RESOLUCIÓN CONTRACTUAL Y DESTINO DE LOS DATOS Y CONTENIDOS GENERADOS POR LOS USUARIOS DE SERVICIOS DIGITALES*

TERMINATION OF CONTRACT AND DESTINATION OF DATA AND CONTENT GENERATED BY USERS OF DIGITAL SERVICES

Sergio Cámara Lapuente
Catedrático de Derecho Civil
Universidad de La Rioja
ORCID ID: 0000-0002-1207-4432

Recibido: 13.12.2019 / Aceptado: 09.01.2020
DOI: https://doi.org/10.20318/cdt.2020.5226

Resumen: Durante el uso de los contenidos y servicios digitales puestos a disposición del consumidor por los distintos proveedores, los usuarios facilitan y crean gran cantidad de datos. El tratamiento legal del control sobre el destino de estos datos se bifurca en la actualidad en dos normas: por una parte, si se trata de datos personales, se aplicará el Reglamento (UE) General de Protección de Datos de 2016 (RGPD); por otra parte, respecto a contenidos generados por los usuarios que no sean datos personales, las reglas de la reciente Directiva (UE) 2019/770, de 20 de mayo de 2019 sobre contratos de suministro de contenidos y servicios digitales (DCSD) será de aplicación tras su transposición.

Este ensayo analiza la intersección de las normas sobre protección de datos personales con las normas sobre la defensa contractual del consumidor al tiempo de la extinción de este tipo de contratos por vía de resolución. Para ello compara los rasgos de los derechos de supresión, olvido y portabilidad del Reglamento con los nuevos derechos de impedir el uso de los datos y de recuperarlos establecidos en la Directiva y concluye críticamente acerca del escaso impacto que estos últimos pueden llegar a tener debido a su reducido ámbito de aplicación, las escasas facultades y las excesivas excepciones incorporadas finalmente en uno de los preceptos centrales de la Directiva 2019/770.

Palabras clave: contenidos digitales, servicios digitales, resolución, contrato de suministro, datos personales, portabilidad, derecho al olvido, derecho de supresión, Directiva (UE) 2019/770, Reglamento General de Protección de Datos, conformidad, contenidos generados por los usuarios, consumidor.

Abstract: During the use of digital content and services made available to the consumer by different traders and platforms, users provide and create large amounts of data. The legal treatment of control over the destination of these data currently splits into two pieces of legislation: on the one hand, in the case of personal data, the 2016 (EU) General Data Protection Regulation (GDPR) will apply; on the other hand, in the case of user-generated content other than personal data, the rules of the recent Direc-

*Este trabajo tiene su base en la ponencia expuesta en el Congreso Internacional *El Derecho privado en el nuevo* paradigma digital (Colegio Notarial de Cataluña, Barcelona, 3 y 4 de octubre de 2019) y se enmarca en el Proyecto I+D (Retos) DER2017-84748-R (Ministerio de Ciencia, Innovación y Universidades): *Mercado Único Digital Europeo y Protección de los Consumidores: perfilando los derechos de las partes en contratos de suministro de contenidos digitales*, del que es investigador principal el Prof. S. Cámara Lapuente. Una versión en inglés, reducida y con variantes, puede verse en R. Schultze, D. Staudenmayer, S. Lohsse (dirs.), *Data as Counter-Performance Contract Law 2.0?,* Nomos, Baden-Baden, 2020 (en prensa).

tive (EU) 2019/770 of 20 May 2019 on contracts for the supply of digital content and services (DCSD) will apply after transposition in Member States.

This paper analyses the intersection of the rules on personal data protection with the rules on the contractual protection of the consumer at the time of the extinction of this type of contract by means of termination. To this end, it compares the features of the rights to erasure, to be forgotten and to portability of the Regulation with the new rights to prevent further use of data and to retrieve them established in the Directive, and critically concludes that the latter may have little impact due to their reduced scope of application, the limited powers and the excessive exceptions finally incorporated in one of the central articles of Directive 2019/770.

Keywords: digital contents, digital services, termination, contract of supply, personal data, portability, right to erasure, right to be forgotten, Directive (EU) 2019/770, General Data Protection Regulation, conformity, user generated contents, consumer.

Sumario: I. Extinción del contrato y resolución contractual. II. Derechos en juego sobre los datos al resolver el contrato. 1. Comparación entre acceso/portabilidad/supresión del RGPD y recuperación/impedimento del uso de la DCSD. 2. Evolución legislativa, fundamento y crítica. 3. Datos objeto de disposición: "datos personales facilitados" vs. "cualquier contenido distinto de los datos personales, que el consumidor hubiese facilitado o creado". III. Comparación e interacción entre los nuevos derechos. 1. Derecho de supresión y derecho a impedir el uso de los datos. A) Reglas y excepciones. B) Cómo. C) Prueba. 2. Derecho de portabilidad y derecho de recuperación de datos. A) Reglas y excepciones. B) Cómo. C) Prueba. 3. Relación entre los derechos en el momento de su ejercicio. 4. La plasmación de los derechos en la práctica actual. 5. Un balance final.

I. Extinción del contrato y resolución contractual

1. La Directiva 2019/770, de 20 de mayo de 2019 sobre contratos de suministro de contenidos y servicios digitales (en adelante, DCSD o Directiva 2019/770)[1] sólo se ocupa de los derechos del usuario respecto a la disposición de sus datos, sean estos personales o de otro tipo, en caso de *resolución* del contrato. Tanto en contratos en que se pagó un precio –en dinero o en una representación digital de valor–, como en contratos en que sólo se facilitaron datos personales[2], como en contratos, en este sentido, mixtos (precio más datos personales)[3], la resolución podrá deberse a tres causas: la falta de suministro (art. 13)[4], la falta de conformidad (arts. 14-18) o la modificación de los contenidos o servicios que afecte negativamente al consumidor (art. 19.3). En los tres casos el empresario suministrador ha podido tratar los datos personales o utilizar de diversas formas los datos no personales cargados por el consumidor hasta que se produce la resolución, cuyo efecto normal en el Derecho privado es la restitución de las contraprestaciones intercambiadas por las partes contractuales.

2. Ciertamente, el ámbito objetivo de la Directiva, centrada en los remedios sólo de los tres referidos supuestos (según el art. 1: conformidad, suministro y modificación), limita los aspectos sometidos a plena armonización en la Unión Europea. Pero cuando los Estados Miembros transpongan la Directiva deberían hacerse una serie de preguntas, dado que, de acuerdo con el art. 3.10 DCSD, les corresponde la competencia para regular el Derecho contractual, incluidos los efectos de estos contratos, así como las consecuencias de la resolución[5] no reguladas en la norma europea. En concreto, los Estados miem-

[1] 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 (*DOUE* L 136, de 22.5.2019).

[2] Art. 3.1 y considerando 25.

[3] *Vid.* considerando 67.

[4] Y véase el considerando 20 en relación con la aplicación de las medidas correctoras establecidas en la Directiva 2011/83/UE de 25 de octubre de 2011, sobre los derechos de los consumidores, en lugar de las ahora establecidas en la DCSD, en caso de suministro de contenido digital en un soporte material.

[5] Parece más bien un error de traducción desde el inglés la mención que figura en la versión oficial en castellano de "terminación" (*termination*) del contrato en el art. 3.10 DCSD: "La presente Directiva no afectará a la facultad de los Estados

bros podrían expandir las reglas de la Directiva sobre el destino de los datos a supuestos de extinción contractual distintos de la resolución o crear reglas distintas para esos casos. Y ahí vienen las preguntas:

a) ¿Incide la causa de extinción en las reglas sobre la disponibilidad de los datos? Por ejemplo, si dicha causa es imputable al consumidor y no al empresario.
b) ¿Son suficientes las precisiones de la Directiva al distinguir contenidos digitales, servicios de almacenamiento en la nube y servicios de redes sociales, o son precisas otras distinciones o reglas ad hoc, como por ejemplo afinar reglas distintas cuando se produce descarga de contenidos y cuando se disfrutan en *streaming*?[6]
c) ¿La regulación nacional habría de establecer reglas sobre el destino de "otros datos" o, según la versión final de la Directiva, sobre "*cualquier contenido distinto de los datos personales*, que el consumidor hubiese facilitado o creado al utilizar los contenidos o servicios digitales suministrados por el empresario*"*, en un contexto distinto de la resolución por las tres causas citadas? En relación con la disposición sobre datos personales la armonización europea ya se ha producido mediante el Reglamento General de Protección de Datos de 2016 (RGPD)[7]: en concreto, el consumidor de contenidos y servicios digitales (el "interesado", a efectos del RGPD) tendrá los derechos de acceso, supresión y portabilidad, no sólo cuando se produzca la resolución del contrato y ni siquiera sólo cuando se extinga éste, sino también *durante* la vigencia del contrato (e incluso aunque no exista tal contrato o haya finalizado).

3. En definitiva, al implementar la Directiva, respecto a "datos no personales", los Estados miembros harán bien en valorar en qué escenarios expandir los nuevos derechos a impedir el uso de esos datos por el suministrador (art. 16.3) y el derecho a recuperarlos (16.4) y, en tal caso, decidir si lo hacen con las mismas facultades, excepciones y límites de la Directiva en los supuestos en que ésta deja fuera de su ámbito algunos contratos de suministro (*vid.* art. 3.1 y el importante considerando 25)[8] o si resulta más oportuno atender a otros modelos. De hecho, aun antes de aprobarse esta Directiva, algunos Estados miembros han comenzado a regular este ámbito de la disponibilidad de los datos no personales en el entorno de los servicios digitales tomando el ejemplo de los derechos establecidos en el RGPD (y, significativamente, el derecho de portabilidad): unos Estados lo hicieron originalmente dentro de sus leyes sobre protección de consumidores; el caso de Francia fue pionero, pues su Ley para una República digital de 2016 introdujo los nuevos derechos de "recuperación y portabilidad" de datos (personales y no personales) "en todo momento" (no sólo al extinguirse el contrato) dentro de su Código de consumo[9], aunque a final de 2018 las

miembros de regular los aspectos del Derecho contractual en general (…) incluidas las *consecuencias de la terminación de un contrato* en tanto en cuanto no estén reguladas en la presente Directiva". El originario art. 3.9 de la Propuesta de Directiva de 9.12.2015 presentada por la Comisión Europea apelaba correctamente a las consecuencias de la "resolución" y así figuró a lo largo de la tramitación normativa (en la traducción oficial al castellano de las enmiendas del Parlamento Europeo y el Consejo de la UE de 2017: *vid. infra* notas 56 y 57). La incorrecta designación –que, por lo demás, a los efectos de este ensayo poca trascendencia tiene pues es obvio que los Estados miembros no sólo tienen margen competencial para regular las consecuencias de la resolución contractual no reguladas en la Directiva, sino cualesquiera otras reglas relativas a la *extinción* de estos contratos, no incluidas en el ámbito de aplicación de esta DCSD– aparece en la versión aprobada en el Parlamento Europeo el 26.3.2019 (Resolución legislativa del Parlamento Europeo aprobando la Propuesta de Directiva, en su edición provisional, referencia P8TA-PROV(2019)0232) y pervive tras la publicación de la corrección de errores de la norma europea (*DOUE* L 305 de 26.11.2019, p. 62 y ss.).

[6] La Directiva 2019/770 incorpora algunas precisiones sobre las, hasta cierto punto, próximas categorías de "acto único de suministro", "serie de actos individuales de suministro" y "suministro continuo durante un período" (art. 11).

[7] Reglamento (EU) 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, *DOUE* L 119 de 4.5.2016, p. 1 y ss.

[8] Considerando 25, que tras delimitar a qué contratos celebrados sin precio (sino sólo obtención de ciertos datos) no se aplicará la Directiva con alguna excepción "cuando esa situación se considere un contrato con arreglo a Derecho nacional", como ocurre con la recolección de metadatos, concluye que "*no obstante, los Estados miembros deben seguir teniendo la libertad de ampliar la aplicación de la presente Directiva a tales situaciones o de regular tales situaciones*, que están excluidas del ámbito de aplicación de la presente Directiva".

[9] Art. 48 de la Ley n° 2016-1321, de 7 de octubre de 2016, *pour une République numérique*, que introdujo en el Código de Consumo los nuevos arts. L-224-42-1/4 sobre "*portabilité et récupération des données*".

nuevas normas francesas de protección de datos derogaron esas disposiciones[10]. Otros Estados miembros, como España, directamente regularon el derecho de portabilidad de datos no personales, para cualesquiera usuarios de redes sociales, al aprobar en diciembre de 2018 sus nuevas reglas sobre protección de datos personales (y sobre éstos últimos se establece una remisión al art. 20 RGPD)[11]. La transposición de la Directiva obligará a revisar la subsistencia o coherencia de esas reglas con el nuevo régimen europeo.

4. Para delimitar a qué supuestos cabría extender los nuevos derechos de recuperación de datos por el usuario y de impedir su uso por el proveedor, es preciso tomar en consideración las muy distintas *causas de extinción* de los contratos de suministro de contenidos digitales y servicios digitales, que pueden clasificarse en *naturales y patológicas*. Entre las primeras podrían comprenderse *i)* la llegada del plazo final en los contratos de duración determinada para los que no se hubiesen previsto mecanismos de renovación o prórroga; *ii)* la denuncia de los contratos de duración indefinida (el art. 16 de la Propuesta de Directiva de la Comisión de 2015 expresamente establecía la "resolución" [*sic*] y sus consecuencias para contratos de duración superior a 12 meses, aunque la regla no pasó a la DSCD); *iii)* el desistimiento unilateral del consumidor dentro del plazo y requisitos fijados en la Directiva 2011/83/EU, en las normas nacionales o en el concreto contrato (o el desistimiento por el empresario si se reservó legítimamente ese derecho); para este supuesto, la nueva Directiva de noviembre de 2019 de modernización de la Directiva 2011/83[12] (arts. 13.5, 13.6 y 13.7) ha introducido precisamente los mismos derechos que la DCSD a recuperar los datos no personales y a impedir su uso por el proveedor tras el desistimiento; *iv)* el nudo disenso de ambas partes.

