El nuevo derecho a la portabilidad de los datos personales en el Reglamento (UE) 2016/679, de 27 de abril de 2016

The new right to personal data portability in Regulation (EU) 2016/679 of 27 April 2016

por

RICARDO PAZOS CASTRO
*Profesor ayudante Doctor de Derecho civil**
Universidad Autónoma de Madrid

RESUMEN: Este trabajo analiza el derecho a la portabilidad reconocido por el artículo 20 del Reglamento general de protección de datos, a saber, un derecho a recibir determinados datos personales en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos —o a que sean transmitidos directamente— a un tercero. Para ello se examinan diferentes cuestiones, siendo las principales el concepto de datos personales y la delimitación de cuáles son susceptibles de portabilidad, las condiciones previas para que el interesado ostente el derecho, el contenido de este, y

* Tanto la investigación previa como la redacción de este trabajo fueron llevadas a cabo cuando el autor era investigador posdoctoral en la Universidad de Santiago de Compostela, disfrutando de una beca en el marco del *Programa de axudas á etapa posdoutoral da Xunta de Galicia (Consellería de Cultura, Educación e Ordenación Universitaria)*.

los límites a los que está sometido. Posteriormente, se abordan tanto los objetivos y beneficios del derecho a la portabilidad de los datos, como sus debilidades y potenciales efectos colaterales negativos.

ABSTRACT: This paper examines the right to portability granted in article 20 of the General Data Protection Regulation, namely a right to receive certain personal data in a structured, commonly used and machine-readable format, and transmit them—or have them transmitted directly—to a third party. Several issues are considered, the main ones being the notion of personal data and defining which of them are portable, the preconditions for the data subject to enjoy the right, the content of the right, and the limits it is affected by. Afterwards, the goals and benefits of the right to data portability, as well as its weaknesses and potentially negative side-effects, are addressed.

PALABRAS CLAVE: Datos personales. Protección de datos. Derecho a la portabilidad de los datos. Derechos digitales. Efecto cerrojo. RGPD.

KEY WORDS: Personal data. Data protection. Right to data portability. Digital rights. Lock-in effect. GDPR.

I. INTRODUCCIÓN

«Los datos se han convertido en un recurso esencial para el crecimiento económico, la creación de empleo y el progreso social». Así comienza la Comunicación de la Comisión Europea de 10 de enero de 2017 *La construcción de una economía de los datos europea*. En efecto, la información se está convirtiendo, si no lo es ya, en el combustible de la economía mundial. Antes de la explosión digital, ya se explicó que la vida económica se basaba en solucionar problemas informativos: la actividad económica humana es la coordinación de múltiples agentes que actúan con base en una información descentralizada, incompleta, contradictoria y en constante cambio (HAYEK, 1945, 519-520). Siendo así, una mayor recopilación, análisis y utilización de la información facilitará el crecimiento económico (GRAEF *et al.,* 2018, 1361). Poniendo en valor la información como recurso esencial en la economía moderna, se alude a «cuatro V» que permiten caracterizar al *Big Data*: volumen (de datos), variedad (de fuentes), velocidad (de análisis) y veracidad (de la información resultante del proceso de análisis) (ZARSKY, 2017, 998-999).

Sin embargo, las nuevas tecnologías también comportan riesgos para la protección de datos personales, así como, en general, para la intimidad y la vida privada. En este contexto, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en adelante, Reglamento general de protección de datos o RGPD)[1], aplicable desde el 25 de mayo de 2018, se ha erigido como un pilar central para paliar los riesgos mencionados y generar la confianza digital que haga posible el desarrollo de la economía de la información[2].

La protección de datos personales es un tema que merece un profundo estudio en el momento actual. La razón es que se trata de un derecho, reconocido tanto en el artículo 16 del Tratado de Funcionamiento de la Unión Europea (TFUE)[3] como en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea[4], que cuenta con una gran relevancia en el ámbito económico y en el desarrollo de las nuevas tecnologías. El presente trabajo pretende contribuir a ese estudio, centrándose en el derecho a la portabilidad previsto en el artículo 20 del RGPD.

La exposición se estructura de la siguiente manera. El apartado II encuadra el derecho a la portabilidad de los datos personales en su contexto regulatorio europeo y español. Para ello se hace una presentación sucinta del Reglamento general de protección de datos y de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (en adelante, LOPDGDD)[5]. El apartado III se centra en el régimen

del derecho a la portabilidad de los datos tal y como ha sido establecido en el Reglamento europeo, analizando la noción de datos personales, las condiciones que deben cumplirse para que haya lugar al derecho estudiado, el contenido de este, sus límites, y otras cuestiones relacionadas. Finalmente, en el apartado IV se exponen los objetivos perseguidos mediante el reconocimiento del derecho a la portabilidad y los beneficios que de él se derivan, así como algunas de sus debilidades y problemas que podrían generarse.

II. LA NUEVA NORMATIVA EUROPEA Y ESPAÑOLA EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

1. El Reglamento general de protección de datos

La Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante, Directiva sobre datos personales)[6], marcó en su momento un notable avance a nivel europeo. Texto de armonización máxima[7], garantizaba un nivel elevado de protección al mismo tiempo que la libre circulación de los datos personales en la Unión Europea (art. 1). Sin embargo, la armonización plena no impedía la pervivencia de una fragmentación normativa a nivel europeo, lo que afectaba a la seguridad jurídica (REDING, 2012, 120-121; ZANFIR, 2012, 150 y 153). Además, las nuevas tecnologías avanzaron rápidamente desde su aprobación, apareciendo desafíos que no podían ser resueltos de manera enteramente satisfactoria, lo que recomendaba una revisión del marco jurídico.

Este es el contexto en el que se aprobó el Reglamento general de protección de datos, cuyo artículo 1 indica que se pretende —al igual que en su momento la Directiva— garantizar tanto el derecho a la protección de datos personales como la libre circulación de estos. Pese a la coincidencia de fines, se observa un cambio en cuanto al fundamento de la normativa. La Directiva se basaba en el artículo 100 A del Tratado constitutivo de la Comunidad Europea[8], que incidía en el mercado interior, mientras que el Reglamento lo hace en el artículo 16 del TFUE, precepto que, como ya se ha dicho, reconoce el derecho a la protección de datos. Hay quien menciona un tercer objetivo del Reglamento, no proclamado expresamente en el texto articulado, consistente en establecer una visión europea de la protección de datos que refuerce la posición de la Unión en la escena internacional (DESGENS-PASANAU, 2018, 6-7).

La opinión mayoritaria con respecto al Reglamento es positiva, sobre todo en Europa. Resulta innecesario citar aquí autores que lo ilustren, siendo

el hecho notorio y sirviendo para ello muchos de los trabajos mencionados en la bibliografía. Más interesante parece constatar la existencia de algunas opiniones disidentes (ZARSKY, 2017; GEUTER, 2018; DOWNES, 2018b; RADIA y KHURANA, 2018; YARAGHI, 2018). Cabe destacar aquella según la cual el célebre escándalo de *Cambridge Analytica* no constituye un argumento a favor de la necesidad de un texto tan amplio y complejo como el Reglamento, sino todo lo contrario. Precisamente, el hecho de que se produjese un escándalo que desembocó en el cierre de la empresa afectada, el daño reputacional sufrido por Facebook —y la caída del valor en bolsa de sus acciones—, y la mayor concienciación de la sociedad con la protección de datos, reflejarían que los efectos disuasorios del mercado son más fuertes de lo que se piensa; de modo que sería suficiente con un marco legal más bien genérico que protegiese a los usuarios contra *hackers*, transferencias ilícitas de datos y otros peligros mayores (EPSTEIN, 2018).

El capítulo III del Reglamento general de protección de datos reconoce diferentes derechos a los «interesados», concepto definido indirectamente en el artículo 4.1) del texto —este precepto contiene en realidad la definición de datos personales— como «personas físicas identificadas o identificables». Son los derechos a la transparencia y a obtener cierta información (arts. 12 a 14), de acceso (art. 15), de rectificación (art. 16), de supresión-derecho al olvido (art. 17), a la limitación del tratamiento de datos (art. 18), a la portabilidad de los datos (art. 20), de oposición (art. 21), y a no ser objeto de una decisión basada únicamente en el tratamiento automatizado (art. 22). Se trata en algunos casos de una actualización de derechos clásicos, otros, como el derecho a no ser objeto de una decisión basada en el tratamiento, parecen adquirir una mayor autonomía, y otros constituyen una novedad, como sucede con el derecho a la portabilidad de los datos personales.

2. La Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, moderniza la normativa española adaptándola a un entorno digital, completando las disposiciones del Reglamento general de protección de datos. Este último es extenso y por su propia naturaleza pretende una unificación legislativa, pero se sirve de cláusulas abiertas y de normas amplias que dejan espacio tanto a la interpretación como al desarrollo por parte de los Estados miembros, incluyendo también numerosas remisiones a los ordenamientos nacionales. Baste un ejemplo. El artículo 8.1 del RGPD establece en dieciséis años la edad para prestar válidamente el consentimiento para el tratamiento

de datos personales con base en su artículo 6.1.a), pero permite que los Estados miembros fijen una edad inferior, con un límite de trece años. La ley española ha reducido hasta los catorce años esa edad (art. 7.1 de la LOPDGDD), mientras que en Francia ha quedado establecida en quince (art. 45 de la Ley núm. 78-17, de 6 de enero de 1978, sobre Informática, Archivos y Libertades[9]).

Desde el punto de vista de los derechos individuales, en la ley española destacan por un lado sus artículos 11 a 18, dedicados precisamente a los derechos de las personas; y, por otro, los artículos 79 a 96, que reconocen una serie de derechos digitales[10]. En cuanto al derecho a la portabilidad de los datos personales, el artículo 17 de la LOPDGDD establece que se ejercerá de acuerdo con lo dispuesto en el artículo 20 del Reglamento europeo. Por otro lado, el artículo 95 de la LOPDGDD reconoce a los usuarios de servicios de redes sociales y servicios de la sociedad de la información equivalentes un derecho de portabilidad, es decir, «a recibir y transmitir los *contenidos* que hubieran facilitado a los prestadores de dichos servicios, así como a que los prestadores los transmitan directamente a otro prestador designado por el usuario, siempre que sea técnicamente posible» (énfasis añadido). Los prestadores de los servicios referidos pueden conservar una copia de los contenidos cuando ello sea necesario para cumplir con una obligación legal, sin que ello les permita difundirlos a través de Internet.

Otro precepto relacionado con el derecho a la portabilidad de los datos personales es el artículo 4 de la LOPDGDD. Tras proclamar que los datos deben ser exactos y, de ser necesario, actualizados (apdo. 1), dispone que al responsable del tratamiento no le será imputable su inexactitud en ciertos supuestos, siempre que haya adoptado todas las medidas razonables para su supresión o rectificación sin dilación (apdo. 2). Uno de tales supuestos, concretamente el previsto en la letra c), es que el tratamiento de datos se efectúe tras haberlos recibido de otro responsable, por haber ejercido el interesado su derecho a la portabilidad.

Tampoco pueden obviarse las disposiciones sobre infracciones. Una vulneración sustancial del derecho a la portabilidad, en particular impidiéndolo, obstaculizándolo o ignorando reiteradamente las solicitudes de los usuarios, constituye una infracción muy grave que prescribirá a los tres años [art. 72.1.k) de la LOPDGDD]. En tratamientos que no requieren la identificación del afectado, y siempre que este haya proporcionado información adicional que permita su identificación, el impedimento, la obstaculización y la no atención reiterada del derecho a la portabilidad constituye una infracción grave que prescribe a los dos años [art. 73.c) de la LOPDGDD]. Cuando no se atienda el derecho a la portabilidad de los datos, pero ello no sea reiterado, la infracción (a la que se atribuye un carácter meramente formal) se califica como leve y prescribirá al año [arts. 74.c) y d) de la LO-

PDGDD]. Además, como se verá más adelante, la portabilidad es gratuita, salvo que concurran determinadas circunstancias muy concretas. Pues bien, la exigencia de un canon para atender la solicitud de portabilidad cuando no concurran tales circunstancias es una infracción muy grave [art. 72.1.j) de la LOPDGDD]. Si concurren tales circunstancias el cobro de un canon es lícito, pero constituye una infracción leve el hecho de que su cuantía exceda del importe de los costes afrontados para cumplir con la solicitud [art. 74.b) de la LOPDGDD].

III. EL DERECHO A LA PORTABILIDAD DE LOS DATOS PERSONALES

1. Introducción

El derecho a la portabilidad de los datos personales se encuentra recogido en el artículo 20 del RGPD, cuyo tenor literal es el siguiente:

«Artículo 20. Derecho a la portabilidad de los datos.

1. El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando:

a) el tratamiento esté basado en el consentimiento con arreglo al artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), o en un contrato con arreglo al artículo 6, apartado 1, letra b), y

b) el tratamiento se efectúe por medios automatizados.

2. Al ejercer su derecho a la portabilidad de los datos de acuerdo con el apartado 1, el interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible.

3. El ejercicio del derecho mencionado en el apartado 1 del presente artículo se entenderá sin perjuicio del artículo 17. Tal derecho no se aplicará al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

4. El derecho mencionado en el apartado 1 no afectará negativamente a los derechos y libertades de otros»[11].

Antes de analizar el artículo 20 del RGPD, debe resaltarse la utilidad de las directrices que ha elaborado el «Grupo de trabajo del artículo 29» sobre el derecho objeto de estudio (GRUPO DEL ARTÍCULO 29, 2016)[12].

No obstante, tales directrices carecen de valor normativo, por lo que el Tribunal de Justicia de la Unión Europea podría decantarse por otra interpretación del Reglamento. Dicho Grupo del artículo 29 ha sido sustituido con efectos a partir del 25 de mayo de 2018 por el Comité Europeo de Protección de Datos, que en su primera reunión respaldó —sin perjuicio de revisiones futuras— varios documentos de aquel Grupo. Entre ellos, las citadas directrices[13].

Por otro lado, la Directiva (UE) 2019/770 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, relativa a determinados aspectos de los contratos de suministro de contenidos y servicios digitales[14], reconoce un derecho que guarda algunas semejanzas con la portabilidad del artículo 20 del RGPD. El artículo 16 de la Directiva («Obligaciones del empresario en caso de resolución») dispone en su apartado cuarto que «salvo en las situaciones contempladas en el apartado 3, letras a), b) o c), el empresario pondrá a disposición del consumidor, previa petición de este último, contenidos, que no sean datos personales, que el consumidor haya facilitado o creado al utilizar los contenidos o servicios digitales suministrados por el empresario. El consumidor tendrá derecho a recuperar dichos contenidos digitales sin cargo alguno y sin impedimentos por parte del empresario, en un plazo razonable y en un formato utilizado habitualmente y legible electrónicamente»[15]. Con el fin de no alargar excesivamente este trabajo, se ha optado por no incluir ninguna referencia a la regulación de fondo de esta Directiva en los subapartados que siguen, reenviando al lector a un estudio específico en el que se compara la portabilidad del Reglamento general de protección de datos y la recuperación de contenidos de la *Propuesta* de Directiva de 9 de diciembre de 2015[16] (JANAL, 2017)[17].

2. La noción de datos personales

El artículo 20.1 del RGPD comienza diciendo que el interesado tiene derecho a recibir los «datos personales» que le incumban. Aunque no se trate de una cuestión específica del derecho a la portabilidad, es imprescindible estudiar este concepto con cierto detalle para hacer una primera acotación de la información que el usuario puede recuperar y transferir con arreglo al Reglamento (en el subapartado siguiente se verá que no todos los datos personales son susceptibles de portabilidad)[18].

La definición de datos personales se encuentra en el artículo 4.1) del RGPD, construyéndose en dos partes. En primer lugar, se dice que consiste en «toda información sobre una persona física identificada o identificable». A continuación, el texto precisa qué se entiende por identificable, diciendo que se considera como tal toda persona respecto de la que es posible de-

terminar su identidad «directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona». El considerando número 26 del Reglamento aclara que, para determinar si una persona es identificable, deben tenerse en cuenta todos los medios que puedan ser utilizados razonablemente por otra para identificarla directa o indirectamente. La ponderación se hace en función de todos los factores objetivos, incluyendo el coste y el tiempo que sean necesarios para poder llevar a cabo la identificación, y en función de la tecnología disponible en cada momento y de los avances tecnológicos[19]. Esto, sumado a que se habla de identificación directa o indirecta, conlleva que una información pueda constituir datos personales aun cuando no permita la identificación por sí sola, debiendo para ello ser combinada con datos adicionales.

Reflejando lo difícil que es retirar una información de Internet una vez que se ha difundido, se ha planteado un enfoque según el cual deban considerarse datos personales ya a día de hoy todos aquellos que en el futuro sí podrían permitir la identificación de una persona (VAN LOENEN *et al.*, 2016, 339). No obstante, probablemente se mantendrá una interpretación más matizada, tomando en consideración los avances tecnológicos previsibles durante el periodo en el que se tratarán los datos (GRUPO DEL ARTÍCULO 29, 2007, 17).

Según la jurisprudencia europea, no se requiere que toda la información que permita la identificación del interesado esté en poder de una sola persona, bastando que esta pueda razonablemente relacionar los diferentes datos[20]. El Tribunal de Justicia también ha precisado que no se alcanza el estándar de identificabilidad «cuando la identificación del interesado esté prohibida por la ley o sea prácticamente irrealizable, por ejemplo, porque implique un esfuerzo desmesurado en cuanto a tiempo, costes y recursos humanos, de modo que el riesgo de identificación sea en realidad insignificante»[21]. Aunque estos pronunciamientos se refieren a la Directiva sobre datos personales, deben considerarse igualmente aplicables en el marco del Reglamento (VOIGT y VON DEM BUSSCHE, 2017, 12).

El recurso a la fórmula «en particular» en el Reglamento —como antes en la Directiva— hace que la enumeración de criterios que permiten la identificación de una persona no sea taxativa. Ello da lugar a una definición de datos personales abierta y flexible, imprescindible para su adaptación a nuevos escenarios que vayan apareciendo con la innovación tecnológica. Además, el legislador europeo utiliza la expresión «toda información» —también lo hizo en la Directiva—, lo que se relaciona con una noción amplia de datos personales que pretende abarcar cualquier tipo de infor-

mación de la que quepa decir que versa sobre el interesado, esto es, que se relacione con una persona[22]. Eso no impide que una misma información pueda referirse a varias personas al mismo tiempo, de tal modo que sean datos personales de todas ellas[23].

Se ha dicho que la distinción entre datos personales y datos no personales puede perder su importancia con el tiempo, e incluso desaparecer, en la medida en que las nuevas tecnologías permitan la identificación de las personas a partir de información no personal (FINCK, 2018, 22). En efecto, si aumentan las posibilidades de hacer semejante identificación, datos que actualmente no son considerados personales entrarían en el ámbito de aplicación del Reglamento. También resulta previsible una pérdida de relevancia de la distinción entre los simples datos personales y los denominados «datos sensibles» que permiten conocer cuestiones tales como la etnia, la raza, la ideología política, la religión o el estado de salud del interesado (art. 9 del RGPD). El *Big Data* permitiría inferir datos sensibles a partir de otros que no lo son. Por ejemplo, construir una imagen sobre la salud de la persona con base en el tipo de alimentos que adquiere en línea, o en el tipo de aplicaciones que tiene descargadas en su terminal móvil (ZARSKY, 2017, 1000 y 1013).

