3.000 personas en 10 países, preguntando sobre el valor financiero en relación con el valor de los activos digitales, como archivos de música y álbumes de fotos en línea, etc. El promedio de EE UU fue de \$ 55,000 (K. Steinmetz, "Your Digital Legacy: States Grapple with Protecting Our Data After We Die", *Time*, noviembre, 2012). Puede consultarse en [<https://techland.time.com/2012/11/29/digital-legacy-law/>] (fecha de consulta 15 de julio de 2021).

Hay investigaciones disponibles sobre la estimación del valor de los datos personales. Una de ellas es de la Organización para la Cooperación y el Desarrollo Económicos sobre metodologías para medir el valor monetario de los datos personales. La OCDE distingue los métodos que se basan en la valoración de mercado y los métodos que se basan en la valoración individual. Los métodos de valoración de mercado se centran en: a) resultados financieros para registros de datos; b) precios de mercado para datos; c) costo de una violación de datos; d) precios de datos en mercados ilegales; e) encuestas y experimentos económicos; y f) datos sobre la disposición de los usuarios a pagar para proteger sus datos⁴⁸.

En consecuencia, podría plantearse la nulidad de las cláusulas de intransmisibilidad, tal y como hemos apreciado, ante la falta de información veraz del valor de los datos. Asimismo, tampoco sería descabellado plantear la excepción de orden público si se imponen las cláusulas de competencia y ley aplicable, abusivas, que obligan a unos usuarios sin medios a acudir a un Tribunal y a la aplicación de una ley que puede ser claramente desfavorable a sus intereses, que, además, puede entrar en colisión con la aplicación de la LOPDyDD.

VI. EL REGLAMENTO SUCESORIO EUROPEO EN LA SUCESIÓN DIGITAL

Una vez determinada la patrimonialidad digital de los datos, pasamos a determinar si el patrimonio digital entra en el ámbito de aplicación del Reglamento sucesorio. Para ello, pongamos experiencias reales. Cuando una persona fallece, sin que otorgue testamento, o incluso habiéndolo otorgado, puede que no prevea nada sobre sus activos digitales y, aun menos, sobre su huella digital. En este sentido, es posible que una persona muy cercana (familiar, amigo, etc.) encuentre la forma de acceder a su Tablet u ordenador, portátil o de sobremesa, donde probablemente tendrá guardada información acerca del acceso a cuentas de redes sociales (*v.gr.*, donde almacena fotos con familiares y con amigos muy cercanos, música que escuchaban juntos, etc.), las cuentas bancarias a las que accede por Internet (no había extractos impresos disponibles), cuentas de correo electrónico, cuentas de almacenamiento en las que guarda sus trabajos de investigación, cuentas de PayPal, tokens comprados como formas de inversión o como

⁴⁸ OCDE, "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value", *OECD Digital Economy Papers*, No. 220. Puede consultarse en [https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en] (fecha de consulta 15 de julio de 2021).

acciones en empresas, criptomonedas, etc. Obvio resulta que cualquier heredero o legitimario querrá saber el estado de la cuenta de PayPal, deseará acercarse al banco donde el causante tenía una cuenta online, intentará acceder al teléfono móvil de Apple donde puede tener una billetera electrónica donde almacenaba las criptomonedas, tokens, etc. Incluso, le entusiasmaría la idea de tener una copia de las fotos almacenadas en la cuenta de redes sociales y acceso a la cuenta de correo electrónico y a las de almacenamiento de Drive.

Con respecto a las cuentas de redes sociales y la cuenta de correo electrónico pueden surgir preguntas sobre la protección de datos o la privacidad, pudiendo el proveedor de servicios utilizar este argumento como principal para negarse a dar acceso o amparar su negativa en el propio contrato, que en su día se firmó. No obstante, la cuestión va a estar en ver qué información se debe dar a los herederos, cuando soliciten acceso a los activos digitales y que podrán hacer para el control de los activos.

No cabe duda, o al menos para nosotros, que todo lo anterior son activos o registros creados, registrados, transmitidos y/o almacenados en formato digital u otra forma intangible por medios electrónicos, magnéticos u ópticos o de cualquier otra forma. Estos registros, en la mayoría de los casos, es evidente que unos tienen un valor económico, pero otros aparentemente no los tienen, tan sólo se considera un valor emocional o no patrimonial.

Lo más probable es que estas cuestiones, las decidan, en primer lugar, los tribunales. Ahora bien, la cuestión va a ser más problemática si cabe, ya que va a surgir la necesidad de plantear⁴⁹ la posible aplicación del Reglamento 650/2012 del Parlamento Europeo y del Consejo, de 4 de julio de 2012, relativo a la competencia, la ley aplicable, el reconocimiento y la ejecución de las resoluciones, a la aceptación y la ejecución de los documentos públicos en materia de sucesiones *mortis causa* y a la creación de un certificado sucesorio europeo; pues, no será raro que pueda darse un elemento extranjero en la sucesión⁵⁰.