Entre las causas patológicas de finalización del contrato, además de, obviamente, la resolución ejercitada por el consumidor, cabe pensar en: *i)* la resolución por el empresario ante incumplimientos cualificados del consumidor; *ii)* el desistimiento injustificado por cualquiera de las dos partes contractuales; *iii*) la nulidad o anulabilidad del contrato conforme a las reglas generales (falta de capacidad, consentimiento viciado, ilicitud del objeto principal, etc.) o los supuestos de imposibilidad sobrevenida de realizar la prestación (v. gr., fuerza mayor o caso fortuito por destrucción de los emplazamientos físicos donde se almacenan los datos, como expresamente recogen los clausulados de *Dropbox* o *WhatsApp*); el considerando 14 DCSD expresamente recuerda la libertad de los Estados miembros para regular las consecuencias de estos incumplimientos derivados de impedimentos que están fuera de control del empresario.

5. Las condiciones generales de los principales proveedores de contenidos y servicios generales clasifican con diversas denominaciones supuestos de extinción del contrato, de mera suspensión de su eficacia, cancelaciones unilaterales posibles para el empresario relacionadas con cambios en su política comercial, modelo de negocio, problemas tecnológicos o modificaciones normativas, por ejemplo. Están extendidas ciertas estipulaciones que se declaran vigentes incluso tras la extinción del contrato (*v.gr., vid. Facebook*, *Twitter* y *WhatsApp*), algunas de las cuales deberán contrastarse con la normativa sobre cláusulas abusivas[13].

6. Mención aparte merece la extinción del contrato de suministro de contenidos y servicios digitales por fallecimiento del usuario. Este caso bien podría encuadrarse como un supuesto más de extinción natural del contrato, como expresamente contemplan la mayoría de las condiciones generales de

[10] El art. L-224-42 del Código de Consumo fue derogado por la Ley n° 2018-493 de 20 de junio de 2018 sobre protección de datos personales (art. 33).

[11] *Vid.*, respectivamente, el art. 95 ("Derecho de portabilidad en servicios de redes sociales y servicios equivalentes", sobre el derecho de los usuarios a "recibir y transmitir los *contenidos* que hubieran facilitado a los prestadores de dichos servicios") y el art. 17 (portabilidad de datos personales con remisión al RGPD) de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDyGDD).

[12] Directiva UE 2019/… del Parlamento Europeo y del Consejo de 8 de noviembre de 2019, por la que se modifican la Directiva 93/13/CEE del Consejo, de 5 de abril de 1993, la Directiva 98/6/CE del Parlamento Europeo y del Consejo, la Directiva 2005/29/CE del Parlamento Europeo y del Consejo y la Directiva 2011/83/UE del Parlamento Europeo y del Consejo, en lo que atañe a la mejora de la aplicación y la modernización de las normas de protección de los consumidores de la UE (aún sin publicación en *DOUE*).

[13] *Vid.*, por ejemplo, sobre las condiciones generales que autorizan cambios unilaterales y resoluciones para estos tipos contractuales, M. B. M. Loos/J. A. Luzak, "Wanted: a bigger stick. On unfair terms in consumer contracts with online service providers", *Journal of Consumer Policy*, 39.1, 2016, pp. 63-90 (pp. 65-67).

los principales operadores del sector, si no fuera porque es posible concebir ciertos contenidos digitales como parte de la herencia del usuario fallecido, de manera que sus herederos podrían tener acceso a sus cuentas de redes sociales, servicios de correo electrónico, servicios de almacenamiento en la nube, etc., como confirmó con esta perspectiva la sentencia del BGH alemán de 12 de julio de 2018 en el asunto *Facebook*. Numerosos matices deben introducirse, distinguiendo entre contenidos ajenos a los que el usuario tuvo acceso mediante una licencia de uso que normalmente se extinguirá a la muerte, contenidos propios protegidos por propiedad intelectual que pueden, adicionalmente, constituir datos personales o no, y auténticos servicios como los antes indicados, que plantean problemas en cuanto a la sucesión por su carácter personalísimo. Más aún, como es sabido, el art. 3 RGPD (y su considerando 27) explicitan que este Reglamento no se aplica a la protección de datos de las personas fallecidas; sin embargo, los diversos Estados Miembros lo están regulando con perspectivas muy distintas acerca de quiénes puede acceder a esos datos (no sólo herederos, sino también familiares o personas vinculadas al difunto), qué facultades tienen respecto a tales datos (un acceso total con copia, un acceso limitado, un derecho a solicitar el borrado de datos y el cierre de las cuentas o su mantenimiento o incluso trasvase a otro prestador de servicios) y cuál es la regla de defecto a falta de testamento o instrucciones del fallecido (bien la sucesión en su posición jurídica o bien la extinción de ésta)[14].

7. En conclusión, a la hora de transponer la nueva Directiva 2019/770 los Estados Miembros deberían dar respuesta a numerosas cuestiones de política legislativa sobre la extinción del contrato y la disposición sobre los datos que han quedado fuera de la armonización plena realizada, respecto a otros datos no personales ("contenidos generados por los usuarios" o CGU, "*user generated contents*" o UGC, facilitados o creados durante el uso), tanto por la DCSD (supuestos distintos de la resolución por falta de suministro o conformidad o por modificación nociva), como por la Directiva de modernización de 2019 de la Directiva 2011/83 (derecho de recuperación de esos datos y abstención de uso por el empresario tras el desistimiento). Así, en concreto, es oportuno considerar estas cuestiones:

1) ¿Debería tener el consumidor los mismos derechos sobre esos datos/contenidos con independencia de la causa de extinción del contrato? En particular, dado que la DCSD confiere derechos de recuperación y abstención de uso ante incumplimientos del empresario, ¿no deberían garantizarse al consumidor similares derechos al menos en *supuestos en que ejercite legítimamente su derecho a cancelar o extinguir* el contrato en supuestos no contemplados por estas directivas?
2) ¿No debería garantizarse legalmente el mismo derecho a la recuperación (y, en su caso, a la portabilidad) de datos *estando vigente la relación contractual*, dado que es una expectativa razonable de todo consumidor, por ejemplo en servicios de *cloud computing* o de redes sociales? De hecho, cabría inferir de la propia DCSD ese derecho a partir de los requisitos objetivos de conformidad, pues según el art. 8.1.a) los contenidos o servicios digitales serán aptos para los fines a que normalmente se destinen otros del mismo tipo y a tenor del art. 8.1.b) deben poseer las cualidades y características de funcionamiento que presenten normalmente los contenidos y servicios digitales del mismo tipo y que el consumidor pueda razonablemente esperar.
3) ¿Habría de tener el empresario un *derecho de retención de los datos no personales* (ciertos contenidos generados por el propio usuario) en caso de incumplimiento o impago de éste como medida de garantía o presión para obtener lo adeudado? El RGPD no ampara ese derecho para datos personales y la DCSD tampoco lo crea para los no personales; el considerando 15 de la Directiva 2019/770 recuerda que los Estados miembros podrán regular si el con-

[14] Para una perspectiva comparada, entre la creciente bibliografía sobre el tema cabe remitir al lector a los siguientes trabajos recientes: G. Resta, "Personal Data and Digital Assets after Death: a Comparative Law Perspective on the BGH Facebook Ruling", *EuCML*, 5, 2018, pp. 201-204; M. J. Santos Morón, "La denominada 'herencia digital': ¿necesidad de regulación? Estudio del Derecho español y comparado", *CDT*, vol. 10, nº 1, 2018, pp. 413-438; S. Cámara Lapuente, "La sucesión *mortis causa* en el patrimonio digital", *Anales de la Academia Matritense del Notariado (AAMN)*, 59, 2019, pp. 375-432 (disponible en http://www.cnotarial-madrid.org/NV1024/Paginas/TOMOSACADEMIA/059-07-SERGIOCAMARA.pdf); M. E. Ginebra Molins, "Voluntades digitales en caso de muerte", *CDT*, 2020, vol. 12, nº 1.

sumidor puede suspender el pago del precio hasta que se produzca la puesta en conformidad o si el empresario puede retener reembolsos hasta que se le devuelva el soporte material. Pero ese considerando no menciona la posibilidad de retener datos el empresario, impidiendo así su supresión, recuperación o portabilidad por el usuario; esto podría establecerse en los contratos de adhesión o hacerse por la vía de hecho, de manera que el empresario tendría una posición de ventaja para presionar al usuario, renegociar o pretender el cobro de penalizaciones o de tarifas por supresión o recuperación[15]. En principio, una tal retención basada en una cláusula no negociada seguramente se considerará abusiva por falta de proporcionalidad[16] y la expectativa del consumidor, incluso en contratos gratuitos, es que el empresario debe cumplir con su obligación esencial de devolverle lo meramente depositado[17].

II. Derechos en juego sobre los datos al resolver el contrato

1. Comparación entre acceso/portabilidad/supresión del RGPD y recuperación/impedimento del uso de la DCSD

8. Las consecuencias para los datos (personales y no personales) en caso de resolución por falta de conformidad se establecen en el art. 16 DCSD, al cual se remiten el art. 13.3 (por falta de suministro) y el art. 19.3 (por modificaciones perjudiciales del contenido); el mismo régimen se replica para el desistimiento en el art. 13 de Directiva 2011/83, tras su modernización por la Directiva 2019/2161/UE, de 27 de noviembre. Dado que para los datos personales del consumidor el art. 16.2 DCSD se remite a las "obligaciones" establecidas para el empresario en el RGPD, resulta inevitable comparar los "derechos" del consumidor como parte contratante respecto a otros datos no personales que facilitó o creó durante la vigencia del contrato (DCSD), con sus derechos como "interesado" en el tratamiento de sus datos personales (RGPD). Y ello es preciso no sólo por deslinde conceptual, sino para diferenciar el alcance y excepciones de cada derecho, verificar si las disparidades están justificadas y, con ello, nuevamente, poder dar respuesta a si los legisladores nacionales deberían replicar las soluciones de la Directiva en ámbitos normalizados o si deberían o no ir más allá.

9. Los principales derechos implicados en una resolución contractual, en lo referente a los datos personales del consumidor, son, según el RGPD, el tradicional derecho de acceso (art. 15), el novedoso derecho de portabilidad (art. 20) y el parcialmente reformado derecho de supresión o "derecho al olvido" (art. 17). Una vez superada la crítica del derecho de portabilidad como una mera extensión del derecho de acceso o una suerte de versión "premium" de aquél, es evidente que la portabilidad tiene carácter propio y que existen diferencias claras entre ambos. El derecho de acceso está más relacionado con la información, la transparencia y el conocimiento que con la disponibilidad o control de los datos; "el interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen" y, en ese caso, además de acceder a esos datos, tiene derecho a recibir amplia información sobre ocho categorías distintas (fines, categorías de datos, destinatarios, plazo de conservación, origen de la información, etc.); además tiene derecho a obtener una copia de sus datos personales "en un formato electrónico de uso común" (art. 15.3). En cambio, el derecho a la portabilidad comprende tres derechos: primero, el 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"; segundo, el derecho a transmitirlos a otro responsable sin que lo impida el anterior; y

[15] R. H. Weber, "Data Protection in the Termination of Contract", en R. Schulze/D. Staudenmayer/S. Lohsse (dirs.), *Contracts for the Supply of Digital Content: Regulatory Challenges and Gaps*, Nomos, Baden-Baden, 2017, pp. 201 y 207.

[16] Esta fue la conclusión que alcanzó el "*Expert Group on Cloud Computing*", constituido por la Comisión Europea: *Synthesis* 5/6 marzo 2014 (disponible en: https://ec.europa.eu/info/business-economy-euro/doing-business-eu/contract-rules/cloud-computing/expert-group-cloud-computing-contractsen, fecha de consulta 10.12.2019).

[17] Con los debidos matices respecto a los legítimos intereses de los empresarios o los derechos de terceros, en este sentido, *vid.* F. M. Roselló Rubert, *Cloud Computing. Régimen Jurídico para Empresarios,* Aranzadi, Cizur Menor, 2018, pp. 365-369.

tercero, el "derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible".

10. Las diferencias son claras[18]: por el objeto, el derecho de acceso comprende cualesquiera datos personales y diversas informaciones adicionales, mientras que el derecho de portabilidad sólo incluye los datos facilitados por el sujeto y que le incumban. Por los fines y facultades, el derecho de acceso busca (considerando 63) permitir "conocer y verificar la licitud del tratamiento" y para eso incluye la posibilidad de obtener una copia de los datos, pero ésta no tiene por qué ser interoperable, como sí ocurre al ejercitar el derecho de portabilidad, de acuerdo con los fines de acentuar la competencia, promover el flujo libre de los datos, evitar mercados cautivos y otorgar un mayor control al interesado con la posibilidad de trasladar directa o indirectamente sus datos a otro responsable del tratamiento: el formato de la copia ha de ser estructurado y "de lectura mecánica" ("*machine-readable*", art. 20.1)[19], no sólo estar "en un formato electrónico" ("*in electronic form*", art. 15.3). Un mero "pdf" (mero texto electrónico) sin metadatos podrá satisfacer el derecho de acceso, pero no la portabilidad a otra plataforma o prestador que, en caso de existir los estándares precisos, deberá ser capaz de procesar y reutilizar los datos que estaban en poder del primer responsable (v. gr., el paso de *Facebook* a *Google+* con todo el perfil, información, *tags*, etc.; o la migración de todos los mensajes, contactos, archivos compartidos, etc. desde *WhatsApp* a *Line* o *Telegram*).