Una dirección de correo electrónico que contenga el nombre y apellidos de una persona debe ser considerada datos personales. De hecho, se trata de este tipo de datos incluso cuando la dirección no incluya el nombre y apellidos, pero utilice un dominio susceptible de ser utilizado para identificar al titular, siempre que esta conexión no requiera hacer esfuerzos desproporcionados (STROIE, 2018, 1). También la dirección IP del usuario constituye datos personales, pues permite su identificación por parte del proveedor de acceso a Internet[24]. En cuanto a las direcciones IP dinámicas, de carácter provisional al variar con cada conexión a Internet, no permiten identificar directamente al interesado (frente a las estáticas, cuyo carácter invariable posibilita una identificación permanente). Sin embargo, si cabe una identificación por vía indirecta, combinando la dirección IP dinámica con otros datos —incluso aquellos que tenga una tercera persona—, y siempre que esta combinación constituya un medio susceptible de ser razonablemente utilizado por parte de una persona para identificar al interesado, la dirección IP dinámica tendrá la consideración de datos personales[25]. No sucede lo mismo si la dirección IP es transformada en una dirección genérica desprovista de cualquier conexión con una cuenta de usuario. El elemento clave es, en todo caso, si la identificación del usuario —directa o indirecta— resulta posible[26].

El Reglamento general de protección de datos se proyecta sobre los datos seudonimizados. Este concepto se deriva del punto 5) del artículo 4 del RGPD, tratándose de datos personales que no pueden atribuirse a una persona sin utilizar información adicional separada y sujeta a «medidas téc-

nicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable». Por el contrario, el Reglamento no resulta de aplicación —tampoco lo era la Directiva sobre datos personales— a la información o datos anónimos, entendiendo por tales los no relacionados con una persona física identificada o identificable, bien en origen, bien porque han sido sometidos a un proceso para que el interesado deje de ser identificable (considerando número 26 del Reglamento; GRUPO DEL ARTÍCULO 29, 2014b, 5-6)[27].

Por supuesto, el hecho de que el Reglamento se aplique a los datos seudonimizados no significa que este proceso de ocultación carezca de consecuencia alguna, ya que puede tener importantes implicaciones a la hora de demostrar el cumplimiento de las obligaciones en materia de seguridad de los datos (VOIGT y VON DEM BUSSCHE, 2017, 15). Por ejemplo, el artículo 34.1 del RGPD impone al responsable del tratamiento la obligación de comunicar al interesado, sin dilación indebida, toda violación de seguridad de los datos personales que suponga un riesgo elevado para sus derechos y libertades. Sin embargo, esta obligación se exceptúa si los datos afectados han sido objeto de medidas de protección técnicas y organizativas apropiadas, constituyendo un ejemplo de tales medidas el cifrado —esto es, convertir la información en ininteligible para toda persona que no tenga autorizado el acceso a la misma— [art. 34.3.a) del RGPD].

Para que la información sea anónima, el Grupo del artículo 29 señala que la conversión debe ser irreversible, con el mismo carácter permanente que se predica de un borrado de los datos. No obstante, dicho grupo admite que siempre habrá un «riesgo residual» de identificación, de ahí que repute técnica de anonimización cualquier mecanismo lo suficientemente robusto para que la identificación sea «razonablemente imposible» (GRUPO DEL ARTÍCULO 29, 2014b, 5-10). El Supervisor Europeo de Protección de Datos parece ir algo más allá. Tras aclarar que el uso de técnicas de anonimización no implica necesariamente que la información sea anónima, reconoce que una total anonimización no siempre es posible, pero afirma que las normas de protección de datos son aplicables «a menos que se garantice completamente una total anonimización» (SEPD, 2012, puntos 43 y 44). Quizás esta conclusión resulte un tanto excesiva.

En la Propuesta de Reglamento de 2012, la definición de «interesado» recogida en su artículo 4.1) decía que se trataba de toda persona física identificada o identificable, ya fuese directa o indirectamente, «por medios que puedan ser utilizados razonablemente por el responsable del tratamiento o por cualquier otra persona física o jurídica, en particular mediante…». El considerando número 23 de la Propuesta refrendaba la referencia a los medios cuya utilización fuese razonable. Como se ha visto, al definir datos personales, el artículo 4.1) del RGPD omite toda referencia a tales medios,

pero su considerando número 26 hace alusión a ellos para determinar si una persona es identificable, incorporando también una referencia a la probabilidad razonable de su uso para identificar a una persona.

La diferencia existente entre los artículos 4.1) de la Propuesta y del Reglamento finalmente aprobado no parece suficiente para sostener que, según el segundo texto, el carácter anónimo de los datos requiere una *total* imposibilidad de identificación. La mención de los medios cuya utilización sea razonable en el considerando 26 del Reglamento no es un descuido, pues su contenido ha sido profundamente examinado en el proceso legislativo, como demuestran los cambios que se han introducido en él con respecto al considerando número 23 de la Propuesta. Además, si se exigiese una total imposibilidad de identificación, y al mismo tiempo se reconociese que siempre hay un riesgo —por pequeño que sea— de que la persona sea identificada, sencillamente no existirían los datos anónimos. La exclusión de estos del ámbito de aplicación del Reglamento perdería pues todo sentido. En conclusión, entiendo que la existencia de un perpetuo riesgo residual de identificación hace que la proclamación del carácter anónimo de unos datos no deba requerir una imposibilidad de identificación perfecta y absoluta, pero que sin duda alguna el nivel exigido para alcanzar ese carácter sea —y deba ser— muy alto (VOIGT y VON DEM BUSSCHE, 2017, 13-14; FINCK, 2018, 22 y 26). En cualquier caso, no siempre será sencillo encontrar la frontera entre la mera encriptación y la anonimización (ZANFIR, 2012, 154, 155 y 159).

El hecho de que la aplicación del Reglamento general de protección de datos quede descartada cuando se está ante datos anónimos no impide que el proceso de anonimización en sí mismo, sí se encuentre sometido a la norma (ZANFIR, 2012, 159; DESGENS-PASANAU, 2018, 245).

Expuesto lo anterior, el derecho a la portabilidad tiene, sin embargo, un ámbito de aplicación no del todo coincidente con el que se ha descrito de manera general para el Reglamento. Puesto que los datos personales objeto de portabilidad son los que incumban al interesado, los datos anónimos o que no conciernan al solicitante quedan excluidos. Por lo que respecta a los datos seudónimos, el Grupo del artículo 29 precisa que pueden ser objeto de portabilidad cuando «estén claramente vinculados con el interesado (p. ej. al haber este proporcionado el identificador correspondiente)» (GRUPO DEL ARTÍCULO 29, 2016, 11). En efecto, de acuerdo con el artículo 11.1 del RGPD, un responsable del tratamiento «no estará obligado a mantener, obtener o tratar información adicional con vistas a identificar al interesado con la única finalidad de cumplir el presente Reglamento», si los fines para los cuales trata datos personales no requieren la identificación de la persona o han dejado de hacerlo. Según el artículo 11.2 del RGPD, en este caso, y siempre que el responsable demuestre que no puede identificar al interesado,

deberá informarle de tal circunstancia, dejando de ser de aplicación los artículos 15 a 20 del RGPD. Ahora bien, esta regla se exceptúa —teniendo el interesado derecho a la portabilidad— cuando facilita la información adicional que permite su identificación.

En este subapartado relativo a la noción de datos personales, no está de más referirse a la cadena de bloques o *blockchain*, el tipo más conocido de la denominada «tecnología de registro distribuido» (*distributed ledger technology*, DLT), hasta el punto de que a veces se usan como sinónimos[28]. La información contenida en una cadena de bloques disfruta de un mayor nivel de seguridad, pero será considerada a menudo datos personales (siempre, claro está, que se relacione con una persona física). Con el fin de aproximar al lector a la relación entre la tecnología de registro distribuido y el concepto de datos personales, se ofrecen algunas observaciones generales, advirtiendo que quien suscribe estas líneas no es, ni mucho menos, un experto en materia de codificación o criptografía[29].

El funcionamiento de la tecnología de registro distribuido se caracteriza por la existencia de dos tipos de claves, pública y privada. Estas podrían entenderse de manera sencilla como, respectivamente, un código de usuario —que solo permite su identificación concreta si se dispone de elementos adicionales— y una contraseña. Además de la clave *pública*, que permite la identificación de la persona si se combina con otros datos, hay otra información recogida en una cadena de bloques que también es relevante a los efectos de la protección de datos: la que concierne los detalles de la transacción realizada utilizando la tecnología referida, ya sea por ejemplo un cronomarcador, ya sea el contenido en sí de la transacción subyacente. Especialmente en este último caso, la posibilidad de que una persona sea identificada no es escasa, por lo que la información se considerará a menudo datos personales.

La información contenida en los registros descentralizados puede quedar recogida en diversos formatos: texto simple, información encriptada, o como un valor *hash* —el resultado de aplicar una función de resumen a una información de entrada—. Que el texto simple y la información encriptada relativas a una persona son datos personales no ofrece demasiadas dudas. En particular, la encriptación constituye una función bidireccional, es decir, la clave adecuada permite revertir el proceso, por lo que se trata de una simple seudonimización. Con respecto a la información objeto de *hash*, la función aplicada es unidireccional, esto es, fácil de llevar a cabo para obtener un valor de salida, pero complicada de invertir desde el punto de vista computacional. Las funciones unidireccionales ofrecen un mayor nivel de seguridad por no ser reversibles, pero no siempre se alcanzará el umbral necesario para considerar la información oculta como anónima. Y es que conociendo la función de resumen y todos los valores de entrada, la primera

puede aplicarse sistemáticamente sobre los segundos, obteniendo todos los valores de salida y pudiendo entonces establecer la correspondencia. Como se ha observado anteriormente, para que una información sea considerada anónima, no parece preciso que la identificación del interesado resulte total y absolutamente imposible, porque siempre hay un riesgo residual en este sentido. Bastará con que el riesgo de identificación sea insignificante debido a que la identificación sea irrealizable en la práctica, por el esfuerzo que conllevaría[30].

3. Condiciones

El artículo 20.1 del RGPD establece que los datos personales objeto de portabilidad son aquellos «facilitados» por el interesado a un responsable del tratamiento. Además de esta condición previa, el precepto impone dos más: el tratamiento debe fundamentarse en el consentimiento del interesado o en ser necesario para la ejecución de un contrato, y debe llevarse a cabo por medios automatizados. Se trata de condiciones cumulativas. A continuación se analizará cada uno de estos puntos[31].

Como se ha expuesto, el derecho a la portabilidad reconocido por el Reglamento europeo se proyecta únicamente sobre datos personales. Pero eso no significa que sean portables cualesquiera datos personales. El Reglamento solo ampara la portabilidad de aquellos que hayan sido *facilitados* por el interesado al responsable del tratamiento. La interpretación de la noción de «facilitar» no es tan sencilla como pudiera parecer, por lo que el Grupo del artículo 29 ha proporcionado algunas claves, siendo el punto de partida que procede una interpretación amplia.

Según dicho Grupo, son datos facilitados por el interesado los suministrados por este de forma consciente y activa —por razones obvias—. Además, y como consecuencia de la interpretación extensiva que corresponde, dice que también deben reputarse datos facilitados los «observados» a raíz de sus actividades, los que resultan del uso de un servicio o un dispositivo[32]. Se ofrecen como ejemplos el historial de búsqueda, la ubicación geográfica, e incluso el ritmo cardíaco que ha sido registrado por un dispositivo. Por el contrario, no son objeto de portabilidad los datos «creados» por el responsable del tratamiento, entendiendo por tales la información deducida, inferida o producto del análisis de los datos que se obtienen de la actividad o comportamiento del interesado (por ejemplo, mediante la aplicación de un algoritmo sobre ellos) (GRUPO DEL ARTÍCULO 29, 2016, 11-12).

La opinión del Grupo del artículo 29, sin embargo, puede ser cuestionada. Aun haciendo una interpretación amplia del Reglamento, resulta dudoso que los datos observados deban considerarse facilitados. La propia Comisión

Europea parece no estar de acuerdo, señalando que el derecho a la portabilidad se ha concebido pensando fundamentalmente en las redes sociales y en la información que el usuario suministra activamente (MEYER, 2017). Diferentes autores parecen asumir que, en efecto, los datos «observados» no son objeto de portabilidad (GRAEF *et al.*, 2014, 4); sin perjuicio de que también se refieran a que, habida cuenta del potencial de tales datos para revelar conductas de los usuarios, sería beneficioso que estos dispusiesen de un mayor control sobre ellos (VAN OOIJEN y VRABEC, 2019, 103). Así pues, no está claro que los responsables del tratamiento deban garantizar la portabilidad de la información no suministrada de forma activa por los interesados.

El tenor literal de la norma lleva a pensar que los datos simplemente observados no están incluidos en el artículo 20 del RGPD, pues «facilitar» tiene una connotación activa[33]. Los artículos 13 y 14 del RGPD plasman esta idea cuando usan el vocablo facilitar y sus derivados, mientras que en sentido pasivo no hablan de datos facilitados por el interesado, sino «obtenidos de» él; esto justificaría una lectura restrictiva del artículo 20 del RGPD (CENTRE FOR INFORMATION POLICY LEADERSHIP, 2017, 8). De hecho, en el Internet de las cosas no puede hablarse estrictamente de una recogida de información directamente de la persona, como sucede con los tradicionales formularios de tratamiento de datos; sino, más bien, de una «producción discreta» de información, pudiendo debatir si es la persona o el propio objeto quien la produce (GRÉGOIRE, 2018, 118 y 122).

Por el contrario, la finalidad protectora del Reglamento y los objetivos específicos del derecho a la portabilidad —sobre los que se hablará más adelante— conducen a una respuesta diferente. Además, en la *Directiva sobre suministro de contenidos y servicios digitales*, el Parlamento Europeo y el Consejo se muestran tácitamente a favor de una interpretación extensiva del Reglamento general de protección de datos. En el considerando número 38 de la Directiva, tras hacer referencia a los derechos a la supresión y a la portabilidad de los datos, se afirma que estos derechos «son de aplicación a todos los datos personales facilitados por el consumidor al empresario *o recopilados por este* en relación con todo contrato que entre en el ámbito de aplicación de la presente Directiva…» (énfasis añadido).

Ante la duda, y mientras el Tribunal de Justicia de la Unión Europea no se pronuncie, creo que debe prevalecer el segundo enfoque, como interpretación más favorable al interesado (JANAL, 2017, 61-62; DE HERT *et al.*, 2018, 199-203). Ello no impedirá que aparezcan áreas grises en las que se discuta si se ha producido una verdadera labor de inferencia, deducción, análisis o estudio de los datos (SWIRE y LAGOS, 2013, 347-348; BOZDAG, 2018, 3; GRAEF *et al.*, 2018, 1373).

Sea como fuere, resulta evidente que la exigencia de que los datos hayan sido facilitados por el usuario limita la efectividad práctica de la portabilidad. Hay información cuya transmisión resultaría muy interesante para el usuario que desea comenzar a utilizar una nueva plataforma, y que probablemente queda fuera del artículo 20 del RGPD. Por ejemplo, fotos del interesado que han sido subidas a una red social por parte de uno de sus amigos (GRAEF, 2015, 507) —también hay quien simplemente manifiesta dudas sobre si constituyen datos facilitados por el interesado los suministrados por un tercero con el consentimiento de aquel (VOIGT y VON DEM BUSSCHE, 2017, 170)—, o la reputación que ha construido un usuario a partir de las opiniones que otros han manifestado sobre él en el ámbito de plataformas de compraventa o de prestación de servicios (DIKER VANBERG y ÜNVER, 2017, 3).

Los datos que no se consideran facilitados por el interesado, pese a no ser portables, sí son objeto de derecho de acceso, ya que este último no se encuentra sometido a la condición previa ahora estudiada (GRUPO DEL ARTÍCULO 29, 2016, nota 20). En virtud del artículo 15.3 del RGPD, el responsable debe proporcionar una copia de los datos personales objeto de tratamiento, mientras que por cualquier otra copia puede percibir un canon razonable establecido en función de los costes administrativos. En cuanto al formato, el mismo artículo solo indica que si la solicitud se hace por medios electrónicos, y salvo que el interesado pida que se le faciliten de otro modo, el responsable deberá proporcionar los datos en un formato electrónico de uso común. En definitiva, aunque el interesado careciese de un derecho a la portabilidad sobre su perfil de consumo, por ejemplo, sí tendría acceso al mismo (DE TERWANGNE *et al.*, 2017, 315).

La siguiente condición previa del derecho a la portabilidad incide en el origen del tratamiento de los datos susceptibles de recuperación y transmisión, origen que debe encontrarse, bien en el consentimiento del interesado, bien en su necesidad para la ejecución de un contrato. El considerando número 68 del Reglamento lo enuncia en forma negativa: el derecho estudiado no se aplica cuando la base jurídica del tratamiento no sea el consentimiento o un contrato.

Con respecto a la primera posibilidad, el artículo 20.1 del RGPD alude a los artículos 6.1.a), 9.2.a). En efecto, para que el tratamiento de datos sea lícito, debe cumplir con alguno de los fundamentos jurídicos enunciados en el artículo 6. La letra a) del apartado primero reputa lícito el tratamiento cuando el interesado ha dado su consentimiento para el mismo, para uno o varios fines específicos. Por su parte, el artículo 9 del RGPD prohíbe como regla general el tratamiento de los datos sensibles (apdo. 1): aquellos que revelan el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, la afiliación sindical, los relativos a la salud o a

la sexualidad, los datos genéticos y los biométricos dirigidos a identificar de manera unívoca a una persona física. Sin embargo, esta prohibición desaparece en ciertos supuestos, siendo uno de ellos que el interesado haya manifestado su consentimiento explícito para el tratamiento de datos para fines especificados, y siempre que un Derecho nacional no prohíba a su vez el levantamiento de la prohibición por el interesado (apdo. 2.a).

El Reglamento general de protección de datos es exigente con relación al consentimiento por parte del interesado, aunque no establezca una forma determinada para prestarlo. El artículo 4.11) del RGPD lo define como una «manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen»[34]. Con ello se pretende que el usuario preste un consentimiento consciente e informado, y no tácito o mediante casillas marcadas de antemano[35]. Este objetivo resulta de la constatación que, si bien cada vez más personas se sirven de nuevas tecnologías que utilizan datos personales, no siempre son conscientes de la cantidad y del tipo de información que generan (MARTÍNEZ PÉREZ, 2018, 238-239). El Internet de las cosas, y, en particular, los *wearables* o dispositivos «ponibles» o «vestibles»[36], es un ejemplo evidente de que un alto uso de tales tecnologías no va necesariamente unido a una consciencia igualmente alta sobre el volumen y el tipo de información personal generada (KAMARA, 2017, 8 y 9; GRÉGOIRE, 2018, 118-121).

Siempre que el tratamiento se base en el consentimiento del interesado, el responsable debe poder demostrar que efectivamente fue prestado (art. 7.1 del RGPD). Además, cuando el consentimiento se preste por escrito para varios asuntos, el referido al tratamiento de datos debe distinguirse claramente de las demás cuestiones, y siempre de forma transparente (art. 7.2 del RGPD). Aunque el precepto se refiere a la inteligibilidad, al fácil acceso y al lenguaje claro y sencillo, el considerando número 42 del Reglamento incluye una referencia a la Directiva sobre cláusulas abusivas[37]. En consecuencia, a pesar de que los términos empleados conduzcan a un plano formal, creo que deben entenderse más allá de la dimensión meramente gramatical, tratándose de la transparencia denominada material, reforzada, cualificada o sustantiva[38]. Se reconoce al interesado el derecho a retirar su consentimiento en cualquier momento, debiendo ser tan sencilla su retirada como lo fue su prestación (art. 7.3 del RGPD). Finalmente, el consentimiento debe ser prestado libremente, aspecto cuya evaluación requiere tener en cuenta si la ejecución de un contrato o la prestación de un servicio está condicionada a que el usuario preste su consentimiento para el tratamiento de datos personales que no son necesarios para dicha ejecución (art. 7.4 del RGPD). Cuando se produce esta supeditación, se presume que el consentimiento del interesado no es libre, según indica el considerando número 43 del Reglamento[39].