1. La repercusión transfronteriza de la sucesión

La finalidad principal del Derecho de sucesiones es definir las normas de adjudicación de la sucesión, así como regular la transmisión de la herencia. En

⁴⁹ U. García Jociles, "El Reglamento europeo 650/2012 y la tecnología: los *smart testaments*", *Derecom*, nº 30 (marzo-septiembre de 2021), pp. 77-89.

⁵⁰ J. Carrascosa González, "Reglamento sucesorio europeo y actividad notarial", *CDT*, 2014, nº 1, pp. 5-44; A. Rodríguez Benot, "La administración de la herencia en las sucesiones internacionales: especial referencia al derecho comunitario europeo", *Academia Sevillana del Notariado*, t. 19, 2009, pp. 253-304.

el espacio europeo de justicia, es imperativo que los ciudadanos puedan organizar su sucesión, en situaciones de sucesión *mortis causa* con repercusiones transfronterizas. En este contexto, debe observarse que el Reglamento 650/2012 se adoptó sobre la base del art. 81.2º TFUE, que se refiere únicamente a los asuntos civiles con repercusión transfronteriza. Por ello, se aplicará cuando se produzca una sucesión *mortis causa* con repercusión transfronteriza, como se desprende de sus considerandos 7 y 67.

Por tanto, se trata de ver si la sucesión internacional digital va a estar conectada o no con dos o más ordenamientos jurídicos, con independencia de la naturaleza, relevancia o intensidad del elemento extranjero⁵¹. Refiriéndonos a los datos, debe observarse que son elementos que se localizan en la nube, fundamentalmente, asociados a la tecnología, siendo destacable la no nacionalidad de ésta. Ahora bien, esto no significa que los servidores, en los que se ubican los datos, no la tengan, aunque este aspecto puede cambiar, en función a la temporalidad de éste.

Lo anterior nos lleva a la necesidad de ver la nacionalidad o residencia habitual del causante o a las mismas en relación con los legitimados o al lugar en el que están ubicados los datos. En este contexto, cabría afirmar que la naturaleza transfronteriza de la sucesión se verificaría cuando estuviesen vinculados con dos o más ordenamientos jurídicos nacionales de tal manera que surgiera la duda de cuál de ellos sería el reclamado para regularla. Para ello resultaría conveniente lo siguiente⁵²:

1ª En primer término el carácter transfronterizo podría derivar de un elemento endógeno de la situación (personal, objetivo o territorial), de un elemento exógeno a la misma, esto es, de la voluntad de los concernidos mediante la determinación como competente de una autoridad extranjera o como aplicable de un ordenamiento foráneo, todo ello para una situación en principio meramente interna.

2ª En segundo lugar se requeriría que el elemento extranjero presentase una mínima importancia hasta el punto de que su presencia en la situación justificase variar la respuesta legal prevista para supuestos internos⁵³. En

⁵¹ A-L. Calvo Caravaca y J. Carrascosa González, *Derecho internacional privado*, op. cit.

⁵² A. Rodríguez Benot (dir.), *Manual de derecho internacional privado*, 8ª ed., Madrid, Tecnos, 2021, p. 23.

⁵³ J.C. Fernández Rozas y S. Sánchez Lorenzo, *Derecho internacional privado*, 11ª ed, Cizur Menor, Civitas, 2020, p. 24. A ello ya se refirió J.A. Carrillo Salcedo señalando que no todo elemento extranjero convierte una situación en una manifestación de la vida internacional de las personas, pues lo que realmente importa es que “la finalidad social de los hechos reclame una reglamentación que corresponda a esa internacionalización” (*Derecho internacional privado*, 3ª ed., Madrid, Tecnos, 1983, p. 39).

esta línea podría entenderse la precisión final del considerando 7 del Reglamento cuando, tras referirse a la sucesión *mortis causa* con repercusiones transfronterizas requiere, se añade que “el espacio europeo de justicia es imperativo que los ciudadanos puedan organizar su sucesión. Es preciso garantizar de manera eficaz los derechos de los herederos y legatarios y de las personas próximas al causante, así como de los acreedores de la herencia”. En otros términos, la relevancia del elemento extranjero habría de estar calibrada por su impacto en el correcto desarrollo de las libertades comunitarias.

3ª Finalmente no sería preciso que el o los ordenamientos extranjeros vinculados con el supuesto en cuestión fuesen de un país cuyas autoridades aplicasen los Reglamentos; pudiendo también ser de un Estado de la Unión cuyas autoridades no lo aplicasen o de un Estado tercero cualquiera. Esta conclusión se observa, por un lado, porque el propio Reglamento nada restringen sobre este particular; y, de otro, produce eficacia universal o *erga omnes* al permitir aplicar, a través de sus preceptos, ordenamientos de cualesquiera de esos otros Estados (art. 20).

En lo que concierne a la llamada dimensión interna del Derecho internacional privado el Reglamento no obligan, aunque sí permite, a los Estados miembros que comprendan varias unidades territoriales con sus propias normas en materia de sucesiones a aplicarlos a los conflictos de leyes que se planteen entre dichas unidades territoriales exclusivamente (art. 36).