11. El rebautizado "derecho al olvido" (art. 17 RGPD) comporta el "derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan", cuando se produzcan algunas circunstancias que hagan ilegítimo el tratamiento de los datos, entre las que destacan que "los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados" o "el interesado retire el consentimiento en que se basa el tratamiento (…) y este no se base en otro fundamento jurídico". Además, si el responsable está obligado a suprimir los datos debe adoptar medidas razonables para informar a otros responsables acerca de que el interesado solicita también la supresión de cualquier enlace, copia o réplica de esos datos personales. Como advierte el considerando 68 del RGPD, el ejercicio del derecho de portabilidad no implica la supresión de los datos, pues ésta ha de pedirse expresamente, ya que, según el art. 20.3, el ejercicio del derecho de portabilidad "se entenderá sin perjuicio del artículo 17".

12. Si ahora se analizan los nuevos derechos establecidos en la Directiva respecto de contenidos (CGU) que no sean datos personales (art. 16.3 DCSD), existe una tentación de emparejar "supresión" con "derecho a impedir el uso de los datos" y "portabilidad" con "derecho a recuperar" los datos. Por una parte, en caso de resolución del contrato, el art. 16.3 DCSD establece que "el empresario *se abstendrá de utilizar*" estos contenidos del usuario, con cuatro excepciones; obligación que, por tanto, comportará el correspondiente derecho del usuario a "*impedir cualquier uso posterior*" de sus datos no personales[20], por más que el empresario tenga esa carga u obligación legal aunque el consumidor no se lo solicite. Por otra parte, según el art. 16.4, previa petición del consumidor (aquí sí es necesario el ejercicio expreso del derecho), "el empresario *pondrá a disposición* del consumidor*"* esos datos no personales; la Directiva, en este caso, explicita en positivo el "*derecho a recuperar* dichos contenidos

[18] *Vid.* P. De Hert/V. Papakonstantinou/G. Malgieri/L. Beslay/I. Sánchez, "The right to data portability in the GDPR: Towards user-centric interoperability of digital services", *Computer Law and Security Review,* 2018, p. 201; W. Li, "A Tale of Two Rights: the Clash and Collaboration of Right to Data Portability and Right to Be Forgotten", en AA.VV., *Managing Risk In the Digital Society,* UOC/Huygens, Barcelona, 2017, p. 176 (*vid.* también en *International Data Privacy Law* [2018] p. 1 y ss.); R. Stoykova, "The Right to Data Portability", *Computer Law Review International* (*CRi*), 3, 2018, p. 66.

[19] Según P. Przemysław Polański, "Some thoughts on data portability in the aftermath of the Cambridge Analytica scandal", *EuCML*, 4, 2018, p. 143, la mera mención legal del formato "de lectura mecánica" realmente implica el uso de un formato electrónico, estructurado y de uso común, aunque eso no debería hacerse equivaler con conseguir la interoperabilidad; pueden verse en ese estudio varios ejemplos de formatos electrónicos usuales que podrían cumplir ambos objetivos.

[20] Como el que tiene el empresario a impedir técnicamente el uso de los contenidos o servicios digitales por el consumidor tras la resolución según el art. 16.5 que bien podría haber estado situado en el art. 17 (obligaciones del consumidor) en vez de en el 16 (obligaciones del empresario), aunque la obligación del empresario de poner a disposición los datos también tras la resolución (considerando 70) puede justificar el emplazamiento del actual 16.5.

digitales sin cargo alguno y sin impedimentos por parte del empresario, en un plazo razonable y en un formato utilizado habitualmente y legible electrónicamente".

13. El paralelismo entre los derechos garantizados por el RGPD y la DCSD es claro, pero no son en absoluto idénticos. En este sentido, podría considerarse que *la nueva Directiva consagra unos derechos (de recuperación y de impedir el uso) amortiguados o suavizados respecto sus modelos de referencia en el RGPD*, tanto por el menor control que otorgan las facultades de la Directiva como por la amplitud de las excepciones incorporadas en la última parte de la negociación del texto europeo.

14. Así, si se compara el *derecho de supresión* (RGPD) con el *derecho a impedir el uso* (DCSD) se aprecian varias diferencias sustanciales (además de las evidentes del tipo de datos implicados y de la existencia del derecho para cualquier causa de extinción o sólo para la resolución):

a) El primero consagra una obligación de resultado (e *in faciendo*) de eliminar los datos personales (a la que equivale la anonimización total), mientras que el segundo no obliga a la supresión, sino que establece una obligación *de non faciendo*, es decir, el empresario "se abstendrá" de usar esos contenidos; puede bastar con hacerlos inaccesibles tanto a otros usuarios como a sus propios empleados[21]. Cabe sostener al menos que esta obligación negativa también es de resultado y no de medios, al haber desaparecido la formulación original de la Comisión (art. 13.2.b de la Propuesta: "el proveedor adoptará todas las medidas que podrían esperarse para abstenerse de utilizar" esos contenidos).
b) Las excepciones también tienen un alcance muy distinto: frente a las causas que justifican continuar el tratamiento de los datos personales (art. 17.3 RGPD) con base en obligaciones legales o razones de interés público y derechos fundamentales como la libertad de expresión e información, el art. 16.3 DCSD consolida una causa cercana a ésta última (que el contenido haya sido generado conjuntamente por varias personas), pero agrega tres causas nuevas que sólo persiguen salvaguardar los intereses del empresario para favorecer la minería de datos, el uso de técnicas de *big data* y, en su caso, la mejora de los servicios ofrecidos. El legislador no ha querido imponer cargas que podrían llegar a ser gravosas para los servicios de redes sociales y de almacenamiento en la nube, aunque en algunos casos imponer una obligación total de supresión hubiera sido muy sencilla de cumplir. La crítica acerca de la introducción estas tres excepciones (letras a, b y c del art. 16.3) es aún más justificada en relación con el derecho a recuperar los contenidos consagrado en el art. 16.4 (*vid. infra* III.1.A y III.2.A).
c) Aunque aparentemente para que se produzca la supresión de los datos personales el interesado ha de ejercitar su derecho, los principios vigentes del RGPD llevan al mismo resultado sin necesidad de solicitar la supresión si los datos ya no son necesarios para la finalidad negocial para la que fueron recogidos, en virtud de los principios de limitación del plazo de conservación y minimización (art. 5.1), pues su tratamiento ya no sería necesario para la ejecución del contrato (art. 6.1.b). Por su parte, la DCSD consagra la abstención de uso directamente como un deber del empresario, pero debe defenderse que existe un correlativo derecho del consumidor a exigir que se cumpla la obligación. En este punto, pese a las diferencias de formulación, la configuración legal está muy próxima.

15. Las diferencias entre *el derecho de portabilidad (RGPD) y el de recuperación (DCSD)* son más evidentes[22] (además, nuevamente, de los datos afectados y las situaciones que justifican el surgimiento de cada derecho):

[21] La obligación se cumpliría, *ad extra*, inhabilitando el acceso a ese contenido por otros usuarios (cesar en su comunicación pública o puesta a disposición, en caso de obras originales) y, *ad intra*, no valiéndose de ese contenido para sus fines empresariales (excluirlo tanto de análisis personalizado como de técnicas de *big data*, eludir el tratamiento de los metadatos asociados, no ceder su uso a otros empresarios, etc.).

[22] Para ulteriores comparaciones sobre la base de versiones previas a la aprobación de la Directiva 2019/770, véase R. Janal, "Data Portability. A Tale of Two Concepts", *JIPITEC*, 2017, p. 59 y ss.; A. Metzger/Z. Efroni/L. Mischau/J. Metzger, "Data-Related Aspects of the Digital Content Directive", *JIPITEC*, 2018, pp. 102-105.

a) El RGPD permite solicitar la transmisión "directa" de los datos personales de un responsable a otro nuevo responsable del tratamiento, si es técnicamente posible (art. 20.2), regla que no se prevé en la DCSD.
b) El RGPD permite solicitar la portabilidad de los datos de cualquier responsable que los haya tratado y no sólo de la contraparte contractual del usuario, que es escenario contractual contemplado en la DCSD.
c) La única excepción contemplada en el RGPD es que la portabilidad no debe afectar negativamente a los derechos y libertades de otros (20.4) y, cuando se ejercite conjuntamente con el derecho de supresión, no afectará al tratamiento necesario para misiones en interés público o en el ejercicio de poderes públicos (art. 20.3); en cambio, la DCSD –que bien podría haber contemplado también la cláusula de salvaguarda de derechos y libertades de terceros, pero no lo ha hecho– sólo establece tres excepciones que merman sin real justificación el control del consumidor sobre datos generados por él (que no tengan utilidad fuera de los servicios del empresario, estén relacionados exclusivamente con la actividad durante el uso o hayan sido agregados con otros datos).
d) La forma de recuperar o recibir los datos, la ausencia de coste y el plazo son similares en el RGPD y en la DCSD, en un calculado paralelismo legal. Sin embargo, aunque el formato electrónico en ambos casos es de lectura mecánica o automática[23], lo que favorecerá la interoperabilidad y el trasvase de contenidos a otra plataforma o proveedor (no es un mero formato electrónico como en el derecho de acceso), falta el rasgo de que el formato sea "estructurado". Esa ausencia no debería interpretarse como un obstáculo a que los contenidos recuperados puedan trasladarse tal cual a otro empresario.
d) ¿Tiene el consumidor un derecho a portabilidad "indirecta", es decir, a realizarla él mismo enviando a otro empresario los contenidos recuperados? Con el silencio de la DCSD se propicia dejar la decisión a los empresarios por medio de sus condiciones generales contractuales, en lugar de, como hubiera sido deseable, intervenir legislativamente para propiciar también la plena portabilidad de los CGU y los datos no personales, con miras a fomentar una auténtica competencia en el mercado único digital. En efecto, el art. 16.4 DCSD no dice, como en cambio hace el art. 20.1 RGPD, que el consumidor tendrá el *derecho "a transmitirlos a otro responsable* del tratamiento *sin que lo impida* el responsable al que se los hubiera facilitado"; se detiene en el derecho a recuperar los contenidos. El Parlamento europeo aprobó una enmienda (nº 47) en 2017 para expresamente incluir este derecho, pero el texto de la Directiva finalmente aprobado no lo contiene.

Ciertamente, la mayoría de los prestadores de servicios digitales suelen resaltar en sus estipulaciones el carácter no exclusivo de la licencia que el usuario otorga al empresario para la difusión de los contenidos que éste carga, crea o comparte con otros usuarios, por lo que el cambio de empresario (de forma coetánea o posterior a la primera relación contractual) queda garantizado. Las mismas condiciones generales suelen resaltar también el carácter "perpetuo" o "indefinido" de esa licencia, que, en cambio, sí entrará en conflicto con el derecho de abstención de uso por el empresario una vez que las reglas de la directiva queden transpuestas. Por poner algunos ejemplos, es el caso de *Apple Stores*, *Google*, *Spotify*, *Twitter* o *WhatsApp*[24]. Por su parte, *Youtube* explicita que la licencia concedida por el consumidor sobre

[23] En ambos preceptos en inglés se impone que sea "*machine-readable*"; la traducción al castellano difiere: de "lectura mecánica" (art. 20.1 RGPD) a "legible electrónicamente" (art. 16.4 DCSD). Este rasgo no estaba en la propuesta original de la Comisión Europea de 2015 (PDCD), sino que fue introducido en las versiones de 2017 aprobadas tanto por el Parlamento Europeo como por el Consejo.

[24] Por poner un solo ejemplo, las condiciones generales de *Spotify* vigentes desde el 12.2.2019 (disponibles en https://www.spotify.com/es/legal/end-user-agreement/#s7), imponen en su § 8 que: "*Usted le otorga a Spotify una licencia no exclusiva, transferible, sublicenciable, gratuita, indefinida* (o en aquellas jurisdicciones que no lo permiten, durante un período equivalente a la duración que estos Contratos más veinte (20) años), *irrevocable, totalmente pagada y mundial para utilizar, reproducir, poner a disposición del público* (p. ej., interpretar o mostrar), publicar, traducir, modificar, crear obras derivadas y distribuir *cualquier Contenido del Usuario relacionado con el Servicio* a través de cualquier medio, ya sea solo o combinado con otro Contenido o material, de cualquier modo y por cualquier medio, método o tecnología, que existan actualmente o que se creen

los contenidos generados por él se cancela al borrar los vídeos. Pero existen otros empresarios que declaran que esa licencia de uso es exclusiva (mientras dure la relación y, en algunos casos, proclaman con dudosa legalidad, que también después) o que el consumidor no podrá borrar determinados contenidos pese extinguir la relación (como comentarios en blogs o en mercados *online*).

Por lo tanto, para ponderar el equilibrio de lo estipulado (sin negociación) en el contrato habrá de contrastarse la cláusula con el parámetro objetivo de la legítima expectativa del usuario medio: en efecto, en servicios de *cloud computing* la expectativa razonable de todo usuario es poder recuperar los contenidos depositados en el servidor y poder transferirlos a donde estime oportuno; no establecerlo así, por ejemplo, sería una clara falta de conformidad por no presentar una funcionalidad que se espera en servicios de ese tipo (art. 8.1.b DCSD). En los servicios de redes sociales, no garantizar esta portabilidad propia o indirecta sin duda contribuye a crear mercados cautivos, en contra de las finalidades propuestas en la Estrategia del Mercado Único Digital. En este sentido, si no se combate desde las normas de protección de consumidores, podría merecer sanción desde el Derecho europeo de la competencia[25]; la Comisión Europea se planteó precisamente la cuestión desde esta óptica en su resolución sobre la adquisición de *WhatsApp* por *Facebook:* los posibles problemas de portabilidad se analizaron expresamente, como efectos de red que podrían ser nocivos para la competencia (dificultad de los usuarios de reconstruir su red de contactos en caso de cambio de proveedor)[26].