Sobre la ejecución de un contrato como origen del tratamiento de datos personales, el artículo 20 del RGPD menciona el artículo 6.1.b). En efecto, una segunda situación en la que un tratamiento de datos deviene lícito es que sea «necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales». Este criterio es de interpretación estricta (GRUPO DEL ARTÍCULO 29, 2014a, 20; GRUPO DEL ARTÍCULO 29, 2018, 9). En consecuencia, el artículo 6.1.b) del RGPD no legitima el tratamiento cuando el contrato tenga por objeto principal la comercialización de los datos obtenidos (en este caso se requeriría el consentimiento del interesado), sino solamente cuando el tratamiento constituye una actividad accesoria pero necesaria para que las obligaciones contractuales sean ejecutadas (LANGHANKE y SCHMIDT-KESSEL, 2015, 220).

De acuerdo con el Grupo del artículo 29, no puede considerarse necesario el tratamiento de datos por el mero hecho de venir impuesto por el responsable del tratamiento. La necesidad es un criterio directo y objetivo: el contrato, para ser ejecutado y cumplir con su finalidad principal, requiere tratar datos personales del interesado. Dos ejemplos serían la dirección para poder hacer entrega de un bien adquirido en línea y los datos bancarios para hacer un pago con tarjeta de crédito (GRUPO DEL ARTÍCULO 29, 2018, 9). El tratamiento debe limitarse a lo que sea necesario para ejecutar el contrato, y cualquier uso que vaya más allá requiere otro fundamento para ser lícito. Por ejemplo, si el usuario adquiere un bien por Internet, el artículo 6.1.b) del RGPD no ampara la elaboración de perfiles sobre las preferencias de ese usuario, ni siquiera cuando prevea ese uso en sus condiciones generales. Además, la ejecución del contrato se entiende como su desarrollo normal, sin incidentes o incumplimientos. Esto no significa que, acaecida una circunstancia que altera su ejecución normal, el tratamiento no pueda quedar amparado con base en otro fundamento (GRUPO DEL ARTÍCULO 29, 2014a, 20-22; SEPD, 2017, punto 52). Dos ejemplos ofrecidos por el Grupo del artículo 29 de datos que «normalmente» serán susceptibles de portabilidad, son los títulos de los libros que el interesado haya comprado *online*, y la lista de canciones escuchadas a través de un servicio de reproducción musical (GRUPO DEL ARTÍCULO 29, 2016, 9-10).

El hecho de que se excluya la portabilidad cuando el tratamiento no tenga su origen, bien en el consentimiento, bien en la ejecución de un contrato, impide el ejercicio del derecho cuando el tratamiento de datos es ilícito. Situación con la que algún autor no está de acuerdo por beneficiar al infractor, planteando la necesidad de corregir la formulación del precepto correspondiente (JANAL, 2017, 62). También queda excluida la portabilidad cuando el tratamiento se efectúe con base en un interés legítimo, supuesto que prevé el artículo 6.1.f) del RGPD, análogo al artículo 7.f) de la Directiva

sobre datos personales. El Reglamento carece de una definición de lo que se entiende por interés legítimo, al igual que sucedía con la Directiva. Esto hace que el concepto resulte flexible y abierto, no existiendo ningún tipo de intereses lícitos que queden excluidos siempre y todo en caso[40].

Un dictamen del Grupo del artículo 29, la jurisprudencia del Tribunal de Justicia de la Unión Europea, y el considerando número 47 del Reglamento nos acercan a esta noción de contornos poco claros. El TJUE ha establecido tres requisitos cumulativos para que un tratamiento de datos se considere lícito con base en el artículo 7.f) de la Directiva, siendo perfectamente aplicable en el marco de la nueva norma: el responsable del tratamiento o los terceros a quienes se comunican los datos deben perseguir un interés legítimo, el tratamiento debe ser necesario para satisfacer este interés, y no deben prevalecer los derechos y libertades fundamentales del interesado[41].

Con respecto a la tercera condición, el considerando número 47 del Reglamento obliga a tener en cuenta las expectativas razonables de los interesados en función de su relación con el responsable del tratamiento. Esta ponderación resulta especialmente importante en la medida en que, como reflejó en su momento el Grupo del artículo 29, el *marketing* y la publicidad pueden amparar un tratamiento de datos (GRUPO DEL ARTÍCULO 29, 2014a, 31)[42], lo cual es confirmado por el considerando citado al aludir a los fines de mercadotecnia directa. Así pues, un responsable del tratamiento podrá alegar un interés legítimo en relación con el tratamiento de datos de un cliente. Pero, de acuerdo con el mismo considerando, los derechos del interesado podrían prevalecer sobre los del responsable cuando el primero no pudiese esperar un tratamiento de datos ulterior (por ejemplo, para dirigirle publicidad) (VOIGT y VON DEM BUSSCHE, 2017, 104)[43]. En la actividad de ponderación de intereses, quizás decante la balanza a favor del responsable del tratamiento el reconocimiento voluntario por su parte de un derecho a la portabilidad en situaciones en las que no esté obligado a garantizarla (GRAEF *et al.*, 2018, 1371).

La última condición previa del derecho a la portabilidad de los datos personales no se refiere al origen del tratamiento, sino a la forma en la que este debe llevarse a cabo: por medios automatizados (art. 20.1.b) del RGPD). El Grupo del artículo 29 ha subrayado que este requisito excluirá «la mayor parte de los archivos en papel» (GRUPO DEL ARTÍCULO 29, 2016, 10). En otras palabras, efectuar un tratamiento de datos utilizando semejante soporte no implica en todo caso la exclusión de la portabilidad respecto de los datos afectados. Dado que el artículo 20.1.b) del RGPD alude al tratamiento que se efectúe por medios automatizados, sin decir expresamente que la automatización debe ser la forma exclusiva de tratamiento, y correspondiendo una interpretación favorable al interesado para dotarle de más control sobre su información personal, considero que la portabi-

lidad es posible cuando el tratamiento se haga por medios automatizados solo parcialmente. La condición se correspondería así con el comienzo del artículo 2.1 del RGPD, que establece la aplicación del texto normativo al «tratamiento total o parcialmente automatizado de datos personales», dejando fuera su segunda parte, que prevé su aplicación igualmente «al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero».

4. Contenido

Entrando en lo que es propiamente el contenido del derecho a la portabilidad de los datos personales, de los artículos 20.1 y 20.2 del RGDP se derivan dos vertientes. Por un lado, el interesado tiene derecho a recibir los datos y a transmitirlos a otro responsable del tratamiento. Por otro, el interesado tiene derecho a que la transmisión de los datos se realice directamente entre responsables del tratamiento, siempre que ello resulte técnicamente posible. Además, en todo caso, la entrega de los datos debe hacerse en un formato estructurado, de uso común y lectura mecánica.

El Reglamento dice que el interesado tiene derecho a la recepción y transmisión de los datos «sin que lo impida el responsable al que se los hubiera facilitado», lo cual debe ser entendido como «sin impedimentos», expresión que utilizaba el artículo 18.2 de la Propuesta de 2012[44]. No se trata solo de que el responsable no pueda impedir totalmente la portabilidad, sino de que no puede poner ninguna traba para evitar o ralentizar alguna de las fases del proceso (por ejemplo, amparándose en obstáculos de carácter técnico o financiero) (VOIGT y VON DEM BUSSCHE, 2017, 175; MIRALLES LÓPEZ, 2018, 406-407). Aunque el responsable debe garantizar una transmisión segura de los datos, lo que puede requerir ciertas actuaciones —como la identificación del interesado—, ello no justificará un exceso de celo que suponga un obstáculo para el éxito del proceso (GRUPO DEL ARTÍCULO 29, 2016, 18 y 22).

No resultará sencillo encontrar el equilibrio entre la seguridad y la agilidad en la transferencia, e incluso podría estarse ante una contradicción inevitable entre ambos objetivos (BOZDAG, 2018, 4-5). Según el artículo 12.6 del RGPD, en el marco de una solicitud con base en los artículos 15 a 21, el responsable del tratamiento puede solicitar al interesado la información adicional necesaria para confirmar su identidad, siempre que albergue dudas razonables con relación a ello. A la vista de este precepto, si un usuario efectúa una solicitud de portabilidad tras acceder a su cuenta desde un dispositivo distinto del que utiliza habitualmente, no está claro si estaría justificado requerir una nueva verificación de la identidad, o si por

el contrario se trataría de un obstáculo indebido (SWIRE y LAGOS, 2013, 374). Algunas plataformas ya realizan una comprobación adicional en el momento de la conexión a una cuenta con un dispositivo desconocido o no habitual. De haber procedido a esta segunda identificación, probablemente no estaría justificado una tercera tras la solicitud de portabilidad. Pero una respuesta distinta también sería razonable, dados los especiales riesgos que implica la transferencia de datos, si completar el procedimiento de comprobación de identidad no supone una gran carga para el interesado.

La transferencia de los datos directamente entre responsables del tratamiento está sometida a una condición adicional: que ello sea técnicamente posible. Algunos autores destacan la vaguedad de este criterio, advirtiendo que lo que para un responsable del tratamiento es posible desde el punto de vista técnico, no lo es necesariamente para otro; de ello podrá derivarse una cierta litigiosidad (DIKER VANBERG y ÜNVER, 2017, 4). El Grupo del artículo 29 dice que la posibilidad técnica se determina en cada caso concreto, pudiendo resultar la transmisión técnicamente *imposible* no solo cuando el receptor no disponga de la capacidad para recibir los datos, sino también cuando no se pueda garantizar la seguridad de la trasferencia entre sistemas (GRUPO DEL ARTÍCULO 29, 2016, 18). No obstante, algunas voces consideran que un responsable del tratamiento no debería poder denegar la portabilidad con base en la falta de seguridad ofrecida por el tercero receptor (CENTRE FOR INFORMATION POLICY LEADERSHIP, 2017, 14). Desde mi punto de vista, en efecto, no cabe decir que la portabilidad resulta técnicamente imposible cuando el transmitente identifique riesgos de seguridad en el tercero. En consecuencia, creo que no puede negarse a transmitir los datos, sin perjuicio de que deba informar al interesado previamente de la existencia de tales riesgos, y cerciorarse de que el usuario desea pese a todo que la transmisión tenga lugar. Esto puede fundamentarse en el deber de transparencia previsto en el artículo 12 del RGPD, así como en el principio de buena fe.

La cuestión relativa a la forma —en sentido amplio— en la que deben suministrarse los datos objeto de portabilidad es uno de los aspectos que presentan un mayor interés.

Según el Grupo del artículo 29, el responsable del tratamiento puede cumplir con las exigencias del Reglamento tanto mediante una transmisión directa de los datos como mediante la puesta en marcha de una herramienta automatizada que permita al usuario extraerlos. La transmisión directa incluye la posibilidad de que el responsable proporcione al interesado un soporte físico que contenga los datos, solución útil cuando la transmisión en línea genere problemas, en particular por el volumen de la información que deba entregarse (GRUPO DEL ARTÍCULO 29, 2016, 16, 18 y 19). No obstante, mientras que la posibilidad de una transmisión en un soporte físico

ofrece pocas dudas, es incierto si una herramienta que permita la extracción manual de los datos personales satisface las exigencias del Reglamento, en la medida en que el interesado tiene derecho a *recibir* los datos personales en un formato estructurado. De hecho, algún autor lo niega, sosteniendo que el Reglamento impone al responsable del tratamiento ofrecer «un conjunto estructurado de datos» (JANAL, 2017, 62).

En mi opinión, ofrecer únicamente la extracción manual de los datos no parece suficiente para cumplir con la normativa. Cosa distinta es que, además de ofrecer al usuario la posibilidad de recibir y/o transmitir a un tercero todos los datos portables en un formato estructurado —por ejemplo, estando marcadas por defecto todas las categorías de datos portables—, se le ofrezca seleccionar qué datos concretos, de entre los portables, desea recibir y/o transmitir, para suministrarlos después estructurados. La base podría encontrarse en el considerando número 63 del Reglamento, si bien este se refiere al derecho de acceso, y no a la portabilidad. El considerando señala que «si trata una gran cantidad de información relativa al interesado, el responsable del tratamiento debe estar facultado para solicitar que, antes de facilitarse la información, el interesado especifique la información o actividades de tratamiento a que se refiere la solicitud». Ahora bien, no es seguro que la facultad prevista en el considerando número 63 pueda aplicarse en el marco del derecho a la portabilidad (SWIRE y LAGOS, 2013, 370), si bien hay voces que se pronuncian expresamente a favor (VOIGT y VON DEM BUSSCHE, 2017, 169-170). Desde mi punto de vista no debería haber inconveniente, no constituyendo la petición del responsable un obstáculo injustificado al ejercicio del derecho, salvo que en su solicitud el interesado ya haya dicho que desea recibir todos los datos portables[45].

En su labor de interpretación del derecho de acceso en el marco de la Directiva sobre datos personales, el Tribunal de Justicia señaló que el interesado no tenía derecho a que el responsable le suministrase una copia íntegra del documento o fichero original en el que constasen sus datos personales. Bastaba la entrega en un formato inteligible para que pudiera tener conocimiento de los datos tratados y comprobar tanto su exactitud como que su tratamiento respetaba la normativa aplicable, para poder ejercitar eventualmente los derechos reconocidos por la Directiva. Por lo tanto, era suficiente con que el interesado obtuviese una idea completa de los datos, si bien el responsable podría cumplir con sus obligaciones suministrando el documento original, en su caso, borrando la información que no tuviese el carácter de datos personales[46].

El derecho a la portabilidad no obliga a suministrar el archivo original, el cual, de hecho, podría no reunir los requisitos de formato impuestos por el artículo 20 del RGPD. Sin embargo, en el contexto de la portabilidad no es suficiente con proporcionar una idea completa de los datos tratados. Y,

además, la finalidad del derecho impone ciertas limitaciones al borrado de los datos no personales que acompañen a los que sí lo son. Piénsese en una fotografía cargada en una red social, en la que aparece el interesado con un determinado paisaje al fondo. Difícilmente la portabilidad sería útil para el usuario si se le entregase un archivo reutilizable pero únicamente con su imagen personal, recortando o limitando el paisaje visible.

El formato en el que se suministren los datos al interesado debe ser estructurado, de uso común y lectura mecánica. El considerando número 68 del Reglamento aparentemente añade otro criterio, al aludir a un formato estructurado, de uso común, de lectura mecánica «e interoperable» (BOZDAG, 2018, 5). No obstante, según el Grupo del artículo 29, la interoperabilidad no es más que el resultado de que se cumplan los tres requisitos anteriores (GRUPO DEL ARTÍCULO 29, 2016, 19). El Reglamento no contiene ninguna definición de los términos señalados, por lo que para su interpretación deberá acudirse a otros textos. Lo cual, sin embargo, no evitará que surjan ciertas dudas y áreas grises (SWIRE y LAGOS, 2013, 345-347; CENTRE FOR INFORMATION POLICY LEADERSHIP, 2017, 13).

Así, la norma estándar ISO/IEC 2382:2015 sobre Vocabulario de tecnologías de la información ofrece la siguiente definición de interoperabilidad como término fundamental: «la capacidad de comunicar, ejecutar programas o transferir datos entre distintas unidades funcionales de un modo que requiera un escaso o nulo conocimiento por parte del usuario de las características diferenciadoras entre dichas unidades»[47]. Debe distinguirse la interoperabilidad de la compatibilidad, que es definida por la misma norma ISO/IEC 2382:2015 como la «capacidad de una unidad funcional para satisfacer los requisitos de una interfaz específica sin modificaciones apreciables». En este sentido, el considerando número 68 del Reglamento aclara que el derecho a la portabilidad no obliga al responsable del tratamiento a mantener o adoptar sistemas de tratamiento técnicamente compatibles. En otras palabras, se trata de que un mismo contenido pueda ser utilizado en equipos o plataformas distintos, pero no que los diferentes contenidos puedan operar en un mismo sistema sin generar conflictos.

Por su parte, la lectura mecánica no equivale a una accesibilidad digital (BOZDAG, 2018, 2). El considerando número 21 de la Directiva 2013/37/UE del Parlamento Europeo y del Consejo, de 26 de junio de 2013, por la que se modifica la Directiva 2003/98/CE relativa a la reutilización de la información del sector público[48], indica que «debe considerarse que un documento se presenta en formato legible por máquina si tiene un formato de archivo estructurado de tal forma que permite a las aplicaciones informáticas identificar, reconocer y extraer con facilidad los datos específicos que contiene. Los datos codificados en archivos estructurados en un formato legible por máquina son datos legibles por máquina. Los formatos legibles

por máquina pueden ser abiertos o propietarios; pueden ser normas formales o no serlo. Los documentos codificados en un formato de archivo que limita este procesamiento automático, por el hecho de que los datos no pueden extraerse o no pueden extraerse fácilmente de ellos, no deben considerarse documentos en un formato legible por máquina…».

La cuestión de la interoperabilidad es una de las dificultades prácticas a las que se enfrenta el derecho a la portabilidad de los datos. Por este motivo, tanto la doctrina como los organismos europeos han incidido en la conveniencia de que se desarrollen formatos interoperables, lo que requerirá la cooperación de los diversos actores implicados en cada sector (considerando número 68 del Reglamento; GRUPO DEL ARTÍCULO 29, 2016, 21; COMISIÓN EUROPEA, 2017, 15; DESGENS-PASANAU, 2018, 95-96). La interoperabilidad es un aspecto íntimamente ligado a la preocupación por favorecer la innovación y la competencia en el mercado[49]. Lo cual, como tendrá ocasión de explicarse, constituye uno de los objetivos principales del derecho a la portabilidad.

El Reglamento general de protección de datos ha renunciado a incluir un artículo como el 18.3 de la Propuesta, que otorgaba a la Comisión la facultad de especificar el formato electrónico estructurado y comúnmente utilizado que debían utilizar los responsables del tratamiento a la hora de transmitir los datos al interesado, así como también para determinar las normas técnicas, modalidades y procedimientos para la transmisión de datos personales entre sistemas. Se pretende mantener una flexibilidad que permita adaptarse a los diferentes sectores y a las numerosas categorías de datos, así como dejar la puerta abierta a la estandarización técnica. Por tanto, el derecho a la portabilidad constituye una obligación relacionada con el diseño tecnológico, pero tecnológicamente neutral (KAMARA, 2017, 7-12). Ciertamente, reconocer a la Comisión esa facultad parecía un paso bastante arriesgado, ya que cabe cuestionar la idoneidad de esa institución para proceder a la definición de estándares técnicos (GRAEF *et al.*, 2014, 5; GRAEF, 2015, 507-508). Otros, por el contrario, lamentan el paso atrás en la versión final del Reglamento (DE HERT *et al.*, 2018, 196).

El formato en el que el responsable entregue los datos personales debe ser adecuado con respecto al tipo de datos, pues lo contrario constituiría un impedimento u obstáculo a la portabilidad, y el interesado no tendría oportunidad de reutilizarlos en otros sistemas, que es lo que se persigue. Si en el sector o contexto de que se trata no hay formatos de uso común, algún autor considera que el responsable del tratamiento cumplirá con entregar los datos en el formato que utilice de manera efectiva en el momento de la solicitud (JANAL, 2017, 63). Pero el Grupo del artículo 29 mantiene que el responsable deberá proporcionarlos mediante la combinación de formatos abiertos de uso común y metadatos adecuados con el mayor grado de detalle

posible, consiguiendo así el nivel más elevado de funcionalidad (GRUPO DEL ARTÍCULO 29, 2016, 20-21).