Dicho lo anterior, téngase en cuenta que la huella digital y activos mencionados anteriormente, en definitiva, son datos que están alojados en la nube. Dicho de otro modo, los datos van a tener un componente internacional intrínseco debido a que los datos con frecuencia son almacenados o transferidos entre servidores situados en diferentes países, donde cualquier interesado puede necesitar buscar y encontrar datos alojados en la nube en su formato original con una finalidad jurídica sucesoria, pero no solo serán los datos, sino también los metadatos y sus copias de seguridad. Téngase en cuenta, además, la ubicuidad para acceder a los mismos. Por ello, podríamos afirmar que van a tener un componente internacional, por su propia naturaleza, y a veces, podrá tener un componente interno, pero, a su vez, internacional⁵⁴.

⁵⁴ Cualquier usuario puede acceder a internet desde su propio Estado de residencia o desde otro, utilizando muy diversos dispositivos, los datos van a estar en uno o varios servidores, que puede estar en el mismo Estado u otros, pero los datos van a circular, por su propio carácter, de manera internacional.

Asimismo, cabría plantear, por ejemplo, posibilidades más complejas en las que un ciudadano español tenga patrimonio y residencia digital⁵⁵, empresa virtual incluida, por ejemplo, en Estonia. Otro supuesto sería, causante con nacionalidad española, domicilio en Andorra, donde tenga además su actividad profesional a través de aplicaciones web, en cualquier otro país, pero residencia digital fija en Estonia y, de otro, tendría su patrimonio digital en Estonia, o viceversa, entendiendo éste un último elemento de relevancia para la sucesión, distinto al de la residencia habitual del causante⁵⁶. Este hecho plantea semejanza con la casuística planteada en el considerando 24 donde se indica que “la residencia habitual del causante puede revelarse compleja. Tal sería el caso, en particular, cuando por motivos profesionales o económicos el causante hubiese trasladado su domicilio a otro país para trabajar en él, a veces por un período prolongado, pero hubiera mantenido un vínculo estrecho y estable con su Estado de origen”. En tal caso, dependiendo de las circunstancias, podría considerarse que el causante tenía su residencia habitual en su Estado de origen, donde

⁵⁵ El gobierno estonio aprobó, en 2014, la emisión de tarjetas de identificación inteligentes. Con ellas, los e-estonios (que no tienen que tener la nacionalidad de este país de la Unión Europea ni siquiera la residencia física en él), accederán a multitud de servicios online así como a la firma digital. Resulta especialmente interesante dos de sus características: 1) su obtención es voluntaria y abierta a todas las personas del mundo (no sólo de la Unión Europea); 2) No tiene en cuenta la residencia física ni la nacionalidad, puesto que la sociedad digital se mueve en otros parámetros y lo que en realidad se ofrece, por el Gobierno estonio, es la estructura digital a la que se puede acceder desde cualquier parte del mundo y los servicios que su utilización proporciona. De esta forma, “puede parecer atrevido, desde postulados propios de un Segundo entorno (sociedad industrial), pero desde el tercer entorno (espacio virtual), en el que las relaciones aparecen mediadas tecnológicamente, la residencia digital pudiera ser un criterio a tener en cuenta” (M.P. Diago Diago, “La residencia digital como nuevo factor de vinculación en el Derecho internacional privado del Ciberespacio ¿posible conexión de futuro?”, *Diario La Ley*, nº 8432 (1 de diciembre de 2014). El servicio está dirigido, principalmente, a aquellos que ya tienen vínculos con Estonia, ya sea a través de negocios, estudios o por turismo. Se trata de plataforma que proporciona y utiliza servicios digitales en todo el mundo. Con ello, se espera que el e-residente atraiga a nuevos clientes a los servicios digitales de Estonia. (A. Cuthbertson, “Estonia First Country to Offer E-Residency Digital”, *International Business Times*, 2014). Por otro lado, habrá que tener en cuenta que cuando hacemos referencia a la residencia digital va a resultar importante referirnos a la identidad electrónica, que se compone, entre otras cosas, de una e-Identidad fundacional (otorgada por el propio Estado, vinculada a su residencia habitual) y una e-Identidad funcional (otorgada por la propia entidad, que actuará dentro de la transacción y, por tanto, va a vincular a la persona con su patrimonio digital). Algo parecido puede utilizarse para ubicar a los servidores y empresas virtuales (En relación a la residencia digital y la identidad electrónica véase A. Merchán Murillo “La identidad electrónica como elemento fundamental del contrato”, *Revista Aranzadi de derecho y nuevas tecnologías*, nº. 47, 2018 y “Cuestiones esenciales en torno a la identidad electrónica”, *La Ley: mercantil*, nº. 42 (diciembre), 2017).

⁵⁶ Conclusiones del Abogado General Sra. M. Campos Sánchez-Bordona, presentadas el 26 de marzo de 2020, E. E. con intervención de: Kauno miesto 4-ojo notaro biuro notarė Virginija Jarienė, K-D. E. C-80/19, ECLI:EU:C:2020:230, ap. 34.

se aprecia que la residencia habitual del causante debe fijarse, por la autoridad que sustancie la sucesión, mediante la evaluación del conjunto de las circunstancias del caso, en un solo Estado miembro⁵⁷. Por tanto, en observancia de los supuestos planteados resulta clara que la sucesión mortis casusa tendría una marcada la repercusión transfronteriza⁵⁸.