16. Tras poner de manifiesto las diferencias entre los derechos concedidos por el RGPD y la DCSD, conviene indagar en algunas claves del proceso de gestación de la Directiva que pueden explicar el fundamento de las decisiones legislativas adoptadas.

2. Evolución legislativa, fundamento y crítica

17. La Propuesta de Reglamento sobre compraventa europea (CESL de 2011) fue el primer intento en la UE de incluir en el ámbito de protección contractual del consumidor a los contratos sobre contenidos digitales en los que no se pagase en dinero, sino que la contraprestación fuese la cesión del uso de datos del consumidor[27]. Sin embargo, el CESL optaba por diferenciar en el régimen de remedios por incumplimiento la forma de pago, para rebajar o excluir algunos remedios si la contraprestación eran sólo datos. La casi coetánea Directiva 2011/83, de 25 de octubre, sobre derechos de los consumidores, definió de forma omnicomprensiva los "contenidos digitales" y omitió referencias a si su ámbito de aplicación incluía también los contratos gratuitos (entendiendo también por estos los que comportaban cesión de datos personales); la interpretación más correcta así lo entendía[28] y ahora lo confirma la "Directiva de modernización" de aquélla, de noviembre de 2019[29].

---

en un futuro. Además de los derechos específicamente otorgados por el presente, usted conserva la titularidad de todos los derechos, incluyendo los derechos de propiedad industrial e intelectual, del Contenido del Usuario. Si procede y la legislación aplicable lo permitiese, usted también acepta renunciar y no hacer valer cualquier "derecho moral" o derechos equivalentes, como su derecho a que lo identifiquen como el autor del Contenido del Usuario, que incluye Comentarios, y su derecho a objetar al trato despectivo de dicho Contenido del Usuario".

[25] I. Graef, "Mandating Portability and Interoperability in Online Social Networks: Regulatory and Competition Law Issues in the European Union", *Telecommunications Policy*, 39-6, 2015, pp. 502-514. Y, con algunas propuestas concretas, I. Graef/D. Clifford/P. Valcke, "Fairness and enforcement: bridging competition, data protection, and consumer law", *International Data Privacy Law*, 8-3, 2018, p. 200.

[26] Comisión Europea, Caso nº COMP/M.7217 – *Facebook/WhatsApp*, 3 Octubre 2014, vid. § 113 y 127-142 (disponible en http://ec.europa.eu/competition/mergers/cases/decisions/m7217201410032031039621 32EN.pdf). *Vid.* J. Vilarino Marzo, *La privacidad en el entorno del cloud computing*, Reus, Madrid, 2018, pp. 117-118.

[27] Cfr. art. 5.b. de la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a una normativa común de compraventa europea, COM(2011)635 final, de 11 de octubre de 2011 (CESL, en sus siglas inglesas).

[28] *Vid.* S. Cámara Lapuente, "La nueva protección del consumidor de contenidos digitales tras la Ley 3/2014, de 27 de marzo", *Revista CESCO de Derecho de Consumo*, 11, 2014, pp. 69-167 (pp. 102-105).

[29] Considerandos 31 a 35 de la Directiva de 8.11.2019 sobre modernización de la Directiva 2011/83 (y otras directivas) y los cambios en consecuencia operados en ésta sobre su ámbito de aplicación y definiciones.

18. La Propuesta de Directiva sobre contratos de suministro de contenidos digitales presentada por la Comisión Europea el 9 de diciembre de 2015 (PDCD) seguía conteniendo una definición única para todo tipo de contenidos digitales, e incluía la conocida, criticada y finalmente eliminada frase de que el empresario suministra los contenidos "*y, a cambio, se paga un precio o el consumidor facilita activamente otra contraprestación no dineraria en forma de datos personales u otro tipo de datos*" (art. 3.1). En ese momento del proceso legislativo, la "contraprestación" comprendía cualquier tipo de datos (personales y no personales) y los derechos del consumidor al resolver el contrato eran los mismos (recuperar e impedir el uso) respecto a cualesquiera datos.

19. Este enfoque sufrió cambios debido, fundamentalmente, a dos puntos de inflexión: por una parte, con posterioridad a la propuesta de la Comisión, el 27 de abril de 2016, se aprobó el RGPD con sus derechos de supresión y portabilidad; es bien conocida la tortuosa tramitación del derecho de portabilidad, introducido en la propuesta de la Comisión Europea en enero de 2012, eliminado en el Parlamento Europeo en 2014 y vuelto a introducir en la versión aprobada por el Consejo en 2015, para acabar en el texto definitivamente aprobado en 2016 con cambios respecto a la propuesta original. Con este contexto se puede entender la resistencia a duplicar tal cual la portabilidad en la nueva Propuesta de Directiva. Por otra parte, el informe del Supervisor Europeo de Protección de Datos (SEPD) de 14 de marzo de 2017 sobre la Propuesta de Directiva sobre contenidos digitales rechazó "cualquier nueva disposición que introduzca la idea de que los ciudadanos pueden pagar con sus datos del mismo modo que con su dinero"[30]; tal fue el impacto de la idea de desterrar la idea de contraprestación en datos personales, que incluso el actual considerando 24 de la DCSD aprobada, recoge como propia una de las frases de aquel informe: "*la protección de datos personales es un derecho fundamental, por lo que los datos personales no pueden considerarse una mercancía*".

20. A partir de ese momento, las versiones de la Directiva aprobadas en 2017, respectivamente, por el Parlamento y el Consejo, adoptaron dos cambios sustanciales: en primer lugar, separaron los derechos que correspondían al consumidor en caso de resolución, rigiéndose los relativos a datos personales por el RGPD y los relativos a "otros datos" no personales por la Directiva. En segundo lugar, diferenciaron entre "contenidos digitales" y dos tipos de "servicios digitales". También adoptaron otras distinciones pertinentes, como la relativa al suministro en un acto, en varios actos o el suministro continuo.

21. La pregunta, en definitiva, es esta: ¿está justificado que en caso de resolución contractual el consumidor tenga derechos tan distintos respecto de sus datos personales y de otros datos no personales, como los contenidos por él facilitados o creados al usar los contenidos y servicio digitales del suministrador? Es evidente que el aspecto de identidad de la persona que comportan los datos personales justifica una protección reforzada, frente a los aspectos de propiedad (intelectual) de sus creaciones y de propiedad de meros datos (si puede hablarse en esos términos)[31]. Se trata de la dicotomía entre derechos inherentes a la persona y derechos de propiedad sobre bienes, con estándares de protección distintos en la tradición europea. Sin embargo, en el caso de la portabilidad de datos personales uno de sus objetivos larvados es, junto con potenciar el control del usuario sobre sus datos (considerando 68 RGPD), evitar efectos de mercados cautivos y promover la competitividad, mediante el cambio de proveedores de servicios[32]; y ese mismo objetivo se puede (y debe) perseguir también, una vez declarado deseable (durante

[30] European Data Protection Supervisor (EDPS), "Opinion 4/2017 on on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content", 14 marzo 2017, pp. 3 y 10.

[31] Sobre este controvertido enfoque, llamado a erigirse en el centro de discusión sobre el diseño normativo del mercado digital, *vid.*, por ejemplo, H. Zech, "Information as Property", *JIPITEC*, 5, 2015, pp. 192-197; E. Tjong Tjin Tai, "Data ownership and consumer protection", *EuCML*, 4, 2018, pp. 136-140; entre nosotros, J. A. Castillo Parrilla, "Economía digital y datos entendidos como bienes", en P. Castaños Castro/J. A. Castillo Parrilla (Dirs.), *El mercado digital en la Unión Europea*, Reus, Madrid, 2019, pp. 293-305.

[32] Como afirmó la Comisión Europea: "with increasing use of certain online service, the amount of personal data collected in this service becomes an obstacle for changing services, even if better, cheaper or more privacy friendly services become available. This could mean the loss of contact information, calendar story, interpersonal communication exchanges and other kinds of personally or socially relevant data which is very difficult to recreate or restore": European Commission, "Commis-

toda la tramitación) en relación con exactamente los mismos contratos de suministro de contenidos digitales[33], con el fomento de la portabilidad (y no sólo la recuperación) de los contenidos facilitados o creados por los usuarios que no sean datos personales. Las excepciones creadas a la recuperación de este tipo de datos y la ausencia de mención de que no han de ponerse obstáculos al consumidor que desee migrar sus contenidos a otras plataformas ponen en riesgo el objetivo de un mercado digital competitivo. El consumidor no tendrá incentivos para cambiar de plataforma con un perfil y unos contenidos que ha podido generar durante años y que la tecnología permite hoy trasvasar fácilmente. Se podrá alegar que existen en la actualidad numerosos metadatos y otros datos no personales que carecen de un estándar internacional que permita su interoperabilidad, pero ese argumento carece de peso para otros que sí lo tienen (geolocalización, historial de navegación, etc.). Y debe recordarse además que tampoco para la portabilidad directa se llegó tan lejos en el RGPD como para imponer su obligación a los responsables del tratamiento, pues sólo se tendrá el derecho "cuando sea técnicamente posible"; más incluso, en general, la interoperabilidad no llega a ser obligatoria sino sólo "sugerida": según el considerando 68 RGPD, "debe *alentarse* a los responsables a crear formatos interoperables que permitan la portabilidad de datos"; lo único obligatorio son los tres requisitos del formato (art. 20.1 RGPD)[34]. Además, desapareció del RGPD la propuesta inicial de la Comisión Europea de que ésta actuase como institución que impusiese ciertos formatos y fomentase estándares interoperables (art. 18.3). En cambio, de forma oportuna, ese papel de la Comisión reaparece de alguna manera, atenuada, en el considerando 50 DCSD respecto al desarrollo de normas internacionales y códigos de conducta sobre el formato para recuperar el contenido que no sean datos personales[35].

22. Por último, existen diversas voces que subrayan que la forma en que la portabilidad ha quedado configurada en el RGPD supone un paso importante hacia la creación de un auténtico derecho absoluto *erga omnes* sobre los datos portables y no sólo un derecho personal frente al responsable[36], concepción esta que confirmaría la necesidad de una mayor igualdad en cuanto a los derechos de disponer sobre contenidos digitales no personales.

3. Datos objeto de disposición: "datos personales facilitados" *vs.* "cualquier contenido distinto de los datos personales, que el consumidor hubiese facilitado o creado"

23. La versión inicial de la Directiva presentada por la Comisión (PDCD) distinguía entre "datos personales" y "otros datos no personales". La sugerencia del Supervisor Europeo de Protección de Datos de eliminar esa distinción y reconducirlo todo al concepto amplio de datos personales del art. 4.1 RGPD y a los derechos recogidos en el Reglamento, por fortuna sólo fue parcialmente atendida, pues hubieran desaparecido por completo los derechos de recuperación e impedimento del uso respecto a "datos no personales". En lugar de esta denominación se optó por referirse a "cualquier contenido distinto de los datos personales, que el consumidor hubiese facilitado o creado al utilizar los contenidos o servicios

sion Staff Working Paper. Impact Assessment Accompanying the Document on the General Data Protection Regulation", SEC (2012)72 final, p. 28.

[33] *Vid.* el considerando 46 de la Propuesta de Directiva de la Comisión (PDCD-2015). Finalmente, el considerando 70 de la Directiva 2019/770 sólo se refiere a salvaguardar el derecho de resolución del consumidor. Las referencias al objetivo de potenciar la competencia y el cambio de proveedores han sido eliminadas (*vid. infra* notas 64-68). La eventual capacidad del derecho de portabilidad de datos personales como factor para generar un mercado más competitivo fueron también resaltadas por el Grupo de Trabajo del Art. 29: Grupo de Trabajo sobre protección de datos del Art. 29 (GT29), "Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE", aprobado el 9 de abril de 2014 (844/14/ES WP 217) p. 56.

[34] De Hert *et al.*, "The right to data portability…", cit., pp. 197 y 200; Stoykova, "The Right to Data Portability", cit., p. 68.

[35] Considerando 50 DCSD: "*los empresarios deben hacer uso de normas, especificaciones técnicas abiertas, buenas prácticas y códigos de conducta, incluso en relación con el formato* comúnmente utilizado y de lectura mecánica *para recuperar el contenido* que no sean los datos personales (…). En este contexto, *la Comisión podría abogar por el desarrollo de normas* internacionales y de la Unión y la elaboración de un código de conducta por las asociaciones de empresarios y otras organizaciones representativas que podrían apoyar la aplicación uniforme de la presente Directiva.

[36] Stoykova, "The Right to Data Portability", cit., p. 66.

digitales suministrados por el empresario" (art. 16) que cubre en teoría las mismas situaciones que los "datos no personales en general"; sin embargo, las excepciones introducidas en la tramitación de la Directiva dejan muy mermado el alcance de los contenidos cubiertos, como ahora se verá.

24. El concepto de "datos personales" del art. 4.1 RGPD es bien conocido, se refiere a cualquier información que pueda vincularse a un individuo concreto[37] y el Grupo de Trabajo del artículo 29" (GT29) y su organismo sucesor han interpretado profusamente el precepto y aclarado con ejemplos distintos supuestos dudosos. Así, en particular, determinados "metadatos" (datos que dan información sobre otros datos)[38], si no son plenamente anónimos también serían datos personales. Sin embargo, la política de privacidad de algunas empresas catalogan expresamente en su clausulados como datos no personales algunos datos que difícilmente escaparían a la definición del RGPD[39].