Una vez examinado el contenido del derecho a la portabilidad, hay que destacar que la portabilidad *no* implica el borrado de los datos por parte del responsable del tratamiento que los transmite, por lo que el interesado podrá continuar disfrutando del servicio prestado por el responsable. El artículo 20.3 del RGPD dice que la portabilidad se entiende sin perjuicio del derecho a la supresión de los datos previsto en el artículo 17. En mi opinión pueden ejercitarse simultáneamente ambos derechos, pero hay autores que sostienen lo contrario (JANAL, 2017, 62). La solicitud sería entendida en el sentido de que el interesado pide al responsable la transmisión de los datos personales, a él mismo o a un tercero, y que, en cuanto se verifique que la transmisión ha sido correcta, proceda a su borrado[50].

En realidad, el ejercicio del derecho a la portabilidad de los datos personales no influye en el ejercicio de ningún otro derecho reconocido por el Reglamento. Tampoco supone una excepción al principio de limitación del plazo de conservación. En efecto, el artículo 5.1.e) del RGPD impone mantener los datos «de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales». Para ello, según el considerando número 39, el responsable del tratamiento debe establecer plazos para su supresión o su revisión periódica: el plazo de conservación debe ser el mínimo estricto. Pues bien, en modo alguno la existencia de un derecho a la portabilidad que el interesado pudiera querer ejercitar en el futuro faculta al responsable para conservar los datos por más tiempo del necesario (GRUPO DEL ARTÍCULO 29, 2016, 7-8).

Como último apunte, debe indicarse que la responsabilidad durante el proceso de portabilidad le corresponde al responsable del tratamiento que transmite los datos, quien deberá garantizar tanto la seguridad en la transmisión como que los recibe el destinatario correcto. Desde el momento en que la información se encuentre en poder del usuario o del otro responsable, el emisor deja de ser responsable respecto del fichero transmitido. Corresponderá entonces al interesado adoptar las medidas oportunas para proteger sus datos en los sistemas que utilice. El tercero receptor se convierte en responsable del tratamiento y asume las obligaciones derivadas del Reglamento, debiendo asegurarse de que, de entre los datos personales recibidos, solo trata aquellos pertinentes y necesarios, y para los fines específicos establecidos (GRUPO DEL ARTÍCULO 29, 2016, 4, 7-8, 18, 22-23). Téngase también en cuenta que, en virtud del artículo 82 del RGPD, la infracción de las normas del Reglamento genera en el infractor el deber de indemnizar a la persona que sufra daños —patrimoniales o no— como consecuencia de aquella.

5. Límites

El derecho a la portabilidad de los datos está sometido a dos límites específicos recogidos en los apartados tercero y cuarto del artículo 20. El primero de ellos dispone que el derecho no se aplica ni al tratamiento necesario para cumplir una misión realizada en interés público, ni al efectuado por el responsable del tratamiento en el ejercicio de poderes públicos que le hayan sido conferidos. Esta primera posibilidad no merece mayor comentario. Por su parte, el límite específico contenido en el artículo 20.4 del RGPD, de mayor interés, consiste en que el derecho a la portabilidad «no afectará negativamente a los derechos y libertades de otros». Se trata de una formulación amplia cuya interpretación resulta problemática.

Evidentemente, hay ocasiones en las cuales una misma información constituye datos personales de varias personas, como, por ejemplo, una fotografía en la que aparecen todas ellas. No es difícil darse cuenta de que, en tales casos, permitir a una portar sus datos puede afectar a las demás (GRIMMELMANN, 2009, 1192-1195; SWIRE y LAGOS, 2013, 348). Por este motivo, algunos autores observaban que el límite del artículo 20.4 del RGPD sería decisivo para la reducción del alcance del derecho (DE TERWANGNE *et al.*, 2017, 314), llegando incluso a cuestionar la utilidad de este último (GEUTER, 2018). Sin embargo, los eventuales conflictos no surgirán únicamente con relación a los datos personales de varios interesados. La limitación también es relevante a los efectos de eventuales derechos de propiedad intelectual de terceros o de la propia plataforma a la que se solicita la portabilidad, en particular derechos de autor, derechos *sui generis* sobre el contenido de una base de datos, y secretos comerciales (GRAEF, 2015, 507; GRUPO DEL ARTÍCULO 29, 2016, 14; GRAEF *et al.*, 2018, 1376-1378). Y no debe olvidarse que la propiedad intelectual está protegida por el artículo 17.2 de la Carta de los Derechos Fundamentales de la Unión Europea.

La implementación del derecho a la portabilidad también encuentra algunos obstáculos en el marco de la tecnología *blockchain*, puesto que la cadena permite observar un historial de transacciones que no afecta únicamente al interesado (POULENARD, 2018, 212). Para cumplir con el derecho a la portabilidad, y en general con las obligaciones derivadas del Reglamento, situar los datos personales fuera de la cadena de bloques y conservar en ella simplemente un indicador del lugar donde se aloja la información es una opción interesante. Sin embargo, esto cuenta con dificultades desde el punto de vista técnico, ya que, si bien los datos sobre la transacción sí pueden ser almacenados fuera de la cadena de bloques, no sucede lo mismo con las claves públicas (FINCK, 2018, 23, 29, 30 y 32).

Planteado el problema, debe descartarse un argumento que reduciría enormemente el alcance de la portabilidad. Dado que el artículo 20.1 del RGPD reconoce al interesado el derecho a recibir y a transmitir los datos personales que le incumban, podría afirmarse que, cuando el conjunto de datos afecte a varias personas, no habrá derecho a portarlos por no concernir únicamente al solicitante. Este argumento no debe triunfar. El artículo 20.4 del RGPD establece el criterio que debe aplicarse: que los derechos y libertades de terceros no se vean afectados negativamente; y el hecho de que la información concierna a varias personas no significa necesariamente que se produzca este efecto perjudicial (DE HERT *et al.*, 2018, 197-198). De este modo, los registros que contienen datos personales tanto del interesado como de otras personas incumben a todos ellos, si bien el nuevo responsable deberá excluir cualquier tratamiento que afecte negativamente a los derechos y libertades de esas otras personas (GRUPO DEL ARTÍCULO 29, 2016, 11).

Dicho lo anterior, ¿cómo interpretar el artículo 20.4 del RGPD, y dónde situar la línea de los efectos negativos para terceros? En la doctrina, algún autor planteó dos posibles enfoques. El primero consistía en permitir la portabilidad únicamente cuando los datos personales, recibidos por el nuevo responsable, se mantuviesen bajo el control exclusivo de la persona que había ejercido su derecho a la portabilidad, y siempre que tales datos fuesen utilizados para fines puramente personales o domésticos[51]. Considerando esta primera opción demasiado restrictiva, proponía una segunda basada en las expectativas razonables del tercero cuyos derechos se ven afectados. Cuando la expectativa fuese que sus datos permanecerían en una determinada plataforma, como parece ser el caso en las redes sociales, la portabilidad de los datos que les conciernan también a ellos no sería posible. Por el contrario, cuando no tuviesen esa expectativa, por ejemplo, en el marco de la utilización de una plataforma de correo electrónico, el artículo 20.4 del RGPD no supondría obstáculo a la transmisión de los datos (JANAL, 2017, 62).

Esta segunda propuesta cuenta con una ventaja. Si el Reglamento pone el énfasis en el control de los datos por parte de los interesados, parece lógico preocuparse por que los terceros afectados también mantengan un cierto control sobre los suyos. El criterio de las expectativas razonables es plenamente coherente con ello (GRIMMELMANN, 2009, 1195-1197). Indudablemente, determinar cuáles son estas expectativas en cada caso concreto no es una tarea sencilla[52]. Pero tampoco lo es dilucidar cuándo los derechos y libertades de terceros se ven afectados de manera negativa. En contra de adoptar como referencia las expectativas razonables, el argumento más claro es que no necesariamente plasmará el criterio del efecto negativo establecido por el legislador europeo.

Reflexionando sobre la cuestión, el Grupo del artículo 29 considera que los derechos y libertades de terceros se verán afectados negativamente

cuando la portabilidad les impida ejercer los derechos que, como interesados, les reconoce el Reglamento. Sostiene dicho grupo que, si la tercera persona afectada no otorga su consentimiento al nuevo responsable, este deberá buscar otro fundamento para el tratamiento de datos, como por ejemplo un interés legítimo [art. 6.1.f) del RGPD] consistente en prestar un servicio al interesado que permita a este último tratar datos para una actividad personal o doméstica. Como ejemplos se proporcionan, por un lado, la lista de correos electrónicos y de contactos de un servicio de correo web, y, por otro, la cuenta bancaria del interesado que contiene transacciones con y datos personales de otras personas. Ahora bien, para que no se produzca un efecto negativo sobre los derechos de terceros, el nuevo responsable del tratamiento debe abstenerse de utilizar los datos personales para otros fines, tales como enriquecer el perfil del tercero o proponerle bienes y servicios. De las directrices del Grupo del artículo 29 resulta, pues, que el tratamiento de los datos personales de terceros por parte del responsable del tratamiento receptor solo está permitido cuando los datos permanezcan bajo el control exclusivo del usuario y sean gestionados únicamente para necesidades personales o domésticas (GRUPO DEL ARTÍCULO 29, 2016, 13-14). No obstante, el Grupo precisa que «los responsables del tratamiento receptores no están obligados a aceptar y tratar datos personales que se hayan trasmitido a raíz de una solicitud de portabilidad de datos» (GRUPO DEL ARTÍCULO 29, 2016, 8).

En relación con el conflicto entre el derecho a la portabilidad y los derechos de propiedad intelectual y secretos industriales de terceros, ciertas organizaciones se han mostrado especialmente preocupadas por los segundos. Aun cuando reconocían que la existencia de tales derechos de terceros no debía permitir escudarse en ellos para impedir u obstaculizar la portabilidad, incidieron en el riesgo de que los receptores de los datos consiguiesen una ventaja injusta a partir de información que había sido analizada por el transmitente empleando sus propios recursos. Por ello, emplazaban al Grupo del artículo 29 para desarrollar la versión inicial de las Directrices sobre el derecho a la portabilidad (CENTRE FOR INFORMATION POLICY LEADERSHIP, 2017, 10).

En la versión revisada y finalmente adoptada, el citado grupo realiza algunas precisiones adicionales sobre la cuestión, aunque lo cierto es que no se explaya demasiado[53]. Al igual que sucede con la presencia de datos personales de terceros, la concurrencia de derechos de propiedad intelectual, de secretos comerciales o de un riesgo empresarial relacionado con ellos no es suficiente por sí sola para denegar una solicitud de portabilidad; pero sí deben ser tomados en consideración por el responsable antes de responder a la misma. Se dice que el derecho a la portabilidad no ampara usos indebidos de la información, tales como prácticas desleales o violación de

los derechos de propiedad intelectual. Y se concluye que los responsables del tratamiento pueden segmentar los datos facilitados por los interesados con el fin de transmitir solo aquellos que no revelen información protegida (GRUPO DEL ARTÍCULO 29, 2016, 14).

Podría pensarse que, cuando los datos afecten a derechos de propiedad intelectual de terceros, la solicitud de portabilidad solo será atendida respecto de los datos que no produzcan tal afectación (VOIGT y VON DEM BUSSCHE, 2017, 173). Sin embargo, parece más correcto concluir que en realidad se impone una ponderación de intereses en la que es necesario distinguir los usos que, de la información protegida por derechos de propiedad intelectual, harán el interesado y el nuevo responsable del tratamiento. El motivo es que el límite del artículo 20.4 del RGPD no reside en una simple interferencia con los derechos de terceros, sino en un efecto negativo sobre ellos, y este efecto es más complicado que se produzca si se considera el uso de los datos por los interesados —quienes, además, pueden estar protegidos por ciertas excepciones y limitaciones a los derechos de propiedad intelectual— que si se toma como referencia al empresario receptor, nuevo responsable del tratamiento (GRAEF *et al.*, 2018, 1379-1381).

Una posible solución al problema de la portabilidad de los datos que afectan a varias personas es la selección de la información específica que será transmitida (GRUPO DEL ARTÍCULO 29, 2016, 14). Ello requiere aplicar en el ámbito del derecho a la portabilidad lo dispuesto para el derecho de acceso en el considerando número 63 del Reglamento. En él se afirma que el derecho de acceso no debe afectar negativamente a los derechos y libertades de terceros, se matiza que ello no debe implicar una negativa total a suministrar toda la información, y se permite al responsable pedir al interesado que especifique los concretos datos o actividades de tratamiento que considera en su solicitud. Sin embargo, como ya se ha dicho, la posibilidad de aplicar este considerando a la portabilidad no es del todo segura (DIKER VANBERG y ÜNVER, 2017, 5). Además, en ocasiones resultará difícil separar los datos personales del interesado de los derechos de propiedad intelectual (GRAEF *et al.*, 2018, 1375).

En todo caso, garantizar la correcta aplicación del límite contenido en el artículo 20.4 del RGPD resulta verdaderamente difícil, si no imposible, si el responsable del tratamiento pretende ofrecer una herramienta completamente automática que el interesado pueda utilizar por sí mismo para solicitar la portabilidad y recibir los datos (VOIGT y VON DEM BUSSCHE, 2017, 172; BOZDAG, 2018, 4).

Dejando a un lado los límites específicos del derecho a la portabilidad, hay que decir que este también podrá verse sometido a límites establecidos de conformidad con el artículo 23 del RGPD. Su apartado primero faculta a la Unión y a los Estados miembros para adoptar medidas legislativas

que limiten el alcance de lo dispuesto en los artículos 12 a 22, y 34, del RGPD. Ahora bien, estas limitaciones deben respetar el contenido esencial de los derechos, así como responder a criterios de necesidad y de proporcionalidad en el marco de una sociedad democrática. Además, se incluye una lista tasada de los intereses que pueden justificar la adopción de las citadas limitaciones. Ya con relación a la Propuesta de Reglamento de 2012, algunos vieron en la citada facultad una potencial fuente de fragmentación normativa (GILBERT, 2012, 858-860).

El derecho a la portabilidad también puede ser objeto de excepciones en el caso de tratamiento de datos con fines de archivo en interés público. El artículo 89.3 del RGPD faculta al Derecho de la Unión y a los Derechos nacionales para prever tales excepciones —no solo con relación a la portabilidad, sino también respecto de otros derechos—. Esta prerrogativa está condicionada a que el derecho objeto de limitación pueda imposibilitar u obstaculizar gravemente la consecución de los fines perseguidos con el tratamiento. En todo caso, las excepciones deben ser necesarias y proporcionadas, establecerse bajo condiciones específicas y asegurar unas garantías adecuadas para los interesados[54]. Por el contrario, el Reglamento no incluye el derecho a la portabilidad entre los que pueden ser objeto de excepciones en caso de tratamiento de datos con fines estadísticos o de investigación científica o histórica, supuesto previsto en su artículo 89.2.

6. El carácter *a priori* gratuito del ejercicio del derecho a la portabilidad

El derecho a la portabilidad no conllevará, en principio, ningún coste para el interesado. El artículo 12.5 del RGPD proclama el carácter gratuito tanto de la información que debe ser facilitada con arreglo a los artículos 13 y 14, como de todas las comunicaciones y actuaciones derivadas de los artículos 15 a 22 y 34. No obstante, al responsable del tratamiento se le conceden dos opciones cuando las solicitudes sean «manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo» (extremo que corresponde demostrar a dicho responsable, según señala expresamente el artículo 12.5): bien cobrar un canon razonable, bien negarse a llevar a cabo actuación alguna. Son varias las cuestiones que merecen un comentario.

En primer lugar, la gran exigencia del artículo 12.5 del RGPD para que el responsable pueda hacer uso de las dos facultades mencionadas, pues se alude a un carácter *manifiestamente* infundado o excesivo de la solicitud (VOIGT y VON DEM BUSSCHE, 2017, 148).

En segundo lugar, este carácter puede determinarse aplicando cualesquiera criterios, pues lo repetitivo de las solicitudes no es más que un

ejemplo, como demuestra el uso del adverbio «especialmente». Ahora bien, todo criterio debe referirse al propio interesado, y no a terceros o al propio sistema técnico puesto en marcha para cumplir con las solicitudes. En otras palabras, como ha observado el Grupo del artículo 29, el responsable del tratamiento no puede cobrar un canon o negarse a actuar por que muchos solicitantes se hayan dirigido a él o por que el sistema de atención de solicitudes le suponga un gran coste. Por el contrario, discrepo de ese mismo grupo cuando dice que, dado que el uso de sistemas automatizados de datos personales reduce la carga que representan las solicitudes repetitivas, habrá pocas situaciones en las que esté justificada la negativa del responsable (GRUPO DEL ARTÍCULO 29, 2016, 17). El Reglamento permite cobrar un canon o negarse a actuar cuando las solicitudes sean manifiestamente infundadas o excesivas. Por consiguiente, cuando una solicitud pueda calificarse así, es irrelevante que al responsable del tratamiento no le suponga una carga excesiva.

Que al responsable no le suponga un gran coste, sin embargo, sí es relevante a la hora de establecer la cuantía del canon que podría eventualmente cobrar. Como tercer apunte, según dispone el artículo 12.5 del RGPD, dicho canon debe ser razonable «en función de los costes administrativos afrontados para facilitar la información o la comunicación o realizar la actuación solicitada». De todas formas, tampoco está claro que al responsable del tratamiento no le suponga un gran coste el ejercicio del derecho a la portabilidad por el hecho de contar con herramientas automatizadas. Como ya se ha explicado, la portabilidad no puede afectar negativamente a los derechos de terceros, y examinar el respeto de esta exigencia probablemente requiera siempre una intervención humana, de modo que el proceso no será tan automatizado y ágil.

7 Portabilidad de datos personales y derecho a la transparencia. El plazo para atender la solicitud de portabilidad

Las referencias a la transparencia en el Reglamento general de protección de datos son ciertamente numerosas, algo que no sorprende. La normativa se inspira en el control de las personas sobre la información que les concierne, lo que requiere la toma de decisiones con conocimiento de causa. La Directiva sobre datos personales también contenía disposiciones sobre transparencia, pero los esfuerzos del Reglamento para mejorar este aspecto eran necesarios, toda vez que los usuarios no siempre son conscientes de la información que se les transmite —a menudo, sencillamente porque no es leída— (DE TERWANGNE *et al.*, 2017, 312). Resulta especialmente interesante el considerando número 39 del Reglamento, que se refiere al principio

de transparencia diciendo que exige que «toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro […] Las personas físicas deben tener conocimiento de los riesgos, las normas, las salvaguardias y los derechos relativos al tratamiento de datos personales así como del modo de hacer valer sus derechos en relación con el tratamiento»[55].

La preocupación por la transparencia se plasma fundamentalmente en los artículos 12 («Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado»), 13 («Información que deberá facilitarse cuando los datos personales se obtengan del interesado») y 14 («Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado»), a lo que podría añadirse el derecho de acceso a los datos reconocido en el artículo 15 del RGPD. Centrándonos en el derecho a la portabilidad, el Reglamento impone expresamente la obligación de informar sobre su existencia [arts. 13.2.b) y 14.2.c) del RGPD].

Sin embargo, los contornos del deber de transparencia permanecen inciertos: ¿qué actuaciones concretas deben llevarse a cabo para garantizar que las personas conocen tanto los derechos relacionados con el tratamiento de datos personales como el modo de hacerlos valer? Indudablemente, las empresas tienen incentivos para suministrar un volumen de información tan amplio como sea posible, a los efectos de minimizar el riesgo de incumplimiento. Pero ello puede perjudicar en última instancia a los usuarios, que se verán inundados por una gran cantidad de información que no retendrán, por lo que no habrá un mayor conocimiento efectivo. Se trata del conocido problema de la sobrecarga de información (BEN-SHAHAR y SCHNEIDER, 2011, 687-688 y 719). Precisar más las obligaciones de información deviene crucial, puesto que difícilmente los usuarios estarán en disposición de hacer uso del derecho a la portabilidad y extraer toda su utilidad si no conocen su contenido y funcionamiento (DIKER VANBERG y ÜNVER, 2017, 6).