De esta forma puede observarse que el elemento extranjero presente en la sucesión *mortis causa* podrá ser de distinto tipo, clase o naturaleza y puede referirse a distintos aspectos de la sucesión, ya sea porque el causante posea nacionalidad extranjera y reside habitualmente en otro país, o bien porque todos o parte de los bienes del causante se encuentran en otro Estado o si los herederos, legatarios o beneficiarios poseen nacionalidad extranjera o residen en otro país⁵⁹.

2. La propiedad digital dentro del Reglamento sucesorio

Una vez determinada la repercusión transfronteriza de la sucesión resultará relevante, para la aplicación del Reglamento, observar si nos encontramos dentro de las definiciones del art. 3 del Reglamento. Se trata de identificar si el patrimonio digital entra dentro de las definiciones de éste⁶⁰.

De esta forma, a modo de ejemplo, podría ser útil citar lo que podría encuadrarse dentro del patrimonio digital del causante⁶¹: nombres de redes inalámbricas y contraseñas, programas financieros como Quicken o cuentas de suscripción de software en línea, como Adobe Cloud, información para indicar cómo y dónde se organizan los archivos en un ordenador y otros dispositivos de almacenamiento, redes sociales, contraseñas de gestión de la reputación en línea en redes sociales (por ejemplo, Facebook o ¿qué pasó con Tuenti?) o profesionales((por ejemplo, LinkedIn), el uso compartido de

⁵⁷ V. Bumbaca, "CJEU on the deceased's habitual residence", *Conflict of Laws.net*, 30 de julio de 2020. Puede consultarse en [<https://conflictoflaws.net/2020/cjeu-on-the-deceaseds-habitual-residence/>] (Fecha de consulta 5 de julio de 2021).

⁵⁸ A este respecto, cabría tener en cuenta que, aunque el causante no haga uso de la facultad de elección, si reside habitualmente en un país distinto del correspondiente a su nacionalidad, la sucesión es ya de por sí "internacional". Al respecto, véase en este punto la Sentencia del TJUE, de 16 de julio de 2020, E. E. con intervención de Kauno miesto 4-ojo notaro biuro notarė Virginija Jarienė, as. 80/19 (ECLI:EU:C:2020:569).

⁵⁹ J. Carrascosa, *El Reglamento sucesorio europeo: análisis crítico*, 2ª, Madrid, Ed. Rapid Centro, 2019, p. 69.

⁶⁰ A. Ripoll Soler, "Hacia un nuevo modelo de planificación sucesoria notarial: la *professio iuris*", *Revista de Derecho Civil*, V. III, nº 2, abril-junio 2016, pp. 44-47.

⁶¹ A. Ybarra Bores, "La sucesión *mortis causa* de ciudadanos ingleses residentes en España: problemas y nuevas perspectivas", *CDT*, vol. 7, nº 1, 2015, pp. 226-254; *id.*, *La sucesión mortis causa de ciudadanos británicos en España*, Valencia, Tirant lo Blanch, 2021, p. 35.

fotos y video, transmisión y uso compartido de música (por ejemplo, Spotify), tiendas de aplicaciones o entretenimiento en línea y de medios (por ejemplo, Netflix, iTunes, Google Play o la tienda de aplicaciones de Windows), cuestiones relacionadas con la presencia en línea o la marca personal (por ejemplo, cualquier sitio web y blogs, sitios de comercio en línea, si tiene un negocio en línea), las copia de seguridad y almacenamiento de archivos en línea (por ejemplo, Dropbox y Google Drive), comercio en línea (por ejemplo, Amazon o eBay), además de cualquier suscripción digital a periódicos locales o nacionales o revistas en línea. Pensemos en juegos en línea o mundos virtuales (v.gr., World of Warcraft, Second Life), cuentas de correo electrónico, cuentas de estudiantes y bibliotecas, cuentas de facturas de servicios públicos que se pagan en línea, cuentas relacionadas con viajes (por ejemplo, cuentas de planificación de viajes, así como programas de fidelización).

En este contexto, puede decirse que el Reglamento sucesorio incide en el Derecho de propiedad estableciendo normas de carácter material y conceptos patrimoniales autónomos. Las de carácter material se refieren a soluciones concretas, las otras integran tanto definiciones como nociones en el contexto del Reglamento (heredero, legatario, ejecutor, entrega de bienes, pagos...) teniendo presente que los conceptos utilizados en los instrumentos de la Unión se han de definir de forma uniforme e independientemente de los Derechos nacionales, pero en este instrumento. Entre los conceptos autónomos que el Reglamento establece destaca el de sucesión *mortis causa*, con en el Derecho patrimonial⁶².