25. Si ahora tratamos de imaginar en general cuáles podrían ser esos "otros datos no personales" involucrados en un contrato de suministro de contenidos o servicios digitales, al menos tres categorías de datos parecen importantes: a) Los datos que no permiten identificar a una persona ni pueden ser conectados con una persona identificada o identificable[40], en definitiva, cuando se trata de datos "*anonimizados*" (*vid.* sobre la "seudonimización" los arts. 4.5 y 11.2 y el considerando 26 RGPD) o de datos "*agregados*[41] con otros datos por el comerciante y no puedan desagregarse"[42], siempre que no permitan identificar a la persona. Los datos no personales que constituyen *contenidos digitales adquiridos* por el usuario desde el proveedor: piénsese en vídeos, películas, canciones *descargadas o transferidas a un servidor* desde el que el usuario los podría descargar o visualizar en cualquier momento. C) Los *contenidos generados por el usuario* que no constituyan datos personales.

En relación con los datos anonimizados, es bien conocida la preocupación de que vuelvan a ser datos personales mediante técnicas de ingeniería inversa y minería de datos, de manera que incluso respecto a la supresión y portabilidad del RGPD a los que remite la Directiva, esa posibilidad debe con-

[37] Art. 4.1 RGPD: "toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, 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".

[38] Se trata de etiquetas o datos anexados a archivos de todo tipo que contienen palabras clave, información sobre autoría, modificaciones, etc., generados automáticamente o de creación humana que sirven sobre todo para la catalogación de los archivos (imágenes, vídeos, páginas, documentos, etc.) en índices y su recuperación en la web semántica. Téngase en cuenta que la Directiva 2019/770 adopta, sin embargo, un enfoque más permisivo respecto a la recolección de metadatos de cara a interpretar si una relación contractual en que sólo se recogiesen éstos y ningún otro tipo de dato personal podría caer en su ámbito de aplicación; según el considerando 25 DCSD, "*la presente Directiva tampoco debe aplicarse a situaciones en las que el empresario recaba únicamente metadatos tales como información sobre el dispositivo del consumidor o el historial de navegación*, excepto cuando esta situación se considere un contrato con arreglo al Derecho nacional".

[39] Veamos este ejemplo de *Apple* ("Política de privacidad", actualizada a 29.8.2019, disponible en https://www.apple.com/es/legal/privacy/es/): "También recopilamos datos de manera que no es posible asociarlos, por sí solos, directamente a una persona determinada (…). Estos son algunos ejemplos de las categorías de datos de carácter no personal que podemos recopilar y los posibles usos que podemos darles: Es posible que recopilemos datos tales como profesión, idioma, código postal, prefijo telefónico, identificador único de dispositivo, dirección URL de referencia, ubicación y zona horaria en la que se utiliza un producto Apple, para conocer mejor la conducta de los clientes y mejorar los productos, servicios y anuncios publicitarios. (…) Es posible que recopilemos información acerca de las actividades de los clientes en el sitio web (…) así como en nuestros demás productos y servicios (…). *Los datos agregados se consideran información no personal a efectos de esta Política de Privacidad* (…); si se combinan datos de carácter no personal con datos de carácter personal, los datos combinados serán tratados como datos de carácter personal en tanto que sigan estando combinados".

[40] Así, el Grupo de Trabajo del art. 29 (GT29), "Dictamen 4/2007 sobre el concepto de datos personales", aprobado el 20 junio 2007, pp. 26-27, señala que las Directivas de protección de datos (ni el RGPD) no se aplicarán "cuando no puede afirmarse que los datos se refieren a una persona física, o cuando no cabe hablar de persona identificada o identificable".

[41] Un ejemplo de este tipo de datos, que el apartado 3.5 de la Política de Privacidad de *Twitter* (https://twitter.com/privacy) titula como "información no personal" es el siguiente: "Compartimos o revelamos datos no personales, como es la información agregada que incluye el número total de veces que las personas interactuaron con un tuit, *el número de personas que hicieron clic en un enlace en particular o que votaron en una encuesta en un tuit (incluso si solamente una persona lo hizo)*, los temas sobre los que las personas están tuiteando en una ubicación en particular o informes para los anunciantes acerca de cuántos usuarios vieron o hicieron clic en sus anuncios".

[42] Cfr. art. 16.3.c) DCSD.

templarse[43]. Lo mismo ocurre con los datos combinados y agregados con otros del proveedor de manera que pierdan su carácter personal, pero puedan recobrar ese carácter[44]. El SEPD ha clarificado en varias ocasiones que los metadatos y los datos anónimos están cubiertos por el RGPD[45] (*vid.* art. 11.2).

26. Para cualificar qué contenidos concretos han quedado finalmente cubiertos en las facultades anejas a la resolución en el art. 16 DCSD ha de partirse de estas premisas conceptuales: en primer lugar, hay que distinguir entre aquellos *datos necesarios para entablar la relación contractual* (como puede ser los relativos a la identidad del usuario, su dirección de correo electrónico, país de residencia e idioma, número de tarjeta de crédito, etc.) *y los datos precisos para ejecutar el contrato* de conformidad con lo ofertado (v. gr., en el ejemplo de una aplicación de entrenamiento físico: la evolución del peso durante el uso de la aplicación, la información sobre los alimentos ingeridos cada día, el seguimiento de las distancias recorridas, etc.). Así como el segundo grupo de datos personales deberán desaparecer de la esfera de control del empresario una vez extinguida la relación –con la simple aplicación del principio de limitación del plazo de conservación del art. 5.1.e RGPD–, en ocasiones los primeros podrían ser retenidos durante un tiempo por él con fines legítimos como exigir responsabilidades (injurias en una red social, usos fraudulentos del servicio, cobro de impagos, etc.).

En principio, el consentimiento para tratar ambos tipos de datos personales es el mismo y siempre que el tratamiento sea "necesario"[46] durará tanto cuanto dure la relación contractual (cfr. art. 7.3 RGPD sobre la revocación del consentimiento)[47]. Según el art. 3.1 DCSD, la Directiva no se aplicará "cuando los datos personales facilitados por el consumidor sean tratados exclusivamente por el empresario con el fin de suministrar los contenidos o servicios digitales con arreglo a la presente Directiva o para permitir que el empresario cumpla los requisitos legales a los que está sujeto, y el empresario no trate esos datos para ningún otro fin". Por lo tanto, *primera categoría de datos (personales y no personales) excluida del ámbito de aplicación de la Directiva: los datos necesarios para celebrar el contrato y para ejecutarlo, si no se procesan para otros usos* –que la práctica enseña que excluirá pocos contratos, pues sí se emplean para otros usos, principalmente comerciales, se informe o no de ellos–.

27. En segundo lugar, puede distinguirse entre "*datos primarios*" y "*datos secundarios*", entendiendo por estos últimos los observados por el responsable del tratamiento, con los que crea perfiles y patrones de comportamiento e intereses, generando así datos-conocimiento y no meros datos-materia prima. Diversos estudios de las ciencias sociales demuestran que permitir a los consumidores recuperar el flujo ulterior de sus datos ayudaría a los consumidores a comprender el alcance de su consentimiento[48].

28. En tercer lugar, profundizando en esta distinción, aún puede diferenciarse entre *"datos facilitados", datos "generados o creados" por el usuario, "datos recabados"* e incluso "*procesados o producidos"* por el empresario. Otros prefieren distinguir entre datos "recibidos, observados, inferidos o predichos" por las empresas[49]. Uno de los conceptos más controvertidos del derecho de portabilidad del

[43] *Vid.* Weber, "Data protection…", cit., pp. 201-202; R. Mańko/S. Monteleone, "Contracts for the supply of digital content and personal data protection", European Parliamentary Research Service (EPRS), European Parliament, 2017, p. 5; Roselló Rubert, *Cloud Computing*…, cit., p. 225 y 391.

[44] *Vid.* considerando 26 RGPD. Y Grupo de Trabajo del art. 29 (GT29), "Dictamen 05/2014 sobre técnicas de anonimización", adoptado el 10 abril 2014 (0829/14/ES WP216), p. 10.

[45] Mańko/Monteleone, "Contracts for the supply…", cit., p. 6.

[46] Véase, recientemente, European Data Protection Board (EDPB), "Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects", adoptado el 8 abril 2019.

[47] Cfr. arts. 6.1.b) y 13.2.e) RGPD. Pero como subraya el EDPB (nota anterior, p. 10), "if the contract is terminated in full, then as a general rule, the procession of data will no longer be necessary … and thus the controller will need to stop processing… Hence, it is generally unfair to swap to a new legal basis when the original basis ceases to exist".

[48] B. Kamleitner/V. W. Mitchell, "Can consumers experience ownership for their personal data? From issues of scope and invisibility to agents handling our digital blueprints", en J. Peck/S. B. Shu (Dirs.), *Psychological ownership and consumer behaviour*, Springer, Cham, 2018, p. 91 y ss.; I. van Ooijen/H. U. Vrabec, "Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective", *Journal of Consumer Policy*, 2019, p. 103 y ss.

[49] G. Malgieri, "Property and (Intellectual) Ownership of Consumers' Information: A New Taxonomy for Personal

art. 20 RGPD es, precisamente, la referencia a que versa sobre "datos personales que le incumban, *que haya facilitado* a un responsable". Es obvio que en ese concepto se comprenderán los datos suministrados "activamente" por el consumidor, como datos de contacto, los contenidos generados por él que carga en una plataforma (vídeo, foto, etc.), los comentarios en foros, etc. En este punto, datos "facilitados" y "generados" se superponen. ¿Pero podrán entenderse también "facilitados" aquellos recabados por el empresario con una actitud "pasiva" del usuario o incluso claramente inconsciente o encubierta, como ocurrirá con registros de actividades del usuario (v. gr., conocer los enlaces de los correos electrónicos en los que pincha, los tipos de películas que interrumpe antes de ver el final, la tensión arterial del usuario)? Para abreviar una larga polémica que cuenta con argumentos a favor[50] y en contra de una interpretación expansiva del término "facilitado"[51], la interpretación generosa del GT29 parece haberse impuesto en la práctica: "la expresión *'facilitados por'* incluye los *datos personales que guardan relación con la actividad del interesado o que se derivan de la observación del comportamiento de una persona, pero no los datos que resultan del análisis posterior de dicho comportamiento"*; el derecho de portabilidad incluirá: "*datos facilitados de forma activa y consciente por el interesado* (por ejemplo, dirección postal, nombre de usuario, edad, etc.); [y también] *datos observados facilitados por el interesado en virtud del uso del servicio o dispositivo*. Estos pueden incluir, por ejemplo, el historial de búsqueda, los datos de tráfico y los datos de ubicación de una persona. Pueden incluir asimismo otros datos en bruto tales como el ritmo cardíaco registrado por un dispositivo ponible"[52].

29. En resumen, de acuerdo con las categorías señaladas, el derecho de portabilidad del art. 20 RGPD comprenderá datos facilitados y creados por el usuario y también los observados/recopilados por el empresario, siempre que no hayan sido sometidos a adicional procesamiento que les dé valor añadido[53]. La Directiva, *sólo* respecto a datos personales, asume ese enfoque y estas categorías, pues en el considerando 24 incluye en su ámbito de aplicación los datos facilitados "*en el momento en que se celebre el contrato o en un momento posterior"*, como cuando sube o crea contenidos digitales; y el considerando 38 recuerda que los derechos de supresión y portabilidad (ambos) del RGPD se aplican en caso de resolución contractual respecto a "todos los datos personales *facilitados* por el consumidor al empresario *o recopilados por éste* en relación con todo contrato que entre en el ámbito de aplicación de la presente Directiva".

30. Pero si ahora acudimos a delimitar *qué contenidos que no sean datos personales* podrá recuperar el usuario en virtud del nuevo derecho concedido por el art. 16.4, encontramos que sólo podrá recuperar los que el consumidor haya "*facilitado o creado*" al usar los servicios. No tendrá derecho a los *recolectados u observados* por el empresario. La excepción del art. 16.3.b precisamente excluye éstos al referirse al contenido que "*esté exclusivamente relacionado con la actividad del consumidor durante el uso* de los contenidos o servicios digitales suministrados por el empresario". Por lo tanto, de los tres tipos de datos no personales que potencialmente podría recuperar el consumidor (los anonimizados y agregados, los contenidos ajenos adquiridos y los generados por el consumidor o UGG), el art. 16.4 sólo permitirá recuperar los últimos y además con una interpretación muy restrictiva. De hecho, el considerando 69, los ejemplifica exclusivamente así: "esos contenidos pueden incluir imágenes digitales, archivos de vídeo y audio y contenidos creados en dispositivos móviles". Si esa restricción puede tener algún sentido en relación con la obligación de abstención de uso que tiene empresario, pues esos datos (no personales) de actividad del usuario pueden serle útiles para mejorar su servicio o servir de base para combinarlos y

Data", *Privacy in Germany (PinG)*, 3, 2016, p. 133 (version disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2916058. Último acceso, octubre 2019).

[50] *Vid.* considerandos 60 y 68.

[51] V. gr., véanse argumentos en De Hert *et al.*, "The right to data portability…", cit., pp. 199-200.

[52] Grupo de Trabajo del Art. 29 (GT29), "Directrices sobre el derecho a la portabilidad de los datos", adoptadas el 13.12.2016, revisadas y adoptadas el 5.4.2017 (16/ES WP 242 rev.01), p. 12.

