Evolución del derecho a la protección de datos y disrupción tecnológica: ¿estamos vallando el campo?

Jesús María Simón Marco
Abogado sénior.
Asesoría Jurídica Internacional de Mapfre

Este trabajo ha sido seleccionado para su publicación por: don César Tolosa Tribiño, don Xabier Arzoz Santisteban, don José Luis López González, don Juan Francisco Mestre Delgado, don Ángel José Sánchez Navarro y don Daniel Sarmiento Ramírez-Escudero.

Extracto

El derecho a la protección de datos personales ha evolucionado rápidamente desde su inexistencia a la compleja regulación actual. No obstante, las nuevas tecnologías suponen un auténtico reto para que dicho derecho pueda ser realmente una realidad, ya sea por la dificultad de proteger toda la información en el entorno de internet o por directamente tratarse de tecnologías que chocan frontalmente contra sus principios, como puede ser el *blockchain* y el principio de inmutabilidad sobre el que se construye.

Palabras clave: disrupción; tecnología; avances.

Fecha de entrada: 03-05-2019 / Fecha de aceptación: 15-07-2019

Cómo citar: Simón Marco, J. M.ª (2020). Evolución del derecho a la protección de datos y disrupción tecnológica: ¿estamos vallando el campo? *Revista CEFLegal*, *233*, 89-120.

Technological disruption and evolution of the rights of data subjects: are we hedging the countryside?

Jesús María Simón Marco

Abstract

The rights of data subjects have evolved from its complete inexistence to its complex modern regulations. However, new technologies represent a real challenge for this rights to become a reality, either because of the difficulty of protecting all the information in the internet environment or because they are technologies that directly clash with its principles, such as the blockchain and the principle of immutability on which it is built.

Keywords: disruption; technology; progress.

Citation: Simón Marco, J. M.ª (2020). Evolución del derecho a la protección de datos y disrupción tecnológica: ¿estamos vallando el campo? *Revista CEFLegal*, *233*, 89-120.

Sumario

1. Evolución del derecho a la protección de datos personales

1.1. Origen del derecho: la privacidad

Cada vez es más frecuente encontrarse con personas que saben que tienen, además de otros muchos derechos, un derecho fundamental a la privacidad de sus datos personales plenamente ejercitable y respaldado por las leyes.

El derecho a la privacidad es consecuencia de la concepción moderna del individuo como sujeto de derechos y deberes. Sin embargo su implantación y desarrollo está ligado a la reciente necesidad de los individuos de protegerse contra injerencias de los medios de comunicación de masas en su esfera privada.

En los Estados Unidos se cita como precedente la publicación en 1890 en la *Harvard Law Review* de un artículo pergeñado por dos abogados estadounidenses que acuñaron por primera vez la expresión «*the rigth to privacy*»[1]. Warren y Brandeis (1890) partieron de la idea de que si el *common law* reconoce el derecho a la propiedad privada, de alguna manera debía poder proteger también la esfera privada de las personas frente a la publicación de artículos y fotografías de personas por parte de la prensa de la época[2].

De este genuino derecho a la privacidad se harán eco las declaraciones universales de derechos que surgen tras el fin de la Segunda Guerra Mundial[3].

---

1 *Vid*. en este sentido Warren y Brandeis (1890), considerado como el ensayo fundacional de la protección de la privacidad en los Estados Unidos. Sin embargo, en la concepción formulada en dicho ensayo no cabe reconocer todavía exclusivamente una dimensión individual o subjetiva del derecho, antes al contrario: la defensa de la privacidad se presenta en una dimensión colectiva y social que coadyuva al mantenimiento y avance del sistema democrático, pues, en última instancia, la privacidad contribuye a establecer los límites del control estatal sobre los individuos y a definir el atributo esencial de la ciudadanía.

2 *Ibid. in fine* «The common law has always recognized a man's house as his castle, impregnable, often, even to his own officers engaged in the execution of its command. Shall the courts thus close the front entrance to constituted authority, and open wide the back door to idle or prurient curiosity?».

3 Entre las cuales debemos citar la Declaración Universal de Derechos Humanos de 10 de diciembre de 1948 (art. 12) y el Pacto Internacional de Derechos Civiles y Políticos de 16 de diciembre de 1966 (art. 17).

Un poco después, en los años 70 del siglo pasado, aparecieron algunas empresas[4] que facilitaban la digitalización de documentos a sus clientes. Los datos digitalizados y almacenados en bases de datos podían consultarse y compartirse por los clientes con acceso.