La configuración del Derecho de propiedad, genéricamente considerado, se encuentra excluido de los Tratados, como puede observarse en el art. 345 TFUE al indicar que “Los Tratados no prejuzgan en modo alguno el régimen de la propiedad en los Estados miembros”. Ahora bien, el Reglamento sucesorio, establece un concepto de sucesión *mortis causa*, que genera la creación o transmisión de propiedad. De una parte, el art. 1.1º dice, simplemente, que el Reglamento se aplica a la sucesión *mortis causa*⁶³. El art. 3 define la sucesión por causa de muerte abarcando cualquier forma de transmisión *mortis causa* de bienes, derechos y obligaciones, ya derivé de un acto voluntario en virtud de una disposición *mortis causa* o de una sucesión abintestato⁶⁴. A este respecto, puede observarse el considerando 9.

De esta suerte, en torno a la sucesión por causa de muerte, relacionando los arts. 1.1º (“El presente Reglamento se aplicará a las sucesiones por causa

⁶² A. Fernández-Tresguerres García, *Las sucesiones “mortis causa” en Europa: aplicación del Reglamento (UE) n° 650/2012*, Cizur Menor, Aranzadi, 2016, pp. 93–94.

⁶³ A. Bonomi y P. Wautelet, *El Derecho Europeo de Sucesiones. Comentario al Reglamento (UE) n° 650/2012, de 4 de julio de 2012*, Cizur Menor, Aranzadi, 2015, p. 177.

⁶⁴ A. Fernández-Tresguerres García, *Las sucesiones mortis causa...*, *op. cit.*

de muerte. No será aplicable a las cuestiones fiscales, aduaneras y administrativas.”), 3.1.a) (“A los efectos del presente Reglamento, se entenderá por: a) «sucesión»: la sucesión por causa de muerte, abarcando cualquier forma de transmisión *mortis causa* de bienes, derechos y obligaciones, ya derive de un acto voluntario en virtud de una disposición *mortis causa* o de una sucesión abintestato”) y 23.e) (“1. La ley determinada en virtud de los arts. 21 o 22 regirá la totalidad de la sucesión. 2. Dicha ley regirá, en particular: e) la transmisión a los herederos y, en su caso, a los legatarios, de los bienes, derechos y obligaciones que integren la herencia, incluidas las condiciones y los efectos de la aceptación o renuncia de la herencia o del legado), junto al considerando 42 (“La ley determinada como aplicable a la sucesión debe regir la sucesión desde la apertura de la misma hasta la transmisión a los beneficiarios de la propiedad de los bienes y derechos que integren la herencia tal como establece esa ley”), se puede observar el concepto de propiedad sucesoria.

En virtud de lo anterior, en conjunción con los principios de equivalencia funcional (el patrimonio digital equivale al patrimonio material, no debiendo ser discriminados aquel respecto de cualquier otro tipo de manifestación) e inalterabilidad del derecho preexistente (es decir, mismos efectos jurídicos dentro del mismo marco normativo existente)⁶⁵, permitiría situar dentro de del Reglamento sucesorio la propiedad digital sucesoria, basada en la transmisión *mortis causa*.

Ahora bien, esto no significa no esté sujeta a problemática, pues la aplicación sucesoria a la transmisión de los derechos a los herederos y beneficiarios puede tener como consecuencia⁶⁶ que al ser investido como tal es posible que no pueda serle atribuido en base a la ley del Estado del lugar de situación de la propiedad digital.

3. El certificado sucesorio europeo

En este apartado, nuestra intención es determinar el posible uso del certificado sucesorio europeo en la materia que está siendo objeto de estudio. Siendo conscientes de que este apartado conlleva la necesidad una mayor profundidad, haremos hincapié en una serie de cuestiones, que serán fundamentales para trabajos venideros. De esta forma, siguiendo al Profesor Carrascosa⁶⁷ puede decirse que el certificado sucesorio europeo no tiene una definición legal. No obstante, siguiendo sus elementos característicos

⁶⁵ R. Illescas Ortiz, *Derecho de la contratación electrónica*, 3ª ed., Cizur Menor, Thomson Reuters, 2019, pp. 43 y 52.

⁶⁶ A. Bonomi y P. Wautelet, *El derecho europeo...*, op. cit.

⁶⁷ J. Carrascosa, *El Reglamento sucesorio europeo...*, op. cit.

previstos en el Reglamento se puede determinar que es aquel documento oficial que acredita la cualidad de heredero, legatario, ejecutor testamentario o administrador de la herencia y que puede ser utilizado por dichos sujetos para invocar, en otro Estado miembro, su cualidad de tales o para ejercer sus derechos como tales.

De esta completa definición resulta obvio el carácter probatorio del certificado sucesorio, así como quién puede instar su expedición, su finalidad y efectos, lo que se puede observar también en los arts. 63 y 69 del Reglamento. En relación a quién puede utilizar el certificado y con qué finalidad hablamos de “los herederos, legatarios que tengan derechos directos en la herencia y ejecutores testamentarios o administradores de la herencia que necesiten invocar, en otro Estado miembro, su cualidad de tales o ejercer sus derechos como herederos o legatarios, o bien sus facultades como ejecutores testamentarios o administradores de la herencia” (art. 63.1º).