De acuerdo con las Directrices del Grupo del artículo 29, en el momento de informar sobre la existencia del derecho a la portabilidad, deberá garantizarse que se distingue claramente este derecho de otros, en particular del derecho de acceso. Esto incluye la diferencia en cuanto a los tipos de datos relevantes a los efectos de cada uno de ellos. Cuando sean varios los formatos en los que los datos portables pueden ser suministrados, el responsable del tratamiento debe explicar la repercusión de las diversas opciones. Si la transmisión directa entre responsables se ve impedida por motivos técnicos, tendrá que informar sobre las dificultades existentes. En la medida en que la recuperación de los datos por parte del interesado genera riesgos de seguridad, se dice que el responsable del tratamiento debe informar al

usuario de que corresponde a este adoptar las medidas oportunas para reducir los riesgos de conservación de la información recibida; si bien se apunta que, como práctica óptima, el responsable del tratamiento puede hacer recomendaciones en cuanto a formatos, herramientas de cifrado y otras medidas de seguridad. Por último, si el usuario desea cerrar una cuenta, se recomienda al responsable incluir de nuevo información sobre el derecho a la portabilidad, con el fin de que el usuario pueda recibir sus datos y transferirlos a un tercero antes del cierre efectivo de aquella (GRUPO DEL ARTÍCULO 29, 2016, 15 y 21-23).

En cuanto al plazo para responder a una solicitud de portabilidad, este será, en principio, de un mes. De conformidad con el artículo 12.3 del RGPD, cualquier solicitud de un interesado con base en los artículos 15 a 22 del RGPD genera para el responsable del tratamiento la obligación de informar sobre sus actuaciones al respecto en dicho plazo[56]. No obstante, se admite una prórroga por dos meses adicionales cuando ello sea necesario por el número o la complejidad de las solicitudes. Si el responsable se sirve de la facultad de prorrogar el plazo, debe informar al interesado y explicarle los motivos que le llevan a ello dentro del mes siguiente a la solicitud. El canal por el que debe suministrarse la información debida no es enteramente libre. Si el interesado realiza su solicitud por medios electrónicos, la respuesta debe proporcionarse también por tales medios —cuando ello sea posible—, salvo que el interesado haya manifestado su voluntad de que se le haga llegar de otro modo. Por el contrario, el Reglamento no dice nada si el medio utilizado por el interesado no es electrónico.

El artículo 12.4 del RGPD impone al responsable del tratamiento, para el caso de que este no dé curso a una solicitud, un deber de información tanto sobre las razones de la negativa como de la posibilidad de reclamar ante una autoridad de control o ante los tribunales. Esta obligación debe satisfacerse «sin dilación», y, en todo caso, dentro del mes siguiente a la recepción de la solicitud. Si hubiese dificultades técnicas que hiciesen imposible la transmisión de los datos entre responsables, la negativa del responsable del tratamiento a la portabilidad directa será considerada como tal a los efectos del artículo 12.4 del RGPD (GRUPO DEL ARTÍCULO 29, 2016, 18).

8. ¿Son válidas la renuncia del interesado al derecho a la portabilidad y la limitación contractual del derecho por el responsable del tratamiento?

El Reglamento no se pronuncia expresamente ni sobre la posibilidad de renunciar al derecho a la portabilidad —absoluta o solo con carácter temporal—, ni sobre las eventuales limitaciones contractuales al mismo que

pudiera prever el responsable del tratamiento. Su validez es por lo tanto dudosa. Quizás las renuncias y limitaciones al derecho a la portabilidad se rijan por cada Derecho nacional, aunque esto conllevaría un riesgo de fragmentación normativa. El tema merece un análisis más pausado que el que puede dedicársele en el presente estudio, por lo que solo se harán algunas observaciones generales al respecto.

Una respuesta negativa a la validez de las limitaciones contractuales del derecho a la portabilidad encuentra apoyo en el artículo 20 del RGPD, que dice que el responsable del tratamiento no puede poner impedimentos a la portabilidad del interesado. Desde un punto de vista más abstracto, también puede fundamentarse en la importancia del derecho a la portabilidad y en su relación con el derecho fundamental a la protección de datos; así como en los objetivos perseguidos por la norma —que se comentarán en el próximo apartado—, los cuales se verían menoscabados si se tolerasen limitaciones y exclusiones. Sin embargo, cuando el responsable trata los datos personales con varios fundamentos distintos al mismo tiempo, recabando el consentimiento del interesado a pesar de que no le sería necesario, cabe sostener la validez de excluir contractualmente la portabilidad: este derecho solo surge cuando el tratamiento de los datos se basa en el consentimiento o es necesario para la ejecución de un contrato, y el responsable habría recabado dicho consentimiento para reforzar su posición, no para empeorarla obligándose a garantizar la portabilidad[57].

En realidad, la posibilidad de limitar contractualmente el derecho a la portabilidad conecta con un debate mucho más amplio, que es el referente al grado de autonomía y de libertad contractual deseable en materia de protección de datos, especialmente en el marco de contratos relacionados con el mundo digital. Se trata de un debate tan interesante como inevitable en la época contemporánea, pero entrar en él nos alejaría demasiado de la perspectiva del trabajo[58].

Simplemente planteando sus términos generales, en un lado se sitúan las posiciones escépticas sobre la conveniencia de dejar un mayor espacio a la libertad contractual, en un contexto de complejidad tecnológica y de sobrecarga informativa que incrementa la posición de debilidad de algunos contratantes (LUQUIN BERGARECHE, 2018, 265, 271-272 y 277-283). Se cuestiona el control como piedra angular en materia de protección de datos, defendiendo la necesidad de que las personas cuenten con «menos, pero mejores» elecciones (HARTZOG, 2018). Estas opiniones parecen sólidas, sobre todo si se repara en que, por el momento, las personas no cuentan con una adecuada comprensión de los riesgos relacionados con la intimidad en el entorno digital[59]. Además, esta corriente no se encuentra demasiado alejada de lo que viene siendo el espíritu de, en particular, las normas de protección de los consumidores. Pero estas opiniones escép-

ticas podrían ser objeto de críticas por su carácter paternalista (ZARSKY, 2017, 1007) —con sus numerosos ángulos (RIZZO y WHITMAN, 2009, 908-909)—. También se dirá que, si las personas están interesadas en una mayor protección de datos, las empresas tienen incentivos para responder a esas preferencias (BEAUGRAND *et al.*, 2017, 230 y 240); posiblemente utilizando el argumento de que las cláusulas contractuales son características del propio bien o servicio que se contrata, formando todo ello un conjunto inseparable cuyo resultado global se integra en el precio (EASTERBROOK, 1996, 214-215)[60].

Un aspecto que quizás influya en el devenir de la discusión sea la eventual proliferación de sellos y certificaciones que garanticen un determinado nivel de protección en materia de datos. Estos instrumentos son promovidos por el propio Reglamento general de protección de datos (art. 42)[61], pueden aumentar la transparencia del mercado, y las empresas se servirían de ellos en el proceso competitivo[62]. No obstante, será necesario esperar un tiempo para observar si son lo suficientemente eficaces. Hay otro aspecto que podría ir ganando en importancia, decantando la balanza a favor de una mayor autonomía del consumidor en el entorno digital. Es el hecho, reconocido por quienes no son tan favorables a dejar a la libertad contractual un amplio margen de actuación en este ámbito, de que la rapidez con la que aparecen las novedades tecnológicas hace que el legislador deba responder a ellas «con escaso margen temporal para una reflexión serena» (LUQUIN BERGARECHE, 2018, 276). Si no hay tiempo para llevar a cabo un análisis profundo de la situación, hay quien dirá que resulta conveniente decantarse por normas dispositivas; especialmente cuando se trata de nuevas tecnologías, un campo complejo y dinámico en el que la probabilidad de adoptar una norma errónea o ineficiente es más elevada que en otros (EASTERBROOK, 1996, 207-211, 215-216). Pero este argumento no convencerá a todo el mundo.

Con respecto a las renuncias *a posteriori* al derecho a la portabilidad de los datos por parte del interesado, conviene diferenciar dos situaciones.

La *primera* es la renuncia, temporal o permanente, articulada a través de un contrato con el responsable del tratamiento a cambio de ciertas ventajas. La clave para dilucidar la validez de esta renuncia quizás resida en determinar si el derecho a la portabilidad de los datos personales pertenece a un orden público (económico) «de dirección» o «de protección». En el primer caso, el legislador quiere ordenar la actividad económica y contractual de una determinada manera, por lo que una derogación de la norma iría en contra del objetivo perseguido. En el segundo caso, se trata de reequilibrar una situación, interviniendo en favor de una de las partes (TERRÉ *et al.* 2013, 426-431). En este segundo caso, una vez que las normas de protección han podido cumplir con su cometido, la renuncia a la protección dispensada

por el ordenamiento no atenta contra los objetivos del legislador, por lo que no parece haber motivo para impedirla. Un ejemplo claro es el derecho que tiene el consumidor a oponerse a que un juez declare abusiva una cláusula, después de que dicho juez le haya informado de la existencia de una estipulación que considera abusiva y por tanto no vinculante, facultándose al consumidor para que preste en ese momento un consentimiento libre e informado (algo que solo hará, cabe suponer, si el empresario le ha ofrecido determinados beneficios en contrapartida)[63].

El caso del derecho a la portabilidad resulta complejo. Como podrá comprobarse, en él confluyen el derecho fundamental a la protección de datos, la voluntad de reforzar la posición del interesado otorgándole más control sobre su información personal, y la promoción de la competencia. Todo dependería, en consecuencia, de a cuál de estas dimensiones se le otorgase más importancia. A mi juicio, debe primar la vertiente del control de la persona sobre los datos que le conciernan, por lo que considero que la renuncia *a posteriori* a cambio de una contrapartida debe ser válida, favoreciendo así la autonomía personal. La primacía de la vertiente del control puede apoyarse en el considerando número 68 del Reglamento, que comienza diciendo «para reforzar aún más el control sobre sus propios datos», explicando después el derecho a la portabilidad.

La *segunda* situación es la renuncia temporal que pretende el interesado sin ningún tipo de contrapartida por parte del responsable del tratamiento. En mi opinión, esta renuncia —que no es tan extraña como pudiera parecer— también debería ser válida. La portabilidad genera el riesgo de que, con un solo acceso no autorizado a los datos de una persona, estos sean fácilmente transferidos a un tercero (SWIRE y LAGOS, 2013, 373-375). Reconocer a las personas la facultad de *suspender* su derecho a la portabilidad aumenta la seguridad digital, siendo un instrumento particularmente interesante para cuando se alberguen dudas sobre la seguridad de una cuenta (CENTRE FOR INFORMATION POLICY LEADERSHIP, 2017, 11), de manera similar a la suspensión temporal de acceso a la propia cuenta que ya permiten ciertas plataformas.

IV. ALGUNAS REFLEXIONES EN TORNO AL DERECHO A LA PORTABILIDAD DE LOS DATOS PERSONALES

En este apartado se exponen, en primer lugar, los objetivos perseguidos mediante el reconocimiento del derecho a la portabilidad. Tales objetivos son loables, y resulta sencillo identificar los beneficios que se pueden derivar de él. Ahora bien, no pueden desconocerse ciertos efectos negativos potenciales del derecho estudiado, algo que se comentará a continuación.

1. Los objetivos del derecho a la portabilidad

El derecho a la portabilidad se inscribe en el Reglamento general de protección de datos, lo que hace que su función en el plano más general sea el de una de las piezas que permiten alcanzar los objetivos de dicho texto normativo. En consecuencia, el derecho se integra en un régimen jurídico dirigido a garantizar un derecho fundamental como es la protección de datos personales y a facilitar la circulación de estos en la Unión Europea (GRAEF *et al.*, 2018, 1366-1367). No cabe duda de que uno de los efectos principales del derecho a la portabilidad es reforzar el control de las personas sobre sus datos, tal y como refleja el considerando número 68 del Reglamento. De hecho, la norma estándar ISO/IEC 19941:2017, en materia de interoperabilidad y portabilidad en *cloud computing*, define la portabilidad de los datos como la capacidad para transferirlos fácilmente de un sistema a otro sin tener que reintroducirlos (art. 3.2.1). Todo ello evoca claramente el control —e incluso la propiedad (SWIRE y LAGOS, 2013, 373; GRAEF *et al.*, 2018, 1368)— sobre el contenido objeto de transferencia (DE HERT *et al.*, 2018, 201). Además, la portabilidad genera una mayor visibilidad de los datos personales tratados (VAN OOIJEN y VRABEC, 2019, 102-103). Por ello, supone un paso hacia la «soberanía digital» (FOX, 2018).

Cuestión distinta es que, según algunos autores, el Reglamento no responda correctamente a las conclusiones efectuadas por estudios sobre el comportamiento y la psicología de los consumidores, de tal forma que sus disposiciones no sean todo lo eficaces que podrían desde el punto de vista de la promoción de una verdadera autonomía (VAN OOIJEN y VRABEC, 2019).

A su vez, las nociones de control, de capacidad de elección y de soberanía, conducen a la autodeterminación personal —incluyendo su dimensión informativa— y al libre desarrollo de la personalidad —pudiendo hablarse de una personalidad digital— (ZANFIR, 2012, 151-152, 155 y 161; ZARSKY, 2017, nota 53). Finalmente, el derecho a la protección de datos se relaciona con el derecho a la intimidad, si bien ambos son derechos autónomos (VAN DER SLOOT, 2017, 5-8). En definitiva, el derecho a la portabilidad contribuye a la dimensión más personal de la protección de datos.

Al mismo tiempo, la portabilidad permite reequilibrar la relación existente entre los responsables del tratamiento de datos personales y los interesados, garantizado que estos últimos «desempeñan un papel activo en el ecosistema de datos» (GRUPO DEL ARTÍCULO 29, 2016, 4). Esta observación sirve de enlace con el fundamento más comercial o economicista del derecho a la portabilidad[64]. En esta línea, surgen eslóganes como «Mis datos son míos», cuya formulación en inglés *My data is mine* es el título de la declaración firmada por varias asociaciones de consumidores —entre

ellas la española Organización de Consumidores y Usuarios (OCU)— en junio de 2017 para reivindicar que el desarrollo de la economía digital debe producirse respetando los derechos fundamentales, y en particular la intimidad, el respeto a la vida privada y la protección de datos[65]. En efecto, cuando se comenta el derecho a la portabilidad, a menudo se acentúan sus ventajas desde el punto de vista del mercado y de la competencia. Confluyen así la protección de datos y un marcado carácter económico (DE HERT *et al.*, 2018, 195-196).

Por ejemplo, se apunta a la generación de confianza entre los consumidores con respecto al entorno digital, favoreciendo así el desarrollo económico y la innovación (REDING, 2012, 124; ZANFIR, 2012, 153, 154 y 157; VOIGT y VON DEM BUSSCHE, 2017, 2; COMISIÓN EUROPEA, 2018, 1). Detenerse en este argumento resulta innecesario, pues la relación entre la confianza y el desarrollo del mercado es ampliamente conocida, sirviendo como fundamento de numerosas disposiciones legislativas relacionadas con la protección de los consumidores en el ámbito de la Unión Europea (TWIGG-FLESNER, 2016, 184-186)[66].

Asimismo, en una economía digital con grandes empresas que manejan ingentes cantidades de datos, la portabilidad reduciría los riesgos de monopolización, al mismo tiempo que permite que los usuarios se beneficien de la creación de riqueza generada a partir del tratamiento de su información personal (VAN OOIJEN y VRABEC, 2019, 102). La posibilidad de recibir y transmitir fácilmente datos personales reduce la dependencia de los empresarios con los que ya se ha contratado, esto es, disminuye el efecto «cerrojo» o «retención» (*lock-in effect*). La portabilidad favorece la movilidad de los clientes al facilitar el cambio de proveedores y de sistemas (JANAL, 2017, 60; JÜLICHER y DELISLE, 2017, 88), y aumenta las posibilidades de compartir y reutilizar datos, con el consecuente incremento de oportunidades de beneficiarse de servicios complementarios (ZANFIR, 2012, 152; GRAEF *et al.*, 2018, 1369 y 1387); algo especialmente importante cuando las personas almacenan y utilizan sus datos en la nube y de manera descentralizada (MULA, 2018). Recuérdese que el derecho a la portabilidad de los datos personales no implica el borrado de estos por parte del primer responsable del tratamiento-transmitente, lo que muestra a las claras la voluntad de alcanzar una interconexión de sistemas (DE HERT *et al.*, 2018, 202-203).

El derecho a la portabilidad también puede ser una herramienta de la que se sirvan los empresarios para obtener información, proponiendo a sus clientes —o a potenciales clientes— ejercer su derecho respecto de otros responsables del tratamiento para transmitirles después a ellos los datos obtenidos, a cambio de ciertas ventajas (GRAEF *et al.*, 2018, 1382 y 1387).

Todo esto abre un gran abanico de posibilidades para las empresas, que podrán innovar, crecer, establecerse y mejorar sus prestaciones, con los correspondientes beneficios para los usuarios (GRUPO DEL ARTÍCULO 29, 2016, 4-6). El incremento de la competencia por esta vía previsiblemente desembocará en una bajada de los precios y en la aparición de nuevos modelos de negocio (BAPAT, 2013, 4; BEAUGRAND *et al.*, 2017, 41, 230 y 232). A medida que la tecnología evolucione, aumentará el número de situaciones en las cuales disfrutar de la portabilidad resultará útil. Piénsese, por ejemplo, en los denominados «consumidores algorítmicos». Las personas no solo se auxiliarán de algoritmos para tomar decisiones económicas, sino que, directamente, delegarán estas decisiones en los propios sistemas automatizados. Estos sistemas actuarán con base en determinados parámetros preestablecidos —susceptibles de actualización mediante *self-learning*— y a partir de la información acumulada sobre las preferencias, intereses y patrones de comportamiento de los usuarios. La portabilidad de los datos permitiría cambiar fácilmente de un algoritmo a otro[67].

En resumen, el derecho a la portabilidad, aun cuando tenga como primer objetivo reforzar el control de las personas sobre sus datos, incide positivamente en otras esferas, en particular de ámbito económico: favorece la circulación de datos, aumenta la confianza de los consumidores, reduce el efecto cerrojo y promueve la competencia, elementos necesarios para el buen funcionamiento del mercado único digital.

Los mismos argumentos, a saber, el aumento del control sobre la información que afecta a una persona y la promoción de la competencia, aparecen con relación a otras iniciativas ligadas a la portabilidad. Por ejemplo, el «Grupo de Investigación sobre Derecho de los servicios digitales» ha elaborado un *Discussion Draft of a Directive on Online Intermediary Platforms* cuyo artículo 8.5 recoge un derecho a la portabilidad de las opiniones emitidas o recibidas en línea (RESEARCH GROUP ON THE LAW OF DIGITAL SERVICES, 2016). En él se dice que, finalizado el contrato entre la plataforma y el profesional o entre la plataforma y el cliente, el operador de la plataforma debe facilitar una función que permita la transferencia de las evaluaciones en línea (*reviews*) a otro sistema de *feedback* reputacional, en un formato estructurado, de uso común y lectura mecánica. Aparece el concepto de «capital reputacional», en el sentido de que la reputación digital acumulada pertenece a la persona sobre la que versa la información —lo que reenvía a las ideas de control y de propiedad—, al mismo tiempo que se destaca la mayor facilidad para cambiar de plataforma, evitando el citado efecto cerrojo —lo que se relaciona con la competencia— (BUSCH, 2018, 55-56).

Tanto si se atiende a la dimensión más personal de la protección de datos, como si es la vertiente economicista la que recibe atención, el derecho a la

portabilidad se presenta como un atractivo mecanismo para alcanzar los objetivos pretendidos. Objetivos que, por otra parte, son difícilmente criticables. Así las cosas, las virtudes del derecho a la portabilidad parecen obvias.