[53] De acuerdo con GT29, "Directrices sobre el derecho a la portabilidad", cit., p. 12: "por el contrario, todos los datos personales que hayan sido creados por el responsable del tratamiento como parte del tratamiento de datos, p.ej. mediante un proceso de personalización o recomendación, mediante categorización del usuario o creación de perfiles, son datos que se deducen o infieren de los datos personales proporcionados por el interesado y no están cubiertos por el derecho a la portabilidad de los datos".

tratarlos con otros datos con diversos fines, no se entiende por qué un tal recorte del derecho a recuperar datos no personales. El consumidor puede tener un interés legítimo en conocer, incluso tras la resolución del contrato, por ejemplo, su historial de actividad y navegación, la frecuencia y períodos en que accedía a servicio de juego *online* cuando era adicto o sus datos de geolocalización observados al usar una aplicación o red social (v. gr., *Facebook*, si el consumidor quiere probar a alguien, por ejemplo, que no estaba en determinado lugar en un momento dado). El art. 16.3.b ni siquiera limita la exclusión a los casos en que devolver esos datos fuese desproporcionado para el empresario. Simplemente queda excluido en todo caso. Se trata de una decisión de política legislativa, desde mi punto de vista, equivocada y contraria a la generación de un alto nivel de protección del consumidor exigida en el art. 169 TFEU.

III. Comparación e interacción entre los nuevos derechos

1. Derecho de supresión y derecho a impedir el uso de los datos

A) Reglas y excepciones

31. Cuando el contratante de contenidos o servicios digitales retira su consentimiento al tratamiento de datos personales, como típicamente ocurrirá con la extinción del contrato por resolución, podrá exigir que se borren o supriman todos los datos personales en poder del responsable, si el tratamiento no se basa en otro fundamento jurídico (art. 17.1.b RGPD). Este otro fundamento podría ser, por ejemplo, el "interés legítimo" del empresario, para realizar mercadotecnia directa de sus productos y servicios digitales[54], salvo oposición del usuario (art. 17.1.c) también a estas ulteriores comunicaciones. De las seis situaciones en que el art. 17 RGPD reconoce la obligación de suprimir los datos personales, junto a la revocación del consentimiento, destaca para el escenario de los contratos de suministro digital la contemplada en el art. 17.1.f) en relación con el art. 8.1.a) RGPD: cuando los datos se obtuvieron en relación con la oferta directa a menores de 16 años de servicios de la sociedad de la información.

32. El contratante que resuelve el contrato (o de cualquier otra manera lo extingue) podrá dirigirse claramente a su contraparte como responsable del tratamiento de sus datos personales (red social, blog, plataformas de comercio electrónico, servicio de almacenamiento en la nube, etc.); además, podrá exigir a éste que informe a otros responsables que estén tratando estos datos de la solicitud del interesado de la supresión de cualquier enlace a ellos o cualquier copia o réplica (art. 17.2 RGPD), que es propiamente la traslación al reglamento del "derecho al olvido" en el entorno en línea inspirado en resoluciones judiciales bien conocidas[55]. Ahora bien, esta segunda obligación del empresario en su calidad de responsable del tratamiento de datos está atenuada con lógicos cánones de proporcionalidad: "el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas". No es, por tanto, un derecho absoluto. Adicionalmente, al amparo del derecho al olvido de origen jurisprudencial creado por la STJUE de 13 de mayo de 2014 (*Google Spain*), el interesado podrá solicitar directamente a esos terceros intermediarios que generan enlaces y búsquedas no ya la supresión de los datos de la fuente a la que redirigen, sino el uso de protocolos de exclusión tipo *robot.txt* u otras medidas oportunas para dificultar la búsqueda.

33. El art. 17.3 RGPD establece cinco excepciones o límites al ejercicio del derecho de supresión. Las dos más relevantes en el escenario de resolución del contrato de suministro de contenidos y servicios digitales son las siguientes: por una parte, cuando el tratamiento sea necesario "para la formulación, el ejercicio o la defensa de reclamaciones" (17.3.e), lo cual será especialmente aplicable cuando las partes contractuales no estén de acuerdo acerca del incumplimiento de las obligaciones que dieron

[54] Considerando 47 RGPD. Véase también el entendimiento del *marketing* directo como legítimo interés del responsable del tratamiento en GT29, "Dictamen 06/2014 sobre el concepto de interés legítimo…", cit., p. 29 y ss.

[55] Art. 17.2 y considerando 66. *Vid.* STJUE 13 mayo 2014, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, asunto C-131/12 (ECLI:EU:C:2014:317).

lugar a la resolución, o cuando ésta fue promovida por el empresario. Por otra parte, pese la terminación, el tratamiento de datos continuará (17.3.a) "para ejercer el derecho a la libertad de expresión e información". Así, la revelación voluntaria de datos personales propios o manifestaciones abiertas a todo el público en redes sociales (como *Facebook* o *Twitter*) encontrarán en este límite un importante valladar a su total desaparición cuando tienen réplica o comentario en ejercicio de la libertad de expresión o cuando los medios de comunicación se hacen eco de ellos al amparo de la libertad de información.

34. Como ya se explicó, la obligación del empresario de abstenerse de usar los contenidos digitales facilitados o creados por el usuario que no sean datos personales presenta la diferencia esencial en la DCSD de no exigir el borrado o eliminación de tales datos. Es conocida la gran dificultad técnica que existe para la supresión o borrado absoluto y sin huella en el contexto del Internet 2.0, al existir réplicas fuera de la plataforma de origen de los contenidos, copias provisionales o definitivas en otros servidores, etc., que escapan del control del prestador del servicio inicial. El legislador no ha querido imponer cargas especialmente gravosas sobre redes sociales y servicios de almacenamiento cuando no existen datos personales implicados. La principal excepción a este derecho a impedir el uso figura desde la propuesta inicial de la Directiva presentada por la Comisión Europea: si se cumplen cumulativamente lo que debe entenderse como dos requisitos, tanto el empresario como el resto de usuarios de sus servicios digitales tendrán derecho a seguir usando los CGU. Esos requisitos son que el contenido "haya sido generado conjuntamente por el consumidor y otras personas" y, segundo, que "otros consumidores puedan continuar haciendo uso del contenido". Este uso por otros consumidores debe interpretarse como concausa, no como consecuencia de la excepción. En el fondo, el fundamento de esta excepción tiene su acertado fundamento en consideraciones similares a las del art. 17.3.a RGPD, relacionadas también con la libertad de expresión e información, además de con principios básicos de la propiedad intelectual. Así, por ejemplo, no será posible la retirada de contenidos que merezcan la consideración de obras derivadas cuando el titular de los derechos de propiedad intelectual autorizó previamente la transformación (v.gr., de un vídeo o fotografía), ni el borrado de comentarios o entradas en redes sociales en hilos de conversación, ni el borrado de los mensajes recibidos en aplicaciones de mensajería instantánea como *WhatsApp*, ni los correos electrónicos recibidos.

35. Sin embargo, en las versiones del Parlamento Europeo y del Consejo se introdujeron tres excepciones más que limitan considerablemente lo que podrían haber sido derechos razonables del consumidor a una restitución plena de contraprestaciones (o de creaciones propias) una vez que éste ha salido de la relación contractual por incumplimiento del empresario. Según el art. 16.3 DCSD, el empresario no tendrá por qué abstenerse de usar ese contenido cuando:

> "a) no tenga *ninguna utilidad fuera* del contexto de los contenidos o servicios digitales suministrados por el empresario;
> b) esté *exclusivamente relacionado con la actividad del consumidor durante* el uso de los contenidos o servicios digitales suministrados por el empresario;
> c) haya sido agregado con otros datos por el empresario y *no pueda desagregarse* o solo pueda desagregarse realizando esfuerzos desproporcionados."

36. Sobre esas tres excepciones, que se aplican igualmente –y con menos sentido aún, en algún caso– al derecho de recuperación de contenidos del consumidor, conviene hacer las siguientes consideraciones conjuntas:

a) Curiosamente, los considerandos de la Directiva, tan locuaces e ilustrativos dando ejemplos concretos, no aportan absolutamente ninguno para estas tres excepciones (considerandos 69 y 71), que reproducen literalmente, ni tampoco explican su justificación. Sólo respecto al derecho a recuperar datos, el considerando 71 indica que "en tales casos, *los contenidos no tienen ninguna utilidad ni interés práctico relevantes para el consumidor*, a la vez que se tienen en cuenta los intereses del empresario". La primera afirmación es un manifiesto exce-

so, al presumir *iuris et de iure* esa ausencia de interés: el consumidor sí puede tener diversas razones para conocer su historial de actividad (superar una adicción, reconstruir sus movimientos, escribir unas memorias, demostrar a terceros su carácter activo en el entorno digital o su habilidad con determinados programas de ordenador, etc.); la falta de utilidad fuera del servicio digital original será cierta cuando lo que se pretendiera con la recuperación fuera trasvasar o portar los contenidos a una plataforma distinta si el formato no es interoperable (por ejemplo, un avatar en un juego digital, las gemas o accesorios adquiridos en un juego, los *likes* o *ratings* respecto a contenidos propios de una plataforma, los dibujos o diseños en un programa de código cerrado), pero para el consumidor puede tener una utilidad, siquiera sea emotiva o sentimental recuperar de alguna manera esos contenidos construidos con tiempo y, en su caso, dinero, aunque no pueda "usarlos" interactivamente en otro contexto.

b) La versión aprobada se parece mucho a la sugerida por el Consejo[56]. En la versión aprobada en el Parlamento Europeo[57], para las tres excepciones se incluía al menos la cláusula compensatoria o de equilibrio sobre la no abstención de uso sólo respecto a "los contenidos de cuya utilización no sea posible abstenerse *sin realizar un esfuerzo desproporcionado e irrazonable*"; y similar límite de proporcionalidad existía también en esa versión parlamentaria respecto a la puesta a disposición de los contenidos.

c) Por lo tanto, al configurar estas excepciones, la balanza se ha inclinado en exceso a favor de los intereses del empresario: así sucede también al no exigir que sea imposible desagregar los datos, sino que si sólo pueden desagregarse con esfuerzos desproporcionados prevalecerá el interés del empresario. Este límite podría incluso dar lugar a fáciles picarescas empresariales, pues bastará agregar determinados datos, lo que será habitual, por ejemplo, en el internet de las cosas.

37. En conclusión, estas tres excepciones tienen más sentido, desde el punto de vista del equilibrio de los intereses, en relación con el derecho a impedir el uso, que con el derecho a recuperar los contenidos. Tanto la actividad del usuario como la agregación con otros datos tienen un componente de utilidad en la actividad empresarial (menos justificación se encuentra a seguir usando todo tipo de contenidos del usuario en la plataforma si ésta tiene formato cerrado y no interoperable, porque se niega al consumidor un razonable pseudo "derecho al olvido" una vez que resuelve el contrato, cuando no generó conjuntamente con otros esos contenidos). Prejuzgar la falta de utilidad para el consumidor de los propios contenidos que él generó con su actividad es un exceso normativo que prácticamente afrenta la dignidad de la persona: que ésta no sea identificable a través de esos contenidos no significa que no tengan para ella un valor y utilidad indudable. Mientras la posibilidad de seguir usando el empresario los CGU creados conjuntamente y usados por varios consumidores tiene apoyo constitucional, el resto de límites busca en realidad no entorpecer los modelos de negocio basados en el *big data*.

B) Cómo

38. El actual estado de la tecnología revela las dificultades de conseguir una supresión o borrado total y definitivo de los datos. Obviamente, la fórmula más definitiva será la inutilización o destrucción del *hardware* (discos duros) en que el empresario almacena la información; pero aparte de su carácter antieconómico, tampoco esta acción asegura la desaparición de los datos en internet, dadas las copias periódicas que suelen hacerse de los sitios web no sólo por sus creadores sino por terceros, las copias en

[56] Consejo de la Unión Europea, *Orientación General: Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a determinados aspectos de los contratos de suministro de contenidos digitales (primera lectura)*, 9901/17 ADD 1, Bruselas, 1 junio 2017, p. 32.

[57] Parlamento Europeo, *Informe sobre la propuesta de Directiva del Parlamento Europeo y del Consejo relativa a determinados aspectos de los contratos de suministro de contenidos digitales (COM(2015)0634 – C8-0394/2015 – 2015/0287(COD)),* Comisión de Mercado Interior y Protección del Consumidor, Comisión de Asuntos Jurídicos (ponentes: Gebhardt, A. Voss), A8-0375/2017, 27 noviembre 2017, p. 82.

la memoria caché, etc. Tres factores dificultan, por tanto, la eliminación total: la persistencia de datos, las redundancias y el respaldo[58]. La técnica más empleada consiste en la *sobreescritura de los datos*: los datos que se ordena borrar son sobreescritos por datos nuevos que se almacenan en el mismo dispositivo de *hardware*, de manera que cuantas más veces se escriba sobre los datos inicialmente borrados (que no desaparecen por completo con esa técnica) más difícil será recuperarlos[59].

39. En relación con datos personales, a la supresión puede equivaler su anonimización absoluta e irreversible[60]; en cambio, la "seudonimización" –que consiste en la sustitución de un dato por otro atributo en un archivo o registro, aunque los datos podrían volver a ser identificables con una persona concreta si la información adicional con la que se operó el proceso fuese reversible– no comporta supresión, aunque pueda ser una técnica útil para potenciar el derecho al olvido (esto es, dificultar su acceso) en buscadores y páginas de terceros.