El carácter probatorio aparece reflejado en el art. 63.2º donde pueden observarse algunos ejemplos⁶⁸ probatorios, como la cualidad de heredero o legatario y la atribución de bienes, entiéndase con ello también de los bienes digitales. Este efecto probatorio, de la cualidad y de la atribución, han de relacionarse con los efectos del art. 69, que a su vez deben unirse a las cuestiones sucesorias que conforme al art. 23 se regirán por la ley sucesoria.

Respecto a los efectos habrá que tenerse en cuenta el art. 69 junto con el considerando 71 que no dice que “el certificado debe surtir los mismos efectos en todos los Estados miembros. No debe ser un título con fuerza ejecutiva por sí mismo, pero debe tener efecto probatorio y se ha de presumir que demuestra de manera fidedigna elementos que han quedado acreditados de conformidad con la ley aplicable a la sucesión o con cualquier otra ley aplicable a elementos específicos, tales como la validez material de las disposiciones *mortis causa*”. Junto a esto debe tenerse en cuenta que el certificado sucesorio no acredita la propiedad de los bienes hereditarios, ya que no constituye un título de propiedad⁶⁹.

⁶⁸ Ya que puede certificarse, por ejemplo, la ley aplicable que conduzca a la finalidad expresada, tal y como puede verse en el art. 69.2º *ab initio* y en el formulario V del Reglamento de ejecución (UE) no 1329/2014 de la Comisión de 9 de diciembre de 2014 por el que se establecen los formularios mencionados en el Reglamento (UE) nº 650/2012 del Parlamento Europeo y del Consejo relativo a la competencia, la ley aplicable, el reconocimiento y la ejecución de las resoluciones, a la aceptación y la ejecución de los documentos públicos en materia de sucesiones *mortis causa* y a la creación de un certificado sucesorio europeo.

⁶⁹ I. Anton Juárez, “Certificado sucesorio europeo”, en A.-L. Caravaca y J. Carrascosa Gonzalez (dirs.) *Litigación Internacional en la Unión Europea (IV). Comentario al Reglamento 650/2012 del Parlamento europeo y del Consejo sobre sucesiones mortis causa*, Cizur Menor, Aranzadi, 2019, pp. 313–360.

De lo anterior, se denota que el certificado sucesorio participa de la acreditación del *iter sucesorio*, pero no va a constituir certeza en la existencia de la propiedad digital, lo que conllevará necesaria indagación por la autoridad emisora de las declaraciones y demás documentos presentados por el solicitante, que no estará exenta de problemática.

VII. CONCLUSIONES

No es fácil hablar de la muerte. A nadie le gusta recordar su propia mortalidad, pero la muerte es algo a lo que todos enfrentamos y, aunque, es posible que no se pueda controlar, si se puede controlar, a veces, lo que se deja atrás. Por adoptar una postura proactiva, puede asegurarse, con la problemática manifestada, que existe patrimonio digital y, por tanto, propiedad digital, lo que nos permite hablar de que hay objeto digital de la sucesión. La determinación no está exenta de problemática ni discusión jurídica, ni tampoco hay garantía de que, a pesar de establecer la voluntad de uno, en relación con el patrimonio digital, se vaya a llevar a cabo.

Al observarse la existencia de este patrimonio digital, se ha observado como la misma puede entrar dentro de la aplicación del Reglamento sucesorio; pues, como se ha observado, tiene una repercusión transfronteriza, entra dentro de las definiciones del art. 3 y, a su vez, podrá usarse el certificado sucesorio para la acreditación de *iter sucesorio*.

La repercusión transfronteriza puede observarse en que el elemento extranjero presente en la sucesión *mortis causa* podrá ser de distinto tipo, clase o naturaleza y puede referirse a distintos aspectos de la sucesión, ya sea porque el causante posea nacionalidad extranjera y reside habitualmente en otro país. Asimismo, puede advertirse la que la propiedad digital sucesoria, basada en la transmisión *mortis causa*, aunque esto no significa no esté sujeta a problemática. Finalmente, como decimos, el certificado sucesorio participa de la acreditación del *iter sucesorio*, del patrimonio digital, pero no constituye certeza en la existencia de la propiedad digital, lo que conllevará necesaria indagación por la autoridad competente.

BIBLIOGRAFÍA

- Anton Juarez, I.: "Certificado sucesorio europeo", en A.-L. Caravaca y J. Carrascosa Gonzalez (dirs.) *Litigación Internacional en la Unión Europea (IV). Comentario al Reglamento 650/2012 del Parlamento europeo y del Consejo sobre sucesiones mortis causa*, Cizur Menor, Aranzadi, 2019, pp. 313–360.