Evidentemente, nada es perfecto. Es posible argumentar que la configuración del derecho a la portabilidad según el artículo 20 del RGPD implica automáticamente poner obstáculos al cumplimiento de sus finalidades protectora y competitiva. Por un lado, porque solo engloba datos personales, y, por otro, porque se excluyen los datos personales no facilitados por el interesado (JANAL, 2017, 63-64). Estas críticas apuntarían en la dirección de que la normativa se ha quedado corta. Sin embargo, en el siguiente subapartado se adoptará la perspectiva contraria, a saber, que el artículo 20 del RGPD podría haber ido demasiado lejos.

2. Algunos efectos negativos potenciales del derecho a la portabilidad

Antes de abordar la cuestión, conviene subrayar que no se pretende presentar una enmienda a la totalidad del derecho a la portabilidad, ni afirmar que comporta más desventajas que beneficios. Esto requeriría un estudio más exhaustivo, por lo que no es posible extraer semejante conclusión de las observaciones que siguen. Si este subapartado es más extenso que el anterior, ello no se debe a que existan más argumentos en contra del derecho a la portabilidad que a su favor. El motivo es que las ventajas del derecho a la portabilidad son más claras, mientras que sus potenciales efectos negativos requieren una mirada más pausada, resultando en ocasiones contraintuitivas. Dicho lo cual, hay tres razones que recomiendan no omitir ciertas debilidades del derecho a la portabilidad. La primera, ofrecer un análisis equilibrado de la realidad objeto de estudio. La segunda, vislumbrar posibles causas por las cuales quizás no se consigan los beneficios pretendidos. Y la tercera, plantear el origen de nuevos problemas que podrían surgir, algo esencial para su eventual solución.

Desde el punto de vista de la portabilidad como un derecho que concreta o materializa la protección de datos, cabría preguntarse si una proliferación de los derechos subjetivos resulta en una especie de banalización de los derechos fundamentales. Numerosas voces manifiestan la necesidad no solo de reconocer nuevos derechos digitales, sino también de dotarlos de un reconocimiento a nivel constitucional. Así, una mayor circulación de datos personales debería ir acompañada de la creación y el fortalecimiento de derechos individuales relacionados (RALLO, 2018, 150-151). Se trata no de ver la tecnología como algo negativo, sino de asegurar que en la sociedad tecnológica del futuro los derechos individuales son la preocupación central (HOSEIN, 2018, 148). Sin embargo, algunos autores ya han abierto el debate

sobre en qué medida la protección de datos a nivel europeo constituye un verdadero derecho fundamental. Se dice que algún aspecto de la protección de datos sí alcanza ese umbral —por ejemplo, los datos sensibles—, al mismo tiempo que se constata que muchos otros no responden a los estándares clásicos de los derechos fundamentales[68]. El detalle de la regulación europea sobre la materia, el tipo de regulación aprobada, el procedimiento legislativo (SWIRE y LAGOS, 2013, 366-369), y el hecho de que las normas parezcan establecer un compromiso de intereses (ZARSKY, 2017, 1002-1003), son elementos que inclinan a pensar que parte de la normativa de protección de datos constituye, más bien, una regulación del mercado que guarda una cierta relación con la protección de los consumidores (VAN DER SLOOT, 2017, 19-28).

Sea como fuere, el reconocimiento de nuevos derechos —posiblemente necesario a medida que se produzca un mayor desarrollo tecnológico— nunca debería perder de vista que ello implica a menudo la imposición de nuevas obligaciones, con el fin de no ir demasiado lejos y de contar siempre con la suficiente justificación. En efecto, cuando se plantean derechos que comportan obligaciones positivas a cargo de otros, surgen automáticamente dos tendencias contrarias. En la medida en que los derechos suponen ventajas para los sujetos que los ostentan, hay un incentivo para expandir su alcance. Con las obligaciones sucede lo contrario, ya que se perjudica a quienes se les imponen, restringiendo su libertad, por lo que se recomienda la prudencia (BENTHAM, 1864, 93-95).

Desde el punto de vista de la seguridad, el derecho a la portabilidad comporta diferentes peligros. Uno de ellos ya ha sido mencionado, cual es que el acceso a la cuenta de un usuario por un tercero no autorizado permite la transferencia de todos sus datos portables. Por este motivo, se ha defendido la validez de una renuncia temporal por parte del interesado, como mecanismo que reduce las consecuencias perjudiciales de accesos indebidos a una cuenta. Otro peligro de la portabilidad es la sensación de seguridad que infunde en los usuarios, por el mayor control que les confiere sobre sus datos. Esta percepción tiene como contrapartida que las personas son más proclives a difundir información, incluyendo la de carácter sensible, preocupándose menos por adoptar una conducta prudente. Un sentimiento de mayor protección generado por vía legislativa podría, en consecuencia, reducir el grado de control efectivo y, paradójicamente, perjudicar a quienes se intenta favorecer (VAN OOIJEN y VRABEC, 2019, 99).

Otro riesgo del derecho a la portabilidad se deriva de la obligación implícita de conservar los datos en formatos interoperables (KAMARA, 2017, 11). Las empresas podrán desarrollar los formatos que estimen oportunos, pero siempre deberán estar en disposición de satisfacer las solicitudes de portabilidad sin impedimentos excesivos. Esto genera un coste de almace-

namiento al mismo tiempo que aumenta los riesgos de vulnerabilidad, los cuales, a su vez, harán que las empresas se vean obligadas a invertir en nuevos sistemas de seguridad (BAPAT, 2013, 4; RADIA y KHURANA, 2018). Los beneficios de una mayor interoperabilidad tienen como consecuencia negativa un incremento del riesgo de ataques y de fugas de datos, sobre todo cuando se trata de empresas pequeñas, con limitados recursos para alcanzar un alto nivel de seguridad (DIKER VANBERG y ÜNVER, 2017, 6).

Introducida la cuestión de los costes, se vislumbran las críticas más economicistas hacia el derecho a la portabilidad. Como se ha explicado, este derecho pretende reducir el efecto cerrojo y favorecer la competencia. Y, en principio, las empresas más pequeñas estarán especialmente interesadas en la promoción de la interoperabilidad (MULA, 2018, 404 y 406). Pero el derecho a la portabilidad —y en general, el Reglamento europeo— supone unos costes que pueden no ser desdeñables para un empresario (BEAUGRAND *et al.*, 2017, 234; CENTRE FOR INFORMATION POLICY LEADERSHIP, 2017, 2; DIKER VANBERG y ÜNVER, 2017, 4; DOWNES, 2018b)[69]. En particular, evaluar si la portabilidad afecta negativamente a derechos de terceros probablemente exija una intervención humana. Tales costes actúan como una barrera de entrada al mercado, por lo que la portabilidad produce al mismo tiempo dos efectos opuestos (GRAEF *et al.*, 2018, 1386-1387; MIRALLES LÓPEZ, 2018, 403). Así, los beneficiados podrían ser en realidad las empresas ya presentes en el mercado y, de entre ellas, las más grandes. Además, estas compañías ya disponen de un elevado nivel de información y conocimientos. Nivel que, debido entre otros al principio de limitación de la finalidad del tratamiento de datos recogido en el artículo 5.1.b) del RGPD, será más difícil de alcanzar para las empresas pequeñas que comienzan a operar (ZARSKY, 2017, 1007; RADIA y KHURANA, 2018). En definitiva, el mayor coste relativo para estas últimas puede suponer en última instancia un freno a la innovación (SWIRE y LAGOS, 2013, 352-353).

No sorprende pues que ciertas voces manifestasen que el resultado del Reglamento general de protección de datos sería el refuerzo de la posición de las grandes empresas que cuentan con los recursos necesarios para cumplir con la regulación, dando lugar a una mayor concentración del mercado (GEUTER, 2018; RADIA y KHURANA, 2018). Asimismo, el incremento de costes puede hacer que algunas empresas —incluso con grandes recursos— decidan no ofrecer sus servicios en la Unión Europea, perjudicando a los usuarios (ZARSKY, 2017, 1019). Un ejemplo citado frecuentemente es el del diario *Chicago Tribune*, cuya página web permanece inaccesible desde Europa en el momento de escribir estas líneas[70].

Otros autores han puesto en duda que el efecto cerrojo sea un problema grave. A fin de cuentas, son muchas las empresas poderosas en un momen-

to dado que se han visto relegadas a una posición secundaria gracias a la innovación, o que, incluso, han desaparecido (RADIA y KHURANA, 2018). Habiendo decaído —o caído— innumerables compañías consideradas invulnerables, parece que la mejor solución ante un efecto cerrojo es simplemente más tecnología (DOWNES, 2018a)[71]. La experiencia enseña que las tecnologías más disruptivas y que suponen un mayor progreso no provienen de las grandes empresas cuyo modelo de negocio se basa en productos de gran calidad y prestaciones aun a costa de incrementar el precio. Al contrario, la disrupción tecnológica aparece en productos económicos y de calidad aparentemente no muy elevada, que después progresan hasta un nivel tal que es difícil recordar los inicios tanto de la idea tecnológica en sí como de la empresa que la había propuesto (CHRISTENSEN *et al.*, 2001). De hecho, el sector de la tecnología parece especialmente indicado para tolerar ciertos monopolios, puesto que las empresas que adquieren tal posición tienen más dificultades para llevar a cabo innovaciones de carácter disruptivo. En suma, el dominio de una empresa en un momento determinado no refleja necesariamente un poder de mercado que le permita excluir a nuevos competidores (DIKER VANBERG y ÜNVER, 2017, 7)[72].

Es cierto que en determinados sectores a los que afecta especialmente el derecho a la portabilidad, como es el de las redes sociales, concurren ciertas circunstancias especiales. Cuanto más tiempo lleva un usuario en una red social, invirtiendo tiempo en la creación y desarrollo de su perfil, y acumulando contenidos en él, se hace difícil cambiar a otra plataforma sin un derecho a la portabilidad. Pero no es menos cierto que la heterogeneidad de las preferencias de los consumidores permite que nuevas plataformas puedan acceder al mercado, si bien su número quizás nunca llegue a ser elevado (GRAEF, 2015, 503-504). En todo caso, estas dinámicas todavía no son bien conocidas. Las redes sociales son una creación más o menos reciente, y hay ejemplos de algunas que contaban con una gran implantación y que actualmente han perdido importancia o que, directamente, ya no existen.

A todo ello hay que añadir que la existencia de un efecto cerrojo es una llamada a la innovación, ya que cualquier oportunidad de beneficio atrae recursos hacia la actividad de que se trate (POSNER, 2003, 10). Si un empresario sabe que, desarrollando un producto o servicio exitoso podrá beneficiarse de ese efecto, crecen los incentivos para alcanzarlo. El derecho a la portabilidad de los datos personales reduce la expectativa de beneficio de los modelos de negocio basados en la información. Así pues, los efectos beneficiosos de la reutilización de datos que permite la portabilidad pueden quedar ensombrecidos por la falta de incentivos para innovar (SWIRE y LAGOS, 2013, 357-360). Esto también afecta a las redes sociales: tendrán más facilidad para recibir datos de nuevos usuarios, pero menos incentivos para invertir en la gestión de la información (GRAEF, 2015, 508). Las

personas, a pesar de su creciente sensibilidad por cuestiones relativas a la intimidad y a la protección de datos, difunden voluntariamente un gran volumen de información en Internet[73]. Y lo hacen porque desean disfrutar de ciertos servicios basados en un modelo de negocio que depende de la información, prefiriendo «pagar» dando acceso a sus datos que abonando una cantidad monetaria (BEN-SHAHAR y STRAHILEVITZ, 2016, S5). De hecho, si no difundiesen esa información, los servicios que recibirían —por ejemplo, los resultados ofrecidos por los motores de búsqueda— serían de peor calidad, o incluso podrían no existir —piénsese en las redes sociales— (GRIMMELMANN, 2009, 1190; YARAGHI, 2018).

En definitiva, no está claro si el derecho a la portabilidad tiene un efecto positivo o negativo sobre la competencia. Quizás tenga un efecto procompetitivo a corto plazo, pero anticompetitivo si se observa desde un prisma dinámico y a largo plazo. Por el momento, en el sector tecnológico es difícil que desaparezca una cierta concentración. Ante ello surgen dos alternativas: una más o menos amplia regulación para que las condiciones sean aceptables, pero asumiendo el riesgo de perpetuar esa concentración y de frenar la innovación; o una menor regulación con peores resultados mientras el mercado reacciona y se adapta, pero con más posibilidades de desarrollo tecnológico, disrupción y progreso (YOO, 2012, 48-49)[74]. Todo ello invita a otro debate, referido a si las situaciones subóptimas que el derecho a la portabilidad está llamado a corregir serían mejor encauzadas a través del Derecho de la competencia[75].

Desde el punto de vista de la innovación, hay otros dos aspectos que podrían reducir el efecto positivo del derecho a la portabilidad. El primero de ellos es que los responsables del tratamiento iniciales reciben de manera continua información de primera mano, mientras que los nuevos responsables consiguen una información ajena en origen y en un momento puntual. El segundo es que, para que la portabilidad alcance todo su potencial, se requiere un cierto grado de interoperabilidad. Pero, una vez alcanzado este, las empresas podrían verse incentivadas a mantenerse en los formatos existentes, en lugar de desarrollar otros nuevos (GRAEF *et al.*, 2018, 1387-1388).

Un último elemento que no debería desconocerse es que, a pesar de que aparentemente los consumidores ganarían con una mayor interoperabilidad, en realidad hay muchos de ellos cuyas preferencias apuntan en la dirección contraria. En el mercado tecnológico existen ejemplos de marcas que no se caracterizan por permitir una gran interoperabilidad y que cuentan con una clientela fiel. La menor interoperabilidad, más allá de poder infundir en los consumidores una sensación de «sofisticación», también tiene una incidencia sobre la seguridad y la intimidad: la empresa genera una imagen comercial de gran preocupación por estas cuestiones, siendo la menor inte-

roperabilidad ofrecida una herramienta para minimizar el riesgo asumido por sus clientes (SWIRE y LAGOS, 2013, 378-379).

V. CONCLUSIONES

I. El presente trabajo ofrece un análisis del derecho a la portabilidad de los datos personales reconocido por el artículo 20 del RGPD, y al que también se hace referencia en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales. Dicho análisis revela la incertidumbre existente con relación a algunos aspectos del citado derecho, que constituye una novedad en la normativa sobre protección de datos.

II. Son susceptibles de portabilidad los datos personales «facilitados» por el interesado a un responsable del tratamiento. Sin embargo, existe la duda sobre si los datos simplemente observados por el responsable a partir de la actividad del interesado deben considerarse facilitados por este o no. A mi juicio, la interpretación más correcta del Reglamento, teniendo en cuenta su redacción, es que los datos simplemente observados no deben considerarse «facilitados». Sin embargo, el Grupo del artículo 29 se ha pronunciado en sentido contrario. Sea como fuere, mientras el Tribunal de Justicia de la Unión Europea no se pronuncie expresamente al respecto, entiendo que debe seguirse la opinión del mencionado grupo, por ser más favorable al interesado.

III. En virtud del artículo 20 del RGPD, el interesado tiene derecho a recibir del responsable del tratamiento los datos personales que le incumban, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable; así como, siempre que sea técnicamente posible, a que tales datos sean transmitidos directamente de responsable a responsable. El ejercicio del derecho a la portabilidad no conlleva el borrado de los datos personales que conserva el responsable del tratamiento transmitente.

IV. El proceso de portabilidad debe llevarse a cabo sin que el responsable del tratamiento ponga trabas que lo impidan o ralenticen. Ahora bien, puesto que debe garantizarse una transmisión segura de los datos, habrá que conseguir un equilibrio entre este objetivo y la rapidez en la transferencia. Aun cuando el Grupo del artículo 29 se haya manifestado en sentido contrario, pienso que el hecho de no poder garantizar la seguridad de la transferencia no debería equipararse a una imposibilidad técnica de transmisión directa de responsable a responsable. Desde mi punto de vista, el responsable deberá comunicar al interesado que existen problemas de seguridad, y preguntar a este último si desea que sus datos sean transferidos

al tercero pese a todo. En caso de respuesta afirmativa, no podrá negarse a ejecutar la transferencia.

V. El Reglamento general de protección de datos no ofrece ninguna definición de lo que se entiende por formato «estructurado, de uso común y lectura mecánica», por lo que habrá que recurrir a otras fuentes para delimitar estos conceptos, que, en definitiva, plasman un requisito de interoperabilidad en el formato. En particular, se plantea la duda de cómo satisfacer la exigencia del texto normativo si en el ámbito relevante no existen formatos que puedan considerarse de uso común. Quizás la entrega de los datos por parte del responsable en el formato usado efectivamente por él sea suficiente, pero también cabe la posibilidad de que deban entregarse en un formato abierto de uso común y acompañados de metadatos, con el fin de aumentar la funcionalidad de los contenidos transmitidos. En todo caso, el formato debe adecuarse al tipo de datos que se tratan, para hacer posible su reutilización por el interesado.

VI. Una de las mayores dificultades existentes en relación con el derecho a la portabilidad se deriva de uno de sus límites. El Reglamento dice que la portabilidad no puede afectar negativamente a los derechos y libertades de otros, lo que engloba tanto datos personales como derechos de propiedad intelectual. El mero hecho de que haya terceros que se vean afectados por el ejercicio del derecho a la portabilidad no es motivo suficiente para denegar la transferencia. Pero sí cuando esos terceros sufran consecuencias negativas, algo que no siempre será sencillo de determinar.

VII. Desde una perspectiva más general, se han presentado tanto los objetivos perseguidos por el derecho a la portabilidad y los beneficios que este puede reportar, como algunas de sus debilidades y peligros. Con ello no se ha querido poner en cuestión el derecho a la portabilidad en su conjunto. Simplemente, se trata de reflejar que incluso un derecho tan atractivo como este tiene algunos aspectos negativos, de mayor o menor entidad, que podrían explicar un eventual fracaso —o una mayor lentitud— a la hora de alcanzar los objetivos pretendidos por el legislador, así como generar nuevos problemas.

VIII. Desde el punto de vista de sus aspectos positivos, el derecho a la portabilidad constituye un elemento de la normativa encaminada a garantizar el derecho fundamental a la protección de datos personales. Con el derecho objeto de estudio se refuerza el control de las personas sobre sus datos, favoreciendo la autodeterminación personal. Asimismo, la portabilidad cumple objetivos de marcado carácter económico, puesto que facilitará a los usuarios cambiar de un proveedor de servicios a otro y reutilizar sus datos en el marco de otros servicios, ya sean complementarios del anterior o independientes. En definitiva, el derecho a la portabilidad está llamado a reducir el denominado «efecto retención» (*lock-in effect*), promoviendo la competencia.

IX. El derecho a la portabilidad también cuenta con algunos aspectos —al menos potencialmente— negativos, quizás menos visibles que sus ventajas, pero indudablemente presentes. Cabe plantearse en primer lugar si, al aumentar el catálogo de derechos relacionados con la protección de datos, el carácter de derecho fundamental de esta se ve difuminado, perdiendo solidez. En segundo lugar, el derecho comentado trae consigo riesgos de seguridad. Por ejemplo, con un acceso puntual no autorizado a la cuenta de usuario de una persona en una determinada plataforma, se pueden extraer de manera sencilla y rápida todos sus datos personales. Además, la sensación de mayor control sobre los datos personales que infunde la existencia del derecho a la portabilidad puede hacer que los usuarios adopten conductas menos prudentes. En tercer lugar, el derecho a la portabilidad también podría dar lugar a consecuencias poco deseables desde un punto de vista económico. Por ejemplo, la posibilidad de disfrutar eventualmente de un «efecto retención» es un incentivo para las empresas, que intentarán innovar para conseguir el beneficio resultante de él. Así, eliminar o reducir dicho efecto mediante el derecho a la portabilidad implica, necesariamente, reducir el rendimiento potencial de cualquier innovación, desincentivándola.