40. La obligación del empresario de abstenerse de usar los contenidos que no sean datos personales puede cumplirse igualmente con las técnicas de destrucción, borrado y sobreescritura descritas; el NIST (*National Institute of Standards and Technology*) incluye entre las técnicas de la así llamada "*sanitization*" tres métodos: limpiar, purgar y destruir los datos. O bien podría cumplirse la obligación legal simplemente con el "bloqueo" de los datos, que consiste en su identificación y reserva para impedir su tratamiento salvo cumplir obligaciones legales, de manera que el personal que normalmente tendría acceso a ellos dentro de la empresa tampoco podría acceder, sino sólo una persona con la máxima responsabilidad y únicamente cuando hubiese un requerimiento judicial o administrativo al efecto. Se trataría, en definitiva, de utilizar las técnicas propias del derecho a la limitación del tratamiento (art. 18 RGPD), como podría ser, por ejemplo, "trasladar temporalmente los datos seleccionados a otro sistema de tratamiento" (considerando 67 RGPD).

41. En la práctica del mercado digital, las empresas implementan diversas soluciones: *Facebook* ofrece una vía más definitiva para eliminar totalmente todo tipo de datos, como es la "desactivación" de la cuenta y otra temporal o transitoria, que consiste en la "suspensión" de la cuenta con posibilidad de retorno. *Youtube* permite que el usuario revoque la licencia de uso de los contenidos facilitados por él a la plataforma, pero declara irrevocable el consentimiento para publicar los comentarios realizados por el usuario en relación con los contenidos audiovisuales de este canal (lo cual tendría cabida en la excepción del art. 16.3.d DCSD sobre contenidos creados conjuntamente por varios usuarios).

42. En cuanto al plazo para suprimir los datos personales, el art. 17.1 RGPD establece que se hará "sin dilación indebida" y por aplicación del criterio general del art. 12.3 RGPD, como máximo un mes desde la recepción de la solicitud, prorrogable a dos meses. En la práctica varios operadores importantes no cumplen esos plazos, al congelar los datos más tiempo del preciso e incluir una suerte de período de arrepentimiento extraordinario[61].

---

[58] M. Henriques/J. Ding, "Purging the Cloud: Data Destruction in the Age of Cloud Computing", *Womble Carlyle*, 23 junio 2014; K. Aissaoui/H. Ait/H. Belhadaoui/M. Rifi, "Survey on data remanence in Cloud Computing environment", *2017 International Conference on Wireless Technologies, Embedded and Intelligent Systems* (WITS), Fez, 2017, pp. 152-155.

[59] Sobre estas medidas, *vid.* Roselló Rubert, *Cloud Computing*…, cit., p. 385.

[60] Véase una detallada exposición de técnicas de anonimización y seudonimización en Grupo de Trabajo del art. 29 (GT29), "Dictamen 05/2014 sobre técnicas…, cit., p.12 y ss., en particular la aleatorización (adición de ruido, permutación, privacidad diferencial), generalización (con medidas de agregación, anonimato k, diversidad l, proximidad k), etc. Sobre su aplicación por *Google*, *vid.* nota siguiente.

[61] De las condiciones generales examinadas en el presente ensayo, destaca *Google* por su transparencia en cuanto a los distintos tiempos empleados para eliminar distintos datos y la distinción entre lo conservado, lo eliminado totalmente y lo eliminado progresivamente: *vid.* https://policies.google.com/technologies/retention?hl=es y también sobre cómo emplean las citadas técnicas de generalización y adición de ruido en https://policies.google.com/technologies/anonymization?hl=es. *Twitter*, por ejemplo, establece plazos demasiado largos y otras empresas utilizan una notoria vaguedad (*Apple*).

C) Prueba

43. La demostración de que se ha cumplido el deber de supresión o el deber de abstenerse de usar los datos no sólo es de difícil prueba, sino que además ésta será poco convincente si no intervienen terceros que acrediten la eficacia de las medidas adoptadas por el empresario.

Algunas técnicas, como la reescritura de datos, permiten obtener una garantía documental del proceso, mientras que otros mecanismos de borrado tienen más dificultades de certificación[62]. La prueba del *non facere* (abstenerse de usar) es aún más difícil que la del *facere* (borrar) sin una suerte de auditorías informáticas de terceros que refrenden las manifestaciones del responsable del tratamiento, salvo que la infracción aflore precisamente por acreditarse el uso de los contenidos y la trazabilidad de su origen. Por eso, el enfoque del RGPD (arts. 42 y 43) es el adecuado y prácticamente único posible, al instar a los Estados miembros, autoridades de control, al Comité y la Comisión a promover la creación de mecanismos de certificación y de sellos y marcas para demostrar el cumplimiento de obligaciones como éstas. Y por la misma razón, la falta de previsión en la nueva Directiva es una laguna importante. En todo caso, hasta la fecha, las autoridades nacionales de control han sido firmes en sancionar a las plataformas de contenidos y servicios digitales cuando no han suprimido los datos personales pese a ser legítimamente requerido por los usuarios[63].

2. Derecho de portabilidad y derecho de recuperación de datos

A) Reglas y excepciones

44. Aunque en las versiones finalmente aprobadas de los considerandos del RGPD y de la DCSD los fundamentos de ambos derechos parecen separarse[64], el examen de los considerandos y manifestaciones durante la tramitación legislativa de ambas normas permite hallar unas finalidades semejantes: favorecer la competencia entre los operadores de mercado, evitando mercados cautivos y plataformas cerradas[65], con un interés de fondo en alentar la creación de formatos interoperables[66]; garantizar el derecho del consumidor a resolver el contrato ante incumplimientos sin el temor a perder datos o contenidos para él valiosos[67], lo que, en definitiva, en el terreno de los datos personales se traduce en reforzar el control sobre sus propios datos[68]. En esta línea, el considerando 70 DCSD aclara que "el empresario, previa solicitud del consumidor, debe poner dicho contenido a disposición de este *tras* la resolución del contrato"; por lo tanto, también *tras* extinguirse el contrato por esa vía y no sólo antes de la resolución, aunque no se fija un plazo límite para esa recuperación postcontractual.

45. El derecho de portabilidad contaba con antecedentes exitosos en el ámbito europeo: en el sector de las telecomunicaciones primero se aprobó la portabilidad de los números de teléfono (Directiva 2002/22/EC). Desde otra perspectiva, el Reglamento (EU) 2017/1128 de 14 de junio de 2017, relativo a la portabilidad transfronteriza de los servicios de contenidos en línea en el mercado interior, eliminó las trabas al disfrute de estos servicios derivadas de las limitaciones territoriales de las licencias de uso sobre material sometido a derechos de autor.

46. El derecho de portabilidad recaerá sobre sobre datos personales propios del interesado ("que le incumban") que "facilitó", en el amplio sentido antes expuesto, al responsable del tratamiento. Tanto

[62] Roselló Rubert, *Cloud Computing*…, cit., pp. 397-398.

[63] Por ejemplo, la Agencia Española de Protección de Datos sancionó a *Facebook* con 1,2 millones de euros en resolución de 2017 por mantener *cookies* de cuentas eliminadas que seguían recogiendo y tratando información durante 17 meses tras la supuesta supresión.

[64] Actualmente sólo consta el tenor del considerando 69 RGPD y del considerando 70 DCSD.

[65] Considerando 46 de la Propuesta de Directiva de la Comisión (PDCD-2015)

[66] Considerando 68 RGPD.

[67] Considerando 39 de la PDCD-2015 de la Comisión Europea.

[68] Considerando 68 RGPD, *ab initio*.

esta delimitación del tipo de datos implicados como la previsión de que el derecho de portabilidad "no afectará negativamente a los derechos y libertades de otros" suponen un importante límite a una situación común en los servicios de redes sociales, como son los contenidos compartidos en que aparecen datos personales de distintos usuarios, como ocurre en fotos o vídeos en las que aparecen varios sujetos identificables, sean todos o no usuarios de la red social, foros en que quedan registradas opiniones de distintos usuarios, etc., así como las casos de contenidos creados conjuntamente por varios usuarios que contengan datos personales. Una lectura superficial del art. 20.4 RGPD podría llevar a concluir que en esos casos no es posible conseguir nunca la portabilidad, por estar implicados derechos de otros. Sin embargo, el artículo no establece una prohibición total, sino sólo que la portabilidad no afecte negativamente los derechos ajenos. En este sentido, la solución que propone el GT29 resulta equilibrada: los responsables del tratamiento deberían establecer herramientas para permitir a los interesados seleccionar los datos pertinentes y excluir los datos de terceros, así como implementar los mecanismos necesarios para recabar el consentimiento de estos últimos y sólo en este caso permitir la portabilidad en línea[69]. Otra interpretación para que los derechos de terceros no se erijan en todo caso como un impedimento para el derecho de portabilidad, podría ser acudir al resto de reglas y principios del RGPD y, en particular, entender que el usuario que quiere cambiar de red social tiene un interés legítimo en el sentido del art. 6.1.f RGPD[70], interés contra el que no prevalecen en todo caso los derechos ajenos si se examinan, caso por caso, todas las circunstancias (tales como para qué su usan los datos, las expectativas razonables sobre esos usos, garantías adicionales empleadas por el responsable, etc.)[71]. La noción de "expectativa razonable" puede desempeñar un papel importante, pues dependiendo del núcleo más cerrado o abierto de los destinatarios de contenidos dentro de una plataforma, un usuario podría esperar que sus datos sólo pudiesen accederse en esa plataforma pero no en otras o al revés[72].

En definitiva, existen varios otros derechos que cuentan con un grado de prevalencia distinto sobre el derecho de portabilidad: el derecho al olvido, que no puede ser perjudicado por el derecho de portabilidad (art. 20.3 RGPD), los derechos de terceros, que no deberán verse afectados negativamente por la portabilidad (art. 20.4) y los intereses públicos, que prevalecerán en todo caso sobre la portabilidad (art. 20.3)[73].

47. En cuanto al derecho a recuperar los contenidos que no sean datos personales facilitados o creados por el consumidor, la nueva Directiva no pone ningún reparo a recuperar los contenidos generados conjuntamente por el consumidor y otras personas (art. 16.4 DCSD *a contrario)*, incluso aunque éstas sigan haciendo uso del contenido, pues presume que todos los coautores pueden solicitar esa portabilidad, pero ninguno podrá solicitar al empresario que los destruya o impida su acceso en tanto que haya consumidores que puedan usarlos (art. 16.3.d DCSD). En cambio, con restricción excesiva, como ya se ha criticado, la Directiva impide la recuperación de estos CGU en otras tres situaciones (falta de utilidad fuera del contexto original, versar exclusivamente sobre la actividad de uso del consumidor y no poder desagregarse fácilmente de otros datos).

48. Aún cabría preguntarse por la posibilidad de extender los derechos de recuperación y portabilidad a situaciones no contempladas por la Directiva ni por el RGPD, precisamente en el contexto general de extinción de los contratos sobre contenidos y servicios digitales, más allá del caso concreto de la resolución, cuando llegue el momento de transposición de la Directiva. En el escenario de la resolución contractual es claro que "el consumidor se abstendrá de utilizar los contenidos o servicios digitales y de ponerlos a disposición de terceros" (art. 17.1 DCSD) y que el empresario tiene el derecho de hacer inaccesible el contenido o el servicio para el consumidor o inhabilitar su cuenta de usuario (art.

[69] GT29, "Directrices sobre el derecho a la portabilidad…", cit., pp. 18 y 22.

[70] Así, Stoykova, "The Right to Data Portability", cit., p. 70, quien trata de salvaguardar la portabilidad reforzándola con otras reglas generales tales como la excepción de actividades domésticas del art. 2.2.c) RGPD. *Vid.* también de Hert *et al.,* "The right to data portability…", cit., p. 198.

[71] *Vid.* Hert *et al.*, "The right to data portability…", cit., p. 198 y GT29, "Dictamen 06/2014…", cit.

[72] See Janal, "Data Portability…, cit., p. 62.

[73] Sobre este orden de prelación, *vid.* Hert *et al.*, "The right to data portability…", cit., p. 198.

16.5 DCSD). Pero, ¿cuál debería ser la regla en otros supuestos de extinción no patológica o natural? En relación con contenidos puestos a disposición por el empresario (v. gr., películas en *Apple o Google Stores*) o por otros usuarios (v.gr., vídeo en *Youtube*), para responder a esa cuestión es preciso deslindar el modelo de negocio mediante el que se adquirió el derecho al disfrute de la prestación digital: si el usuario podía acceder a los contenidos mediante descarga de una copia de la obra o prestación, existe una expectativa razonable de poder seguir utilizándola tras la extinción del contrato con el proveedor. En tal caso la norma podría garantizar la posibilidad de migrar el contenido a otros dispositivos físicos (ordenador, tableta, etc.) o a su almacenamiento en otro servidor en la nube para continuar su uso[74]. En cambio, si el consumidor accedía a esos contenidos en *streaming* difícilmente podrá pretender tras la extinción del contrato que le ligaba con el empresario seguir gozando de acceso a los contenidos.