- Aziz, A., Telang, R.: "What Is a Digital Cookie Worth?", *SSRN*, marzo, 2016, pp. 3–37.
- Bartolini, C., Santos, C. y Ullrich, C.: "Property and the cloud", *Computer Law & Security Review*, nº 2, abril, 2018, pp. 358–390.
- Bonomi, A. y Wautelet, P.: *El Derecho Europeo de Sucesiones. Comentario al Reglamento (UE) N° 650/2012, de 4 de Julio de 2012*, Cizur Menor, Aranzadi, 2015
- Bumbaca, V.: "CJEU on the deceased's habitual residence", *Conflicto f Laws.net*, 30 de julio de 2020.
- Calvo Caravaca, A-L. y Carrascosa González, J.: *Derecho Internacional Privado*, vol. II, 18ª Granada, Comares, 2018.
- Cámara Lapuente, S.: *La sucesión mortis causa en el patrimonio digital: una aproximación*, conferencia dictada en el colegio notarial de Madrid, salón académico, el 24 de enero de 2019.
- Cámara Lapuente, S.: "La sucesión *mortis causa* en el patrimonio digital: una aproximación", *El Notario del Siglo XXI*, nº 84, marzo-abril, 2019, pp.138–144.
- Cámara Lapuente, S.: "La sucesión *mortis causa* en el patrimonio digital", *Anales de la Academia Matritense del Notariado*, 2019, pp. 375–432.
- Carrascosa González, J.: "Reglamento sucesorio europeo y actividad notarial", *CDT*, nº 1, 2014, pp. 5–44.
- Carrascosa, J.: *El Reglamento sucesorio europeo: análisis crítico*, 2ª ed., Madrid, Rapid Centro, 2019, p. 69.
- Carrillo Pozo, L. F.: "Una síntesis del Reglamento 650/2012: residencia habitual del *de cuius*, funciones judiciales, *professio iuris*. Comentario a la sentencia del tribunal de justicia (sala primera) de 16 de julio de 2020, Asunto C-80/19", *CDT*, marzo 2021, vol. 13, nº 1, pp. 755–766.
- Cerrillo I Martinez, A.: "How do we provide the digital footprint with eternal rest? Some criteria for legislation regulating digital wills", *Computer Law & Security Review*, vol. 34, nº 5 2018, pp. 1119–1130.
- CNUDMI/UNCITRAL: Propuesta del Gobierno del Canadá: posible labor futura en materia de comercio electrónico: cuestiones jurídicas que afectan a la informática "en la nube", Nueva York, 7 a 18 de julio de 2014.
- CNUDMI/UNICTRAL: *Aspectos contractuales de la computación en la nube*, Nueva York, 24 a 28 de abril de 2017.
- Cuerva de Cañas, J. A.: "La propiedad intelectual en el mundo digital", en *Sociedad Digital y Derecho* (T. de la Quadra-Salcedo y Fernández del Castillo (dir.), J.L. Piñar Mañas (aut.), Ministerio de Industria, Comercio y Turismo, 2018, pp. 719–740.
- Cuthbertson, A.: "Estonia First Country to Offer EResidency Digital", *International Business Times*, 2014.
- De Miguel Asensio, P. A.: "Mercado único digital y propiedad intelectual: las Directivas 2019/789 y 2019/790", *La Ley: Unión Europea*, nº 71, 2019.
- Diago Diago, M.P.: "La residencia digital como nuevo factor de vinculación en el Derecho Internacional Privado del Ciberespacio ¿posible conexión de futuro ?", *Diario La Ley*, nº 8432.

- Díaz-Noci, J.: "Intellectual property and transmedia informative products: A comparative, transnational legal análisis", *Hipertext.net: Revista Académica sobre Documentación Digital y Comunicación Interactiva*, nº 20, 2020.
- Edwards, E. y Harbinja, E.: "What happens to my Facebook profile when I die? Legal Issues Around Transmission of Digital Assets on Death", *CREATE Working Paper*, nº 5, 2013, pp. 1-25.
- Fernández-Tresguerres García, A.: *Las sucesiones "mortis causa" en Europa: aplicación del Reglamento (UE) nº 650/2012*, Cizur Menor, Aranzadi, 2016, pp. 93-94.
- Fosch Villaronga E., Kieseberg y P., Li, T.: "Humans forget, machines remember: Artificial intelligence and the Right to Be Forgotten", *Computer Law & Security Review*, vol. 34, nº 2, 2018, pp. 304-313.
- García Jociles, U.: "El Reglamento europeo 650/2012 y la tecnología: los *smart testaments*", *Derecom*, nº 30 (marzo-septiembre de 2021), pp. 77-89.
- Garriga Domínguez, A.: *Nuevos retos para la protección de datos personales en la era de las big data y de la computación ubicua*, Madrid, Dykinson, 2016.
- Illescas Ortiz, R.: *Derecho de la contratación electrónica*, 3ª ed., Cizur Menor, Thomson Reuters, 2019.
- Janeček, V.: "Ownership of personal data in the Internet of Things", *Computer Law & Security Review*, nº 34, 2018, pp. 1039-1052.
- Lehmann, M.: "The Court of Justice on the Succession Regulation: Matthias Lehmann on the E.E. Case", *The European Association of Private International Law*, 21 de octubre de 2020.
- Madrid Parra, A.: "Aspectos jurídicos de la identificación en el comercio electrónico", en *Derecho del comercio electrónico. (primeras jornadas celebradas en la Universidad Carlos III de Madrid)* (Coord. I. Ramos Herranz; Rafael Illescas Ortiz (Dir.), La Ley, 2001.
- Madrid Parra, A.: "La identificación electrónica", *Revista de la Contratación Electrónica*, nº 15, 2001, pp. 5-61.
- Mccallig, D.: "Private but eventually public: why copyright in unpublished works matters in the digital age", *SCRIPTed J Law Technol Soc*, nº 20, 2013, pp. 39-56.
- Mcewen, A. y Cassimally, H.: *Internet de las cosas. La tecnología revolucionaria que todo lo conecta*, Madrid, Anaya Multimedia, 2014.
- Merchán Murillo, A.: *Firma electrónica: Funciones y problemática: especial referencia al Reglamento (UE) nº 910/2014, relativo a la identificación electrónica por la que se deroga la Directiva 1999/93/CE de firma electrónica*, Cizur Menor, Aranzadi, 2016.
- Merchán Murillo, A.: "Cuestiones esenciales en torno a la identidad electrónica", *La Ley: mercantil*, nº. 42, diciembre, 2017.
- Merchán Murillo, A.: "La identidad electrónica como elemento fundamental del contrato", *Revista Aranzadi de derecho y nuevas tecnologías*, nº. 47, 2018.
- Moralejo Imbernón, N.: "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", *ADC*, t. LXXIII, 2020, fasc. I, pp. 241-281.
- OCDE: "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value", *OECD Digital Economy Papers*, nº 220.