X. Es frecuente en los trabajos académicos mencionar la necesidad de realizar más estudios sobre el tema. Fórmula usada quizás en exceso, calificada como «martilleo estándar» en alguna ocasión (EASTERBROOK, 1996, 210-211), no resulta incierta en relación con la protección de datos en general, y con el derecho a la portabilidad en particular. Tal y como ha quedado reflejado, este derecho alberga ciertas áreas grises, su eficacia para promover la competencia e incrementar el control de los usuarios sobre sus datos no es indiscutible, y su relación con la economía de la información permite abrir otras líneas de análisis, tales como la información desde el punto de vista de los derechos de propiedad, y la incidencia del Derecho de la competencia en sectores tecnológicos en los que los datos personales juegan un papel clave.

VI. ÍNDICE DE RESOLUCIONES

- STJUE (Sala 2.ª) de 20 de diciembre de 2017, *Nowak*, C-434/16, ECLI:EU:C:2017:994.
- STJUE (Sala 2.ª) de 20 de septiembre de 2017, *Andriciuc y otros*, C-186/16, ECLI:EU:C:2017:703.
- STJUE (Sala 2.ª) de 4 de mayo de 2017, *Rīgas satiksme*, C-13/16, ECLI:EU:C:2017:336.
- STJUE (Sala 2.ª) de 19 de octubre de 2016, *Breyer*, C-582/14, ECLI:EU:C:2016:779.

- STJUE (Sala 3.ª) de 28 de julio de 2016, *Verein für Konsumenteninformation*, C-191/15, ECLI:EU:C:2016:612.
- STJUE (Sala 1.ª) de 14 de abril de 2016, *Sales Sinués y Drame Ba*, C-381/14 y C-385/14, ECLI:EU:C:2016:252.
- STJUE (Sala 6.ª) de 9 de julio de 2015, *Bucura*, C-348/14, ECLI:EU:C:2015:447.
- STJUE (Sala 3.ª) de 23 de abril de 2015, *Van Hove*, C-96/14, ECLI:EU:C:2015:262.
- STJUE (Sala 9.ª) de 26 de febrero de 2015, *Matei*, C-143/13, ECLI:EU:C:2015:127.
- STJUE (Sala 3.ª) de 17 de julio de 2014, *YS y otros*, C-141/12 y C-372/12, ECLI:EU:C:2014:2081.
- STJUE (Sala 4.ª) de 30 de abril de 2014, *Kásler y Káslerné Rábai*, C-26/13, ECLI:EU:C:2014:282.
- STJUE (Sala 3.ª) de 24 de noviembre de 2011, *ASNEF*, C-468/10 y C-469/10, ECLI:EU:C:2011:777.
- STJUE (Sala 3.ª) de 24 de noviembre de 2011, *Scarlet Extended*, C-70/10, ECLI:EU:C:2011:771.
- STJCE (Sala 4.ª) de 4 de junio de 2009, *Pannon GSM*, C-243/08, ECLI:EU:C:2009:350.
- STJCE de 6 de noviembre de 2003, *Lindqvist*, C-101/01, ECLI:EU:C:2003:596.
- Sentencia del Tribunal General (Sala 4.ª) de 11 de diciembre de 2013, *Cisco Systems y Messagenet* / *Comisión*, T-79/12, ECLI:EU:T:2013:635.

VII. BIBLIOGRAFÍA

BAPAT, A. (2013). The new right to data portability. *Privacy & Data Protection* [En línea], vol. 13, núm. 3, 3-4. Disponible en https://www.huntonak.com/images/content/3/1/v2/3122/The_new_right_to_data_portability_Bapat.pdf.

BEAUGRAND, T., *et al.* (2017). *Protection des données personnelles*. Montrouge: Éditions Législatives.

BENTHAM, J. (1864). *Theory of Legislation*. Londres: Trübner & Co. Disponible en https://ia800301.us.archive.org/2/items/legislation00bentuoft/legislation00bentuoft.pdf

BEN-SHAHAR, O., SCHNEIDER, C. E. (2011). The Failure of Mandated Disclosure. *University of Pennsylvania Law Review*, vol. 159, núm. 3, 647-749.

BEN-SHAHAR, O., STRAHILEVITZ, L. J. (2016). Contracting over Privacy: Introduction. *Journal of Legal Studies*, vol. 45, núm. S2 (Contracting over Privacy), S1-S11.

BOZDAG, E. (2018). Data Portability under GDPR: Technical Challenges. [En línea]. 28 de enero. Disponible en SSRN: https://ssrn.com/abstract=3111866.

BUSCH, C. (2018). European Model Rules for Online Intermediary Platforms. En: U. Blaurock, M. Schmidt-Kessel, K. Erler (eds.). *Plattformen: Geschäftsmodell und Verträge*. Baden-Baden: Nomos (37-57).

CENTRE FOR INFORMATION POLICY LEADERSHIP. (2017). *Comments by the Centre for Information Policy Leadership on the Article 29 Data Protection Working Party's «Guidelines on the right to data portability» adopted on 13 December 2016*. [En línea]. 15 de febrero. Disponible en https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_wp29_data_portability_guidelines_15_february_2017.pdf.

CHRISTENSEN, C., CRAIG, T., HART, S. (2001). The Great Disruption. *Foreign Affairs*, vol. 80, núm. 2, 80-95.

COMISIÓN EUROPEA. (2017). *Anexo. Marco Europeo de Interoperabilidad – Estrategia de aplicación*. Anexo de la Comunicación al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. 23 de marzo. COM(2017) 134 final.

— (2018). *Hacia un espacio común europeo de datos*. Comunicación al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. 25 de abril. COM(2018) 232 final.

— (2019). *Orientaciones sobre el Reglamento relativo a un marco para la libre circulación de datos no personales en la Unión Europea*. Comunicación al Parlamento Europeo y al Consejo. 29 de mayo. COM(2019) 250 final.

DESGENS-PASANAU, G. (2018). *La protection des données personnelles. Le RGPD et la nouvelle loi française* (3.ª ed.). París: LexisNexis.

DIKER VANBERG, A., ÜNVER, M. B. (2017). The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo? *European Journal of Law and Technology* [En línea], vol. 8, núm. 1, 1-22. Disponible en http://ejlt.org/article/view/546/727.

DOWNES, L. (2018a). How More Regulation for U.S. Tech Could Backfire. *Harvard Business Review* [En línea]. 9 de febrero. Disponible en https://hbr.org/2018/02/how-more-regulation-for-u-s-tech-could-backfire.

— (2018b). GDPR and the End of the Internet's Grand Bargain. *Harvard Business Review* [En línea]. 9 de abril. Disponible en https://hbr.org/2018/04/gdpr-and-the-end-of-the-internets-grand-bargain.

EASTERBROOK, F. H. (1996). Cyberspace and the Law of the Horse. *University of Chicago Legal Forum* [En línea], vol. 1996, 207-216. Disponible en https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1204&context=uclf.

EPSTEIN, R. A. (2018). A Frontal Assault on Social Media. *Defining Ideas* [En línea]. 4 de junio. Disponible en https://www.hoover.org/research/frontal-assault-social-media.

FINCK, M. (2018). Blockchains and Data Protection in the European Union. *European Data Protection Law Review* [En línea], vol. 4, núm. 1, 17-35. Disponible en https://edpl.lexxion.eu/data/article/12327/pdf/edpl_2018_01-007.pdf.

FOX, D. (2018). Digitale Souveränität. *Datenschutz und Datensicherheit* [En línea], vol. 42, núm. 5, 271. Disponible en https://link.springer.com/content/pdf/10.1007%2Fs11623-018-0938-9.pdf.

GAL, M. S., ELKIN-KOREN, N. (2017). Algorithmic Consumers. *Harvard Journal of Law & Technology* [En línea], vol. 30, núm. 2, 309-353. Disponible en https://jolt.law.harvard.edu/assets/articlePDFs/v30/30HarvJLTech309.pdf.

GALLEGO, C., AMARANTINIS, C. (2013). Homologación de Interoperabilidad en Cataluña: El Servicio iSalut. *I+S: Revista de la Sociedad Española de Informática y Salud* [En línea], núm. 97, 22-24. Disponible en https://seis.es/wp-content/uploads/2018/02/Revista-97.pdf.

GEUTER, J. (2018). A critical reflection on #GDPR. *Blog Tante* [En línea]. 3 de abril. Disponible en https://tante.cc/2018/04/03/a-critical-reflection-on-gdpr/.

GILBERT, F. (2012). European Data Protection 2.0: New Compliance Requirements in Sight—What the Proposed EU Data Protection Regulation Means for U.S. Companies. *Santa Clara High Technology Law Journal* [En línea], vol. 28, núm. 4, 815-863. Disponible en https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1550&context=chtlj.

GONZÁLEZ-MENESES, M. (2017). *Entender Blockchain*. Cizur Menor (Navarra): Thomson-Reuters Aranzadi.

GONZÁLEZ TAPIA, M. L. (2018). Los derechos digitales en la Ley Orgánica 3/2018. *Diario La Ley*, núm. 9324, 24 de diciembre (LA LEY 15176/2018).

GRAEF, I. (2015). Mandating portability and interoperability in online social networks: Regulatory and competition law issues in the European Union. *Telecommunications Policy*, vol. 39, núm. 6, 502-514.

GRAEF, I., HUSOVEC, M., PURTOVA, N. (2018). Data Portability and Data Control: Lessons for an Emerging Concept in EU Law. *German Law Journal* [En línea], vol. 19, núm. 6, 1359-1398. Disponible en https://ssrn.com/abstract=3071875.

GRAEF, I., VERSCHAKELEN, J., VALCKE, P. (2014). Putting the Right to Data Portability into a Competition Law Perspective [En línea]. 28 de marzo. Disponible en SSRN: https://ssrn.com/abstract=2416537.

GRATZ, J., LEMLEY, M. A. (2018). Platforms and Interoperability in *Oracle v. Google*. *Harvard Journal of Law & Technology* [En línea], vol. 31, núm. especial «Software Interface Copyright», 603-614. Disponible en https://ssrn.com/abstract=3150900.

GRÉGOIRE, S. (2018). Objets connectés et données personnelles. En: F. Chérigny, A. Zollinger (dirs). *Les objets connectés*. Poitiers: Presses universitaires juridiques de Poitiers (117-124).

GRIMMELMANN, J. (2009). Saving Facebook. *Iowa Law Review* [En línea], vol. 94, núm. 4, 1137-1206. Disponible en https://ssrn.com/abstract=1262822.

GRUPO DEL ARTÍCULO 29. (2007). *Dictamen 4/2007 sobre el concepto de datos personales*. 20 de junio (WP 136, 01248/07/ES).

— (2014a). *Dictamen 6/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE*. 9 de abril (WP 217, 844/14/ES).

— (2014b). *Dictamen 5/2014 sobre técnicas de anonimización*. 10 de abril (WP 216, 0829/14/ES).

— (2016). *Directrices sobre el derecho a la portabilidad de los datos*. Adoptadas el 13 de diciembre de 2016, revisadas por última vez y adoptadas el 5 de abril de 2017 (WP 242 rev.01, 16/ES).

— (2018). *Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679*. Adoptadas el 28 de noviembre de 2017, revisadas por última vez y adoptadas el 10 de abril de 2018 (WP259 y rev.01, 17/ES).

HARTZOG, W. (2018). The Case Against Idealising Control. *European Data Protection Law Review* [En línea], vol. 4, núm. 4, 423-432. Disponible en https://edpl.lexxion.eu/data/article/13517/pdf/edpl_2018_04-006.pdf.

HAYEK, F. A. (1945). The Use of Knowledge in Society. *American Economic Review* [En línea], vol. 35, núm. 4, 519-530. Disponible en http://bev.berkeley.edu/ipe/readings/The%20use%20of%20knowledge%20in%20society.pdf.

DE HERT, P., *et al.* (2018). The right to data portability in the GDPR: Towards user-centric interoperability of digital services. *Computer Law & Security Review* [En línea], vol. 34, núm. 2, 193-203. Disponible en https://www.sciencedirect.com/science/article/pii/S0267364917303333.

HOSEIN, G. (2018). After the Law, What's Next? The Cause of Privacy. *European Data Protection Law Review* [En línea], vol. 4, núm. 2, 147-149. Disponible en https://edpl.lexxion.eu/data/article/12793/pdf/edpl_2018_02-005.pdf.

JANAL, R. (2017). Data Portability - A Tale of Two Concepts. *JIPITEC* [En línea], vol. 8, núm. 1, 59-69. Disponible en https://www.jipitec.eu/issues/jipitec-8-1-2017/4532/JIPITEC_8_1_2017_Janal.pdf.

JÜLICHER, T., DELISLE, M. (2017). Step into «The Circle»—A Close Look at Wearables and Quantified Self. En: T. Hoeren, B. Kolany-Raiser (eds.). *Big Data in Context: Legal, Social and Technological Insights*. Cham: Springer, 81-91.

KAMARA, I. (2017). Co-regulation in EU personal data protection: The case of technical standards and the privacy by design standardisation «mandate». *European Journal of Law and Technology* [En línea], vol. 8, núm. 1, 1-24. Disponible en http://ejlt.org/article/view/545/725.

LANGHANKE, C., SCHMIDT-KESSEL, M. (2015). Consumer Data as Consideration. *Journal of European Consumer and Market Law*, vol. 4, núm. 6, 218-223.

LEFF, A. A. (1970). Contract as Thing. *American University Law Review* [En línea], vol. 19, núm. 2, 131-157. Disponible en https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=3809&context=fss_papers.

VAN LOENEN, B., KULK, S., PLOEGER, H. (2016). Data protection legislation: A very hungry caterpillar. The case of mapping data in the European Union. *Government Information Quarterly*, vol. 33, núm. 2, 338-345.

LUQUIN BERGARECHE, R. (2018). Acerca de la redefinición de la autonomía privada en la sociedad tecnológica. *Revista Boliviana de Derecho* [En línea], núm. 26, 260-293. Disponible en http://www.revista-rbd.com/articulos/2018/26/260-293.pdf.

MARTÍNEZ PÉREZ, M. (2018). La protección de datos en las redes sociales: a propósito del «Big Data». En: C. García Novoa, D. Santiago Iglesias (dirs.). *4ª Revolución Industrial: impacto de la automatización y la inteligencia artificial en la sociedad y la economía digital*. Cizur Menor (Navarra): Thomson-Reuters Aranzadi (237-259).

MEYER, D. (2017). European Commission, experts uneasy over WP29 data portability interpretation. *International Association of Privacy Professionals* [En línea].

25 de abril. Disponible en https://iapp.org/news/a/european-commission-experts-uneasy-over-wp29-data-portability-interpretation-1/.

MIRALLES LÓPEZ, R. (2018). Derecho de portabilidad (Art. 20). En: J. López Calvo (coord.). *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos*. Las Rozas: Wolters Kluwer – Bosch (401-408).

MULA, D. (2018). The Right to Data Portability and Cloud Computing Consumer Laws. En: M. Bakhoum, *et al.* (eds.). *Personal Data in Competition, Consumer Protection and Intellectual Property Law*. Berlín: Springer (397-410).

VAN OOIJEN, I., VRABEC, H. U. (2019). Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective. *Journal of Consumer Policy* [En línea], vol. 42, núm. 1, 91-107. Disponible en https://link.springer.com/content/pdf/10.1007%2Fs10603-018-9399-7.pdf.

PAZOS CASTRO, R. (2017). *El control de las cláusulas abusivas en los contratos con consumidores*. Cizur Menor (Navarra): Thomson Reuters Aranzadi.

POSNER, R. A. (2003). *Economic Analysis of Law* (6.ª ed.). Nueva York: Aspen Publishers.

POULENARD, H. (2018). Blockchain versus GDPR. En: AA.VV., *Digitalization in Law. Conference Papers* [En línea]. Vilna: Vilnius University (208-213). Disponible en http://lawphd.net/wp-content/uploads/2018/09/International-Conference-of-PhD-studentand-and-young-researchers-2018.pdf.

RADIA, R., KHURANA, R. (2018). European Union's General Data Protection Regulation and Lessons for U.S. Privacy Policy. *Competitive Enterprise Institute* [En línea]. 23 de mayo. Disponible en https://cei.org/content/european-unions-general-data-protection-regulation-and-lessons-us-privacy-policy.

RALLO, A. (2018). Privacy and Freedom. *European Data Protection Law Review* [En línea], vol. 4, núm. 2, 150-151. Disponible en https://edpl.lexxion.eu/data/article/12795/pdf/edpl_2018_02-006.pdf.

REDING, V. (2012). The European data protection framework for the twenty-first century. *International Data Privacy Law* [En línea], vol. 2, núm. 3, 119-129. Disponible en https://academic.oup.com/idpl/article/2/3/119/660556.

RESEARCH GROUP ON THE LAW OF DIGITAL SERVICES. (2016). Discussion Draft of a Directive on Online Intermediary Platforms. *Journal of European Consumer and Market Law*, vol. 5, núm. 4, 164-169.

RIZZO, M. J., WHITMAN, D. G. (2009). The Knowledge Problem of New Paternalism. *Brigham Young University Law Review* [En línea], vol. 2009, núm. 4, 905-968. Disponible en https://digitalcommons.law.byu.edu/cgi/viewcontent.cgi?article=2461&context=lawreview.

RODRIGUES, R., PAPAKONSTANTINOU, V. (eds.) (2018). *Privacy and Data Protection Seals*. La Haya: Asser Press / Springer.

RÖTTGEN, C. (2017). Like or Dislike—Web Tracking. En: T. Hoeren, B. Kolany-Raiser (eds.). *Big Data in Context: Legal, Social and Technological Insights*. Cham: Springer (73-80).

SEPD (Supervisor Europeo de Protección de Datos). (2012). *Opinion of the European Data Protection Supervisor on the "Open-Data Package" of the European Commission including a Proposal for a Directive amending Directive 2003/98/EC on re-use of public sector information (PSI), a Communication on Open Data and*

Commission Decision 2011/833/EU on the reuse of Commission documents. 18 de abril. Disponible en https://edps.europa.eu/sites/edp/files/publication/12-04-18_open_data_en.pdf.

— (2017). *Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content*. 14 de marzo. Disponible en https://edps.europa.eu/sites/edp/files/publication/17-03-14_opinion_digital_content_en_1.pdf.

VAN DER SLOOT, B. (2017). Legal Fundamentalism: Is Data Protection Really a Fundamental Right? En: R. Leenes, *et al.* (eds.). *Data Protection and Privacy: (In)visibilities and Infrastructures*. Cham: Springer (3-30).

STROIE, I. R. (2018). Algunas reglas en materia de protección de datos. *Blog CESCO* [En línea]. 28 de noviembre, disponible en http://centrodeestudiosdeconsumo.com/images/Reglas_sobre_proteccion_de_datos_-.pdf.

SWIRE, P., LAGOS, Y. (2013). Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique. *Maryland Law Review* [En línea], vol. 72, núm. 2, 335-380. Disponible en https://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=3550&context=mlr.

TERRÉ, F., SIMLER, P., LEQUETTE, Y. (2013). *Droit Civil. Les obligations* (11.ª ed.). París: Dalloz.

DE TERWANGNE, C., ROSIER, K., LOSDYCK, B. (2017). Le règlement européen relatif à la protection des données à caractère personnel: quelles nouveautés? *Journal de droit européen*, núm. 242, 302-316.

TWIGG-FLESNER, C. (2016). The Importance of Law and Harmonisation for the EU's Confident Consumer. En: D. LECZYKIEWICZ, S. WEATHERILL (eds.). *The Images of the Consumer in EU Law*. Oxford y Portland: Hart Publishing (183-202).