Sin embargo, el paso siguiente a la mera digitalización de documentos en bases de datos privadas será la aparición del internet comercial a mitad de la década de los 90, acontecimiento que «democratizó» de manera radical el acceso de todos sus usuarios, mediante un mero clic, a cientos de datos personales de los demás.

Además, internet facilitará el envío de molesta publicidad masiva, así como la utilización y puesta en común entre empresas de todo tipo de ficheros con información personal, del cual serán paradigma los conocidos como «ficheros de morosos»[5].

1.2. Evolución legislativa

La evolución tecnológica será el acicate para el impulso de una legislación sobre la materia, hasta la fecha representada únicamente por acciones tímidas, como algunos trabajos aislados del Consejo de Europa en los años 60[6].

El cambio de régimen en algunos países propiciará el surgimiento de una normativa moderna en la materia, aprovechando la modificación o creación de sus sistemas constitucionales.

En España, la Constitución del 78, en su artículo 18.4, dispuso que: «La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos».

A nivel europeo, la firma del Convenio europeo para la protección de las personas con respecto al tratamiento automatizado de datos con carácter personal de 1981 dará una de-

---

4 Por ejemplo, LexisNexis, que fue pionera en la digitalización de noticias y precedentes judiciales.

5 Ficheros que han generado siempre una enorme polémica por los perjuicios que genera a los individuos el hecho de que dicha información se comparta por los agentes financieros, con mayor razón en el caso de que la información acerca del «moroso» se encuentre desactualizada.

6 Y algún legislador precoz, como el japonés. El régimen jurídico que rige la privacidad y la protección de datos en Japón tiene sus raíces en la Constitución de 1946, cuyo artículo 13 dispone que: «Todos los ciudadanos serán respetados como personas individuales. Su derecho a la vida, la libertad y al logro de la felicidad será, en tanto que no interfiera con el bienestar público, el objetivo supremo de la legislación y de los demás actos de Gobierno».

Sobre la base de dicho artículo, el Tribunal Supremo japonés ha precisado los derechos de las particulares en lo que respecta a la protección de la información personal. En una resolución de 1969, reconoció el derecho a la vida privada y a la protección de datos como un verdadero derecho constitucional.

finición de lo que ha de entenderse por dato personal, fijará unos principios básicos para la protección de datos y sentará unos principios para el flujo interno e internacional de datos.

No obstante lo señalado en nuestra Carta Magna, la primera norma que desarrollará la provisión del artículo 18 tardaría casi 14 años en publicarse: la Ley Orgánica 5/1992, de 29 de octubre, reguladora del tratamiento automatizado de datos personales, conocida como LORTAD.

La LORTAD presentaba en su haber dos aspectos abiertamente positivos: la definición de los principios básicos en materia de protección de datos[7] y el reconocimiento y tutela jurídica de la libertad informática; y un aspecto negativo: una pléyade de excepciones significativas al régimen general, que en la práctica matizaban indeseablemente el ejercicio de un verdadero derecho fundamental.

Por su parte, el Tribunal Constitucional –intérprete competencial máximo de la Constitución–- marcará un hito fundamental al reconocer *el derecho fundamental* a la protección de datos en la STC 94/1998, de 4 de mayo (NSJ003080), al señalar en su fundamento jurídico sexto que el artículo 18.4 de la Constitución:

> No solo entraña un específico instrumento de protección de los derechos del ciudadano frente al uso torticero de la tecnología informática, sino que consagra un derecho fundamental autónomo a controlar el flujo de informaciones que conciernen a cada persona […], pertenezcan o no al ámbito más estricto de la intimidad, para así preservar el pleno ejercicio de sus derechos.

La publicación de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante, la Directiva) obligará a los Estados miembros a desarrollar una legislación interna mucho más compleja y completa en materia de protección de datos, más acorde con el desarrollo de la informática e internet que se venía produciendo desde los principios de la década de los noventa. En España la trasposición se llevó a cabo mediante la aprobación de la Ley Orgánica 15/1999, del 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD).

La LOPD, y su posterior reglamento de desarrollo, constituyen ya una regulación bastante completa de la materia. La LOPD establece con mayor precisión el concepto de dato personal, cuáles son los derechos básicos de los ciudadanos frente a los tratamientos de sus datos personales (los conocidos coloquialmente como derechos ARCO)[8], el principio general

[7] Partiendo del principio cardinal según el cual debe existir una congruencia y la racionalidad en la utilización de los datos personales, en cuya virtud ha de mediar una nítida conexión entre la información personal que se recaba y trata informáticamente y el legítimo objetivo para el que se solicita.