- Osborne Clarke LLP: *Legal study on ownership and access to data (European Commission 2016)*.
- Pabón Cadavid, J.: "Protección legal a los metadatos y la gestión digital de los derechos de autor", *Ius et Praxis*, vol. 26, nº 1, 2020, pp. 57-76.
- Prins, J.E.J.: "The propertization of personal data and identities", *Electronic Journal of Comparative Law*, nº 8, 2004, pp. 3-25.
- Ripoll Soler, A.: "Hacia un nuevo modelo de planificación sucesoria notarial: la *professio iuris*", *Revista de Derecho Civil*, V. III, nº 2, abril-junio 2016, pp. 44-47.
- Rodríguez Benot, A.: "La administración de la herencia en las sucesiones internacionales: especial referencia al derecho comunitario europeo", *Academia Sevillana del Notariado*, t. 19, 2009, pp. 253-304.
- Rodríguez Benot, A.: "El ordenamiento aplicable a la sucesión mortis causa en el sistema español de Derecho internacional privado", *Academia Sevillana del Notariado*, t. 27, 2016, pp. 75-96.
- Rodríguez Benot, A.: "El ordenamiento aplicable a la sucesión mortis causa en el sistema español de Derecho Internacional Privado", *Derecho y fiscalidad de las sucesiones "mortis causa" en España: una perspectiva multidisciplinar* (coord. Jesús Ramos Prieto), Cizur Menor, Aranzadi Thomson Reuters, 2016,
- Rodríguez Benot, A.: "Ley aplicable a la sucesión por causa de muerte en el Reglamento de la Unión Europea 650/2012: especial referencia a la legítima", en *Derecho sucesorio comparado: las experiencias española y mexicana en un contexto internacional* (coord. por César Hornero Méndez, Alfonso Ybarra Bores, Nuria González Martín, Elí Rodríguez Martínez), Valencia, Tirant lo Blanch, 2019.
- Rodríguez Benot, A.: *Manual de Derecho Internacional Privado*, 8ª ed., Madrid, Tecnos, 2021.
- Santos Morón, M.J.: "La denominada "herencia digital": ¿necesidad de regulación? estudio de Derecho español y comparado", *CDT*, vol. 10, nº 1, 2018, pp. 413-438.
- Steel, E., Locke, C. y Cadman, E.: "How much is your personal data worth?", *Financial Times*, 2017.
- Steinmetz, K.: "Your Digital Legacy: States Grapple with Protecting Our Data After We Die", *Time*, noviembre, 2012.
- Sullivan, C.: "Digital identity. From emergent legal concept to new reality", *Computer Law & Security Review*, vol. 34, nº 4, 2018, pp. 723-731.
- Sullivan, C.: "Protecting digital identity in the cloud: Regulating cross border data disclosure", *Computer Law & Security Review*, vol. 30, nº 2, abril 2017, pp. 137-152.
- Sulzberger, A. G.: "How the Times Thinks About Privacy", *New York Times*, 2019.
- Watkins, F.: "Digital Properties and Death: What Will Your Heirs Have Access to after You Die?", *Buff. L. Rev.*, 2014, pp. 193-235.
- Ybarra Bores, A.: "La sucesión *mortis causa* de ciudadanos ingleses residentes en España: problemas y nuevas perspectivas", *CDT*, vol. 7, nº 1, 2015, pp. 226-254.
- Ybarra Bores, A., *La sucesión mortis causa de ciudadanos británicos en España*, Valencia, Tirant lo Blanch, 2021.