B) Cómo

49. La recuperación de los datos, tanto en el RGPD como en la DCSD, implica la posibilidad de descarga directa por parte de los usuarios "sin cargo alguno y sin impedimentos por parte del empresario, en un plazo razonable y en un formato utilizado habitualmente y legible electrónicamente" (art. 16.4 DCSD); el art. 20.1 RGPD sólo añade que ha de tratarse de un formato estructurado. El objetivo es que el formato de los datos pueda acabar siendo interoperable, pero no existe una obligación terminante al respecto. Aunque pueden no existir formatos estandarizados que permitan el trasvase de algunos datos (¿los *likes* en una determinada red social?), lo cierto es que algunos de los principales operadores ya han implementado sistemas de fácil uso que permiten esa recuperación mediante descarga de un archivo .zip con subcarpetas según los contenidos/datos/formatos implicados, como ocurre con la opción de descargar todos los datos que *Google* tiene de un usuario[75]; otros remiten al consumidor a diversas páginas de su interfaz para descargar (y, en su caso, borrar) los contenidos, comenzando por la página de configuración de la cuenta y siguiendo con un peregrinaje a través de diversos enlaces. En cuanto a la portabilidad directa de un responsable de tratamiento a otro, técnicamente es factible con la creación de una API (*application programming interface*) específica; a falta de obligación legal al respecto, el fomento de un mercado digital único requerirá otros incentivos. El ejemplo de *WhatsApp* es ilustrativo, al permitir hacer copia de mensajes y sus archivos adjuntos en las plataformas de almacenamiento en la nube más populares de los tres sistemas operativos más empleados[76], pero no facilita la migración a otros competidores de mensajería gratuita a través de internet.

50. En cuanto al *carácter gratuito* tanto del derecho de recuperación como de la portabilidad, ambas normas lo consagran (art. 12.5 RGPD y 16.4 DCSD), aunque respecto a los datos personales el RGPD establece la posibilidad de un canon razonable o negarse a actuar "cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo". Esta excepción debe entenderse en relación con las peticiones de un concreto usuario, no del conjunto de solicitantes que por su magnitud impliquen costes al proveedor, quien no podrá repercutirlos a los concretos usuarios[77].

51. El *plazo* para atender la petición del usuario en la Directiva se deja abierto ("en un plazo razonable"), en tanto que el Reglamento lo concreta en un mes, prorrogable a dos en caso de complejidad o alto número de solicitudes[78]. En el estado actual de la tecnología es sencillo cumplir con la petición de forma automatizada en breves plazos, pese a lo cual bastantes proveedores fijan en sus contratos una horquilla que va de días a bastantes meses, o se reservan la facultad de fijar el plazo al terminar el contrato.

[74] Siempre que se respeten los derechos de propiedad intelectual sobre ese contenido y siempre que la información precontractual hubiese garantizado esa interoperabilidad, pues las reglas sobre el límite de copia privada entrarán en juego en este supuesto.

[75] https://takeout.google.com.

[76] Esto es, *Android, Windows* y *MacOs*; en particular, permite efectuar una copia de los contenidos en *Google Drive, One Drive* e *iCloud* (*vid.* el proceso en https://faq.whatsapp.com).

[77] GT29, "Directrices sobre el derecho a la portabilidad…", cit., p. 18.

[78] El art. 20 RGPD no fija un plazo; el art. 12.3 RGPD sería de aplicación.

C) Prueba

52. Pueden existir situaciones conflictivas cuando el proveedor asegure que cumplió pero lo hizo, por ejemplo, con un formato ilegible o mediante un enlace que no funcionó e imputa el incumplimiento a la impericia del consumidor o a su entorno operativo. Pero los mayores problemas de prueba estribarán en comprobar si el proveedor de contenidos o servicios digitales restituyó al consumidor *todos* los datos, personales o no personales, que de él tenía. Nuevamente, sin una certificación de terceros de confianza, el usuario ha de confiar en una mera declaración unilateral del proveedor/responsable, sin plena certidumbre de haber recibido, por ejemplo, todos los datos recabados u observados por el proveedor, de si las técnicas aplicadas han anonimizado a plenitud los datos o de si el proveedor cedió datos o contenidos a terceros sin haber recabado el consentimiento del usuario interesado, etc.

3. Relación entre los derechos en el momento de su ejercicio

53. Desde el momento en que la Directiva no impone la eliminación de los datos no personales del consumidor que éste quiere recuperar, sino sólo la abstención de su uso por el empresario, la relación entre ambos derechos es sencilla y compatible. Salvo que el clausulado lo establezca (como ocurre en *Youtube*), el consumidor no tendrá derecho a exigir el borrado de estos CGU. Por eso es posible, como recuerda el considerando 70 DCSD, que el consumidor recupere sus contenidos *después* de resolver el contrato. Esta previsión implícitamente establece una obligación de conservar esos datos no personales a cargo del proveedor. Pero, ¿durante cuánto tiempo? No existe una pista al respecto en la Directiva ni en sus considerandos.

54. Más problemática es la relación entre el derecho de supresión y el de portabilidad en el RGDP. Obviamente el interesado que desee recuperar sus datos o portarlos a otro responsable deberá hacerlo antes de ejercer el derecho de supresión. En este sentido, es posible el ejercicio conjunto de ambos derechos, pero también por separado, siempre que la portabilidad se solicite y consume antes que la supresión. De ahí que solicitar la portabilidad no implica directamente destruir los datos personales, lo cual debe ser objeto de una petición expresa del interesado[79]. La doctrina viene interpretando la mención del art. 20.3 RGPD a que el derecho de portabilidad se entenderá "sin perjuicio" del derecho de supresión, no como una jerarquía en sentido estricto, sino de que la portabilidad no impida la supresión de los datos[80]; en este sentido, la portabilidad no puede ser esgrimida por un responsable del tratamiento como método para retrasar o rechazar la supresión solicitada por el usuario, ni impone al responsable la obligación de conservar datos personales más tiempo del necesario[81].

55. Para valorar toda la potencialidad del derecho de portabilidad hay que considerar *dos escenarios* distintos: el del *consumidor insatisfecho y* el del *consumidor satisfecho* con su proveedor de servicios o contenidos digitales. En el primer caso, los estudios socioeconómicos demuestran que el consumidor querrá ejercitar ambos derechos, cambiar de compañía con la transición más cómoda posible y eliminar todos sus datos personales en poder del primer proveedor. Se trata de un rasgo característico de la llamada "economía del cambio" (*switching economy*)[82]. Por contraposición, un consumidor satisfecho con su proveedor puede querer portar todos sus datos a otro proveedor, sin abandonar el primer servicio ni, por tanto, eliminar los datos que tiene ese empresario. Es decir, no sólo querrá usar sus datos, sino "reusarlos", que es la base de la portabilidad (y eso vale tanto para datos facilitados como para datos observados,

[79] El considerando 68 afirma que el ejercicio del derecho de portabilidad "no debe implicar la supresión de los datos personales concernientes al interesado que este haya facilitado para la ejecución de un contrato, en la medida y durante el tiempo en que los datos personales sean necesarios para la ejecución de dicho contrato".

[80] Li, "A Tale of Two Rights…", cit., p. 183, Hert *et al.*, "The right to data portability…", cit., p. 201.

[81] GT29, "Directrices sobre el derecho a la portabilidad…", cit., pp. 8-9.

[82] Li, "A Tale of Two Rights…", cit., pp. 186 y 189.

sean o no personales)[83]. El escenario del consumidor satisfecho puede darse tanto en casos de mercados sustitutivos, como, más aún, en supuestos de mercados complementarios[84], cuando exportar todos los datos de una cuenta facilita continuar con la misma identidad digital en un servicio totalmente distinto. El consumidor puede tener sus razones, por ejemplo, para tener dos cuentas en redes sociales que se actualicen simultáneamente, dos blogs con los mismos contenidos o una copia de seguridad en un servidor en la nube que se porte periódicamente a otro prestador del mismo tipo de servicio de almacenamiento. Con más razón incluso, podrá el consumidor querer trasvasar sus creaciones, historial de actividad, perfiles, *ratings* o valoraciones, etc. de una red social a otra plataforma que ofrezca servicios totalmente distintos y complementarios, sin abandonar dicha red social (v. gr., de una red social general como *Facebook* a una red de contactos matrimoniales). Un ejemplo de estos mercados complementarios sería el ejemplo de la copia de contenidos de *WhatsApp* en servidores de almacenamiento en la nube. La portabilidad, por lo tanto, ni se ejercitará siempre de forma conjunta con el derecho de supresión, ni es siempre una herramienta que ponga en riesgo la retención de clientes, sino que tiene un gran potencial para la creación de nuevos modelos de negocio y un mercado digital más dinámico. Ahora bien, corresponde ya al Derecho de la competencia y no al Derecho de consumo determinar en qué situaciones (por ejemplo de abuso de posición dominante o en casos de mercados complementarios generados por pequeñas compañías) sería deseable acentuar las obligaciones de portabilidad directa de datos personales y en cuáles no.

4. La plasmación de los derechos en la práctica actual

56. Un examen de las condiciones generales de los contratos de las principales plataformas de contenidos y servicios digitales[85] revela que la mayoría describen con bastante corrección los derechos de *supresión* de datos personales del usuario y remiten a ulteriores páginas sobre cómo realizarlo, *pero pocas entran en una descripción de detalle del derecho de portabilidad* (apenas se refieren a él *Youtube, Facebook* o *Instagram*; algunas se limitan a recordar escuetamente el derecho garantizado por el RGPD, como *Spotify*, sin explicar técnicamente cómo se llevará a cabo*)*; entre las que sí lo hacen destaca el grado de transparencia de *Google* en las condiciones generales de aplicación todos sus servicios y, también, las empresas dedicadas a servicios de almacenamiento en la nube, precisamente, porque una de sus características de esencia, junto a la custodia de los datos, es la posibilidad de que el consumidor recupere los datos almacenados sin mayor inconveniente: en este sentido, *Dropbox* y *Google Play* contienen cláusulas e instrucciones detalladas sobre la portabilidad. Sin embargo, aún es muy escaso el reflejo en los clausulados del derecho a la portabilidad de responsable a responsable (cabe destacar en este sentido los servicios que ofrece *WhatsApp* para hacer copia de su contenido en los tres servicios de almacenamiento más extendidos).

57. Con toda lógica, tanto los servicios de redes sociales como los servicios de almacenamiento no sólo abordan los derechos de supresión y portabilidad (de datos personales), sino también los derechos del usuario a suprimir y recuperar los *contenidos generados por ellos (CGU)*, sean o no éstos datos personales (se adelantan, de esta manera, en algún caso con ventaja sobre la nueva Directiva, en otros no, al futuro régimen). Ahora bien, incluso los catalogados como empresas de suministro de contenidos digitales (por descarga o por *streaming*), que prestan especial atención a las licencias que otorgan a los usuarios para el disfrute de aquellos contenidos, dedican en sus estipulaciones diversas cláusulas a los CGU –por la vertiente de "comercio social*"* que tienen mediante los comentarios, valoraciones, blogs,

[83] Hert *et al.*, "The right to data portability…", cit., pp. 202-203), que formulan diversas sugerencias para lo que denominan el "*adieu scenario*" y el "*fusing scenario*".

[84] V*id.* el estudio empírico de B. Engels, "Data portability among online platforms", *Internet Policy Review*, 5-2, 2016, p. 1 y ss.; también, R. Stoykova, "The Right to Data Portability as a Market Tool", *Computer Law International (CRi)*, 2, 2018, p. 47 y ss.

[85] Para un examen de detalle de los clausulados concretos, *vid.* S. Cámara Lapuente, "Extinción de los contratos sobre contenidos y servicios digitales y disponibilidad de los datos: supresión, recuperación y portabilidad, en P. Castaños Castro/ J. A. Castillo Parrilla (dirs.), *El mercado digital de la Unión Europea*, Reus, Madrid, 2019, pp. 157-249, en especial, pp. 233-243.

listas, etc. que admiten que sus usuarios les faciliten–; en estos casos, cabe encontrar algunas renuncias de los usuarios contrarias a la normativa de propiedad intelectual, al RGPD y a la nueva Directiva.

58. En cuanto a la supresión, las principales redes sociales introducen la excepción relativa a la información que otras personas han compartido sobre el usuario (*Facebook*), las copias que tienen otros usuarios (por ejemplo de mensajes, *WhatsApp*) o las copias de motores de búsqueda o de terceros (v. gr. de tuits públicos, en el caso de *Twitter*). Los plazos que los contratos plasman sobre el derecho de supresión van desde una descripción detallada pero aproximativa de diversos períodos según el tipo de datos que se hayan de suprimir (*Google*), hasta notables inconcreciones (*Apple*), pasando por plazos excesivos (*Twitter*). En algún caso se contempla el cobro de una tarifa por supresión de datos personales (*Youtube*) cuya validez podría cuestionarse según lo dispuesto en el art. 12.5 RGPD.

5. Un balance final

59. A modo de conclusiones, cabe recoger las siguientes ideas críticas: 1) La Directiva 2019/770 no contempla ni impide la posibilidad de extender los nuevos derechos (abstención de uso y recuperación) a otras causas de extinción del contrato de suministro de contenidos y servicios digitales, distintas de la resolución; los Estados Miembros en la transposición deberían plantearse esa opción y nada veda que tomen el modelo del RGPD, más proteccionista, en lugar del de la Directiva para los contenidos no personales. 2) Aunque no es aparente en el articulado de la Directiva, el derecho de recuperación durante la relación contractual, antes de operarse una resolución, podría quedar cubierto por las expectativas legítimas del consumidor *ex* art. 8.1.b DCSD. 3) El balance general que resulta de las facultades, excepciones y objeto sobre el que recaen los dos nuevos derechos de la Directiva en caso de resolución habla de un contenido prácticamente vacío, dado que además la Directiva tampoco se aplica cuando los datos personales facilitados por el consumidor fueran tratados exclusivamente por el empresario para suministrar los contenidos o servicios digitales o para cumplir requisitos legales (art. 3.1). 4) No obstante, debido al carácter expansivo del concepto de "dato personal" y a la remisión expresa de la Directiva (art. 16.2) al RGDP, el usuario puede encontrar en los derechos de supresión u olvido y portabilidad del Reglamento una herramienta de protección de sus intereses a la postre más eficaz que los recién estrenados derechos de una Directiva, por lo demás, pionera en la defensa contractual de los usuarios digitales.