[8] Acrónimo de los derechos de acceso, rectificación, cancelación y oposición al tratamiento.

de prestación del consentimiento para la realización de tratamientos de datos, la figura del responsable del tratamiento como centro de imputación de obligaciones, la del encargado como auxiliar necesario del responsable del tratamiento en el tráfico de datos en las relaciones institucionales y empresariales, la creación y mantenimiento de ficheros de titularidad pública y privada, las transferencias internacionales de datos y el régimen de la Agencia Española de Protección de Datos (AEPD). Todas estas novedades se complementan además en la LOPD con el establecimiento de un régimen sancionador que prevé elevadas cuantías económicas para los infractores, hecho que situará a una normativa hasta entonces medio desconocida por el público en general en una cuestión de rabiosa actualidad para muchas empresas y ciudadanos, que tuvieron que adaptar sus procedimientos para evitar sus temidas consecuencias.

Recién publicada la LOPD, el Tribunal Constitucional dio un espaldarazo definitivo al derecho fundamental a la protección de datos cuando resolvió favorablemente un recurso de inconstitucionalidad interpuesto por el Defensor del Pueblo contra los artículos 21.1 («Comunicación de datos entre Administraciones Públicas») y 24.1 y 2 («Otras excepciones a los derechos de los afectados») de la LOPD por vulneración de los artículos 18.1 y 4 y 53.1 de la CE.

El Tribunal Constitucional entendió que el artículo 21.1 vulneraba la Constitución porque permitía (como excepción a la regla de la necesidad del consentimiento del afectado del artículo 11 de la LOPD) que mediante una *disposición reglamentaria* se exceptuase la necesidad de obtener el consentimiento del titular afectado, excepción que el Tribunal Constitucional entendió que solo podía establecer una norma con rango ley.

Por su parte los apartados 1 y 2 del artículo 24 eximían a la Administración de cumplir con las obligaciones de información y advertencia a los interesados a las que se refiere el artículo 5.1 y 2 de la LOPD si tal cosa pudiere impedir o dificultar gravemente las funciones de control y verificación de las Administraciones públicas o cuando afectase a la persecución de infracciones administrativas. Dichas disposiciones también fueron declaradas inconstitucionales.

Pero lo más relevante de la Sentencia 292/2000, de 30 de noviembre (NCJ051718) fue que el Tribunal Constitucional aprovechó para pronunciarse claramente sobre el derecho fundamental a la protección de datos y deslindarlo del derecho a la intimidad, al señalar en sus fundamentos 5.º y 6.º:

> Este derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad del art. 18.1 CE, con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar, *atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley*, aquella que conforme al art. 18.4 CE debe limitar el uso de la informática, bien desarrollando el derecho fundamental a la protección de datos (art. 81.1 CE), bien regulando su ejercicio (art. 53.1 CE). La peculiaridad de

> este derecho fundamental a la protección de datos respecto de aquel derecho fundamental tan afín como es el de la intimidad radica, pues, en su distinta función, lo que apareja, por consiguiente, que también su objeto y contenido difieran.
>
> […] La función del derecho fundamental a la intimidad del art. 18.1 CE es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad (por todas STC 144/1999, de 22 de julio [NFJ068939], FJ 8). En cambio, *el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado*.

2. El régimen legal del derecho a la protección de datos en la actualidad

Desde 1999 la revolución tecnológica no ha cesado. Internet ha pasado de ser anecdótico a ser la realidad cotidiana de muchísimas personas. Los gigantes de las redes sociales, de telefonía, los buscadores de información y las grandes empresas de distribución han puesto a la orden del día la importancia de contar con enormes bases de datos sobre el comportamiento de las personas. Incluso se ha modificado en muy pocos años la manera en la que las personas se comunican unas con otras.

Esta nueva realidad ha obligado al legislador a hacerse eco de nuevas amenazas y necesidades del derecho a la protección de los datos personales.

En la Unión Europea la legislación anterior ha sido modificada con la entrada en vigor en mayo de 2018 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (conocido coloquialmente como el Reglamento General de Protección de Datos o RGPD).

El Reglamento General de Protección de Datos es una norma directamente aplicable a todos los países de la Unión Europea. Supone, frente al régimen anterior, un avance claro hacia la homogeneización a nivel europeo, puesto que no requiere que los Estados miembros aprueben normas de trasposición ni precisa, en principio, de detalladas normas de desarrollo o aplicación, como sí sucedía en el caso de la Directiva, a la que deroga.

Bajo la Directiva, existían divergencias en la ejecución y aplicación de la misma que podían provocar un distinto nivel de protección en los Estados miembros. Estas diferencias podían constituir, por lo tanto, un obstáculo al ejercicio de las actividades económicas