URQUHART, L., SAILAJA, N., MCAULEY, D. (2018). Realising the right to data portability for the domestic Internet of things. *Personal and Ubiquitous Computing* [En línea], vol. 22, núm. 2, 317-332. Disponible en https://link.springer.com/content/pdf/10.1007%2Fs00779-017-1069-2.pdf.

VALDECANTOS FLORES, M. (2017). El derecho a la portabilidad de los datos en el Reglamento General de Protección de datos. *Diario La Ley*, núm. 2, 11 de enero (LA LEY 139/2017).

VOIGT, P., VON DEM BUSSCHE, A. (2017). *The EU General Data Protection Regulation (GDPR). A Practical Guide*. Cham: Springer.

YARAGHI, N. (2018). A case against the General Data Protection Regulation. *Brookings* [En línea]. 11 de junio. Disponible en https://www.brookings.edu/blog/techtank/2018/06/11/a-case-against-the-general-data-protection-regulation/.

YOO, C. S. (2012). A Clash of Regulatory Paradigms. *Regulation* [En línea] vol. 35, núm. 3, 42-49. Disponible en https://object.cato.org/sites/cato.org/files/serials/files/regulation/2012/11/v35n3-7.pdf.

ZANFIR, G. (2012). The right to data portability in the context of the EU data protection reform. *International Data Privacy Law*, vol. 2, núm. 3, 149-162.

ZARSKY, T. Z. (2017). Incompatible: The GDPR in the Age of Big Data. *Seton Hall Law Review* [En línea], vol. 47, núm. 4, 995-1020. Disponible en https://ssrn.com/abstract=3022646.

NOTAS

[1] DO L 119, de 4 de mayo de 2016, 1.

[2] Por supuesto, la economía de la información no se compone únicamente de los datos personales. Aquellos de carácter no personal también están recibiendo una creciente atención por parte del legislador, como demuestra la aprobación del Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, relativo a un marco para la libre circulación de datos no personales en la Unión Europea (DO L 303, de 28 de noviembre de 2018, 59). Se constatan las posibilidades de aprovechar información no personal, en relación con los bienes y servicios que ilustran la innovación contemporánea (por ejemplo, el Internet de las cosas y la inteligencia artificial), gracias a la creación, recopilación, agregación, organización, tratamiento, análisis, comercialización, distribución, utilización y reutilización de datos (cfr. considerandos número 1, 2 y 9 del Reglamento 2018/1807). Sobre este Reglamento, cfr. COMISIÓN EUROPEA (2019).

[3] DO C 202, de 7 de junio de 2016, 47.

[4] DO C 202, de 7 de junio de 2016, 389.

[5] BOE núm. 294, de 6 de diciembre de 2018, 119788.

[6] DO L 281, de 23 de noviembre de 1995, 31.

[7] Cfr. considerandos números 8 y 10 de la Directiva sobre datos personales; sentencia del TJCE de 6 de noviembre de 2003, Lindqvist, C-101/01, ECLI:EU:C:2003:596, apartados 95 y 96; sentencia del TJUE de 24 de noviembre de 2011, ASNEF, C-468/10 y C-469/10, ECLI:EU:C:2011:777, apartado 29.

[8] DO C 224, de 31 de agosto de 1992, 6.

[9] Journal officiel de la République française de 7 de enero de 1978, 227.

[10] Para una presentación general de los derechos previstos en los artículos 79 a 96 de la LOPDGDD, cfr. GONZÁLEZ TAPIA (2018).

[11] El artículo 18 de la Propuesta de Reglamento de 25 de enero de 2012 (COM (2012) 11 final), que también contemplaba un derecho a la portabilidad, tenía un contenido diferente al del artículo 20 del RGPD: «Artículo 18. Derecho a la portabilidad de los datos. 1. Cuando se traten datos personales por vía electrónica en un formato estructurado y comúnmente utilizado, el interesado tendrá derecho a obtener del responsable del tratamiento una copia de los datos objeto de tratamiento en un formato electrónico estructurado y comúnmente utilizado que le permita seguir utilizándolos. 2. Cuando el interesado haya facilitado los datos personales y el tratamiento se base en el consentimiento o en un contrato, tendrá derecho a transmitir dichos datos personales y cualquier otra información que haya facilitado y que se conserve en un sistema de tratamiento automatizado a otro sistema en un formato electrónico comúnmente utilizado, sin impedimentos por parte del responsable del tratamiento de quien se retiren los datos personales. 3. La Comisión podrá especificar el formato electrónico contemplado en el apartado 1 y las normas técnicas, modalidades y procedimientos para la transmisión de datos personales de conformidad con lo dispuesto en el apartado 2. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 87, apartado 2».

[12] Para una presentación de estas directrices, cfr. VALDECANTOS FLORES (2017).

[13] https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf.

[14] DO L 136, de 22 de mayo de 2019, 1.

[15] Cfr. también considerandos número 70 y 71 de la Directiva sobre suministro de contenidos y servicios digitales.

[16] COM(2015) 634 final.

[17] Para una comparación más sintética entre ambos textos, cfr. GRAEF *et al.* (2018, 1392-1395). Para un análisis de la Propuesta de Directiva desde el punto de vista de la protección de datos, cfr. SEPD (2017).

[18] Quizás el lector advierta que la aplicación del requisito consistente en que los datos «incumban» al interesado podría plantear dificultades cuando la información incluyese datos personales de varias personas. La cuestión será abordada en el subapartado referido a los límites del derecho a la portabilidad.

[19] Cfr. considerando número 26 de la Directiva sobre datos personales.

[20] Sentencia del TJUE de 19 de octubre de 2016, Breyer, C-582/14, ECLI:EU:C:2016:779, apartados 25 y 40 a 43.

[21] STJUE Breyer, apartado 46. Cfr. también GRUPO DEL ARTÍCULO 29 (2007, 16).

[22] Sentencia del TJUE de 20 de diciembre de 2017, Nowak, C-434/16, ECLI:EU:C:2017:994, apartados 33 a 35. Cfr. también GRUPO DEL ARTÍCULO 29 (2007, 6-9).

[23] STJUE Nowak, apartados 44 y 45.

[24] Sentencia del TJUE de 24 de noviembre de 2011, Scarlet Extended, C-70/10, ECLI:EU:C:2011:771, apartado 51; STJUE Breyer, apartados 33 y 34. Cfr. considerando número 30 del Reglamento.

[25] STJUE Breyer, apartados 16 y 36 a 46.

[26] Cfr. conclusiones del Abogado General en el asunto Fashion ID, presentadas el 19 de diciembre de 2018 (C-40/17, ECLI:EU:C:2018:1039), puntos 19 y 56 a 58.

[27] En el marco de la normativa nacional española, según el artículo 72.1.p) de la LOPDGDD, constituye una infracción muy grave «la reversión deliberada de un procedimiento de anonimización a fin de permitir la reidentificación de los afectados».

[28] https://www.bbva.com/es/diferencia-dlt-blockchain/. Para una exposición sencilla sobre cómo funciona la tecnología blockchain, en relación con el Bitcoin, cfr. GONZÁLEZ-MENESES (2017, 62-103).

[29] Las observaciones sobre la relación entre la protección de datos y las tecnologías de registro distribuido se hacen tomando como referencia la exposición de FINCK (2018, 19-26).

[30] Sobre la seudonimización en general, incluyéndose en ella las funciones hash, cfr. GRUPO DEL ARTÍCULO 29 (2014b, 22-25).

[31] Nótese la diferencia con respecto a la ley española. El artículo 17 de la LOPDGDD dice que el derecho a la portabilidad se ejercerá según el artículo 20 del RGPD. Pero, entre los nuevos derechos digitales reconocidos por el legislador español, el artículo 95 de la LOPDGDD prevé un derecho de portabilidad específico, en favor de los usuarios de servicios de redes sociales y servicios de la sociedad de la información equivalentes, que no está limitado a los datos personales (cfr. art. 2.1 de la LOPDGDD). En efecto, el artículo 95 de la LOPDGDD habla de recepción y transmisión de los contenidos facilitados por el interesado al prestador del servicio.

[32] Sobre la información suministrada activamente por el usuario y la obtenida a partir del seguimiento de este, en el marco de las redes sociales, cfr. MARTÍNEZ PÉREZ (2018, 247-251). Sobre el seguimiento en línea en general, cfr. RÖTTGEN (2017).

[33] El diccionario en línea de la Real Academia Española de la Lengua (https://dle.rae.es/index.html), por ejemplo, ofrece como segunda acepción de dicho término «proporcionar o entregar».

[34] Nótese que el consentimiento debe ser como regla general inequívoco, pero en el caso de los datos sensibles se exige un consentimiento explícito.

[35] Cfr. considerandos número 32 y 42 del Reglamento.

[36] Sobre estos dispositivos, cfr. JÚLICHER y DELISLE (2017).

[37] Directiva 93/13/CEE del Consejo, de 5 de abril de 1993, sobre las cláusulas abusivas en los contratos celebrados con consumidores (DO L 95, de 21 de abril de 1993, 29).

[38] Sobre el estándar de transparencia en el marco de la Directiva sobre cláusulas abusivas, cfr. sentencias del TJUE de 30 de abril de 2014, Kásler y Káslerné Rábai, C-26/13, ECLI:EU:C:2014:282; de 26 de febrero de 2015, Matei, C-143/13, ECLI:EU:C:2015:127; de 23 de abril de 2015, Van Hove, C-96/14, ECLI:EU:C:2015:262; de 9 de julio de 2015,

Bucura, C-348/14, ECLI:EU:C:2015:447; de 28 de julio de 2016, Verein für Konsumenteninformation, C-191/15, ECLI:EU:C:2016:612; y de 20 de septiembre de 2017, Andriciuc y otros, C-186/16, ECLI:EU:C:2017:703; así como las conclusiones del Abogado General en el asunto Kiss y CIB Bank, presentadas el 15 de mayo de 2019 (C-621/17, ECLI:EU:C:2019:411).

[39] Las exigencias relativas al consentimiento pretenden asegurar que el interesado ejerce su autonomía con pleno conocimiento de causa. Difícilmente podría cuestionarse este objetivo. Ahora bien, es justo reconocer que, si se ponen demasiadas trabas, el ejercicio de dicha autonomía se ve menoscabado. Se dificulta tanto al interesado ejercer su autodeterminación personal como al empresario obtener el consentimiento de sus clientes y desarrollar su actividad comercial. Por eso, no sorprende que algunos autores hayan criticado las normas del Reglamento relativas al consentimiento y la presunción de la falta de libertad descrita, subrayando que ello puede poner en tela de juicio modelos de negocio que benefician a empresarios y consumidores por igual (DOWNES, 2018b; RADIA y KHURANA, 2018; EPSTEIN, 2018; YARAGHI, 2018). En cierta forma relacionado con esto, del Reglamento se ha llegado a decir incluso que es incompatible con el Big Data o, cuanto menos, que obliga a rearticular este de una forma subóptima e ineficiente (ZARSKY, 2017, 996 y 1002). De ahí que se haya propuesto un cambio del modelo de negocio en el marco del Internet de las cosas, para que no se base en una recopilación y acumulación masiva de datos, de modo que sea plenamente coherente y compatible con las exigencias de la normativa de protección de datos (URQUHART, 2018).

[40] Conclusiones del Abogado General en el asunto Fashion ID, punto 122.

[41] Sentencia del TJUE de 4 de mayo de 2017, Rīgas satiksme, C-13/16, ECLI:EU:C:2017:336, apartado 28.

[42] Cfr. también conclusiones del Abogado General en el asunto Fashion ID, punto 123.

[43] No obstante, de acuerdo con el considerando número 70 del Reglamento, en caso de tratamiento de datos con fines de mercadotecnia directa —incluyendo la elaboración de perfiles relacionada con dicha mercadotecnia— el interesado tiene derecho a oponerse al tratamiento en cualquier momento y sin coste alguno. Cfr. artículos 21 y 22 de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (BOE núm. 166, de 12 de julio de 2002, 25388).

[44] Las diferentes versiones lingüísticas del Reglamento no son totalmente coincidentes en este punto, puesto que, mientras que la versión en inglés dice «without hindrance», la alemana «ohne Behinderung», la italiana «senza impedimenti» y la francesa «sans que le responsable […] y fasse obstacle»; la portuguesa sigue una fórmula más parecida a la española: «sem que o responsável [...] o possa impedir». Además, de todas estas versiones, solo la alemana experimentó un cambio sustancial entre la Propuesta de Reglamento de 2012 («ohne dabei [...] behindert zu werden») y el Reglamento, pero en todo caso sin afectar al sentido de la frase como lo ha podido hacer la versión en español. Sobre la ambigüedad de la expresión «without hindrance» de la versión en inglés, cfr. SWIRE y LAGOS (2013, 344-345).

[45] La Agencia Española de Protección de Datos ofrece un formulario para el ejercicio del derecho a la portabilidad (disponible en https://www.aepd.es/media/formularios/formulario-derecho-de-portabilidad.pdf), mediante el cual el interesado solicita que se le faciliten «sus datos personales». Si se admite que el responsable puede invitar al interesado a precisar más qué datos sea portar, cabría debatir si la fórmula utilizada en el citado documento constituye una solicitud implícita de obtener «todos» los datos susceptibles de portabilidad, o si esto debería indicarse de manera expresa.

[46] Sentencia del TJUE de 17 de julio de 2014, YS y otros, C-141/12 y C-372/12, ECLI:EU:C:2014:2081, apartados 57 a 59.

[47] Se adopta la traducción de GALLEGO y AMARANTINIS (2013, 23) en relación con la norma ISO/IEC 2382-01, de la que procede la definición de la norma ISO/IEC 2382:2015.

[48] DO L 175, de 27 de junio de 2013, 1.

[49] Por ejemplo, en el ámbito de los derechos de autor con relación a interfaces de programación de aplicaciones (*Application Programming Interface,* API), cfr. GRATZ y LEMLEY (2018).

[50] En la ley española, y en el marco del derecho de portabilidad en servicios de redes sociales y servicios de la sociedad de la información equivalentes, el artículo 95 de la LOPDGDD dispone que «los prestadores podrán conservar, sin difundirla a través de Internet, copia de los contenidos cuando dicha conservación sea necesaria para el cumplimiento de una obligación legal». Interpretado a sensu contrario, si no se cumple este criterio, tales prestadores deben borrar automáticamente los contenidos tras ejecutar la portabilidad.

[51] Según el artículo 2.2.c) del RGPD, el texto no se aplica al tratamiento de datos personales «efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas».

[52] Las redes sociales constituyen un buen ejemplo de interacción personal en el que las decisiones de una persona afectan a menudo a la intimidad de terceros, pudiendo producirse discrepancias entre los usuarios con respecto al grado de «publicidad» que debería tener una determinada información. Piénsese, por ejemplo, en una foto cargada en la que uno de los usuarios es etiquetado contra su voluntad. Sobre esta cuestión, cfr. GRIMMELMANN (2009, 1171-1175).

[53] Para un análisis sobre la interrelación entre el derecho a la portabilidad y los derechos de propiedad intelectual, cfr. GRAEF *et al.* (2018, 1375-1386).

[54] Cfr. considerando número 156 del Reglamento.

[55] Sobre la transparencia, cfr. también considerandos número 42, 58 y 60.

[56] Cfr. considerando número 59 del Reglamento.

[57] Sobre la posibilidad de excluir contractualmente el derecho a la portabilidad, cfr. VOIGT y VON DEM BUSSCHE (2017, 175-176).

[58] Respecto de los acuerdos contractuales relacionados con la intimidad de las personas, la posibilidad de renunciar a ciertos derechos y los riesgos que ello genera, cfr. BEN-SHAHAR y STRAHILEVITZ (2016).

[59] Refiriéndose a esta imperfecta evaluación de los riesgos y a por qué las soluciones del mercado pueden no funcionar, cfr. GRIMMELMANN (2009, 1160-1164 y 1178-1184).

[60] Sobre el contrato como un producto, cfr. también LEFF (1970, 144-147); PAZOS CASTRO (2017, 177-182).

[61] Cfr. considerando número 100 del Reglamento.

[62] Sobre la cuestión de los sellos y certificaciones en materia de protección de datos, cfr. RODRIGUES y PAPAKONSTANTINOU (eds.) (2018). De manera más sintética, cfr. VOIGT y VON DEM BUSSCHE (2017, 71-79).

[63] Sentencia del TJCE de 4 de junio de 2009, Pannon GSM, C-243/08, ECLI:EU:C:2009:350, apartados 33 y 35; sentencia del TJUE de 14 de abril de 2016, Sales Sinués y Drame Ba, C-381/14 y C-385/14, ECLI:EU:C:2016:252, apartados 25 y 40; conclusiones del Abogado General en el asunto Dziubak, presentadas el 14 de mayo de 2019 (C-260/18, ECLI:EU:C:2019:405), puntos 83 a 86.

[64] La voluntad de reforzar el control de las personas sobre sus datos conecta con los objetivos de otras ramas del Derecho, como por ejemplo la protección de los consumidores y la defensa de la competencia, tal y como observan DIKER VANBERG y ÜNVER (2017, 5); VOIGT y VON DEM BUSSCHE (2017, 169); y GRAEF *et al.* (2018, 1388).

[65] https://www.mydataismine.com/manifest.

[66] Cfr. considerandos número 4 a 8 de la Directiva sobre suministro de contenidos y servicios digitales.

[67] Sobre los consumidores algorítmicos, incluyendo alguna referencia a la portabilidad en este ámbito, cfr. GAL y ELKIN-KOREN (2017).

[68] Repárese en que el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea, tras proclamar que las personas tienen derecho a la protección de datos personales (apdo. 1), solo menciona expresamente dos derechos concretos de la protección de datos: «a acceder a los datos recogidos que le conciernan y a obtener su rectificación» (apdo. 2).

[69] https://www.forbes.com/sites/oliversmith/2018/05/02/the-gdpr-racket-whos-making-money-from-this-9bn-business-shakedown/#1c49c3734a22.

[70] https://www.chicagotribune.com.

[71] https://www.theguardian.com/technology/2007/feb/08/business.comment; https://www.latimes.com/business/hiltzik/la-fi-hiltzik-xerox-20180213-story.html.

[72] Con relación al sector de las comunicaciones de particulares, cfr. sentencia del Tribunal General de 11 de diciembre de 2013, Cisco Systems y Messagenet / Comisión, T-79/12, ECLI:EU:T:2013:635, apartado 69.

[73] Sobre la manera en la que los usuarios interactúan en las redes sociales, sus motivaciones para difundir información en ellas, los riesgos existentes desde el punto de vista de la intimidad, posibles respuestas —regulatorias o no— ante el problema, y otras cuestiones relacionadas en el ámbito mencionado, cfr. GRIMMELMANN (2009).

[74] El autor citado se refiere a las telecomunicaciones y no a la protección de datos, pero lo cierto es que el primer sector es susceptible de comparación con determinados ámbitos de la economía digital. Por este motivo, la intervención operada en las telecomunicaciones, ya sea con el Derecho de la competencia, ya sea mediante la regulación, puede servir como referencia cuando se analiza la problemática de, por ejemplo, las redes sociales. En esta línea, cfr. GRAEF (2015).

[75] Sobre cómo el Derecho de la competencia puede actuar contra las restricciones a la portabilidad, y cómo la regulación del Reglamento general de protección de datos difiere notablemente del modo en que operarían las normas de aquella rama del ordenamiento, cfr. SWIRE y LAGOS (2013, 349-365); GRAEF, *et al.* (2014, 6-10); DIKER VANBERG y ÜNVER (2017, 6-15); y GRAEF, *et al.* (2018, 1388-1392).

(Trabajo recibido el 1-8-2019 y aceptado para su publicación el 7-11-2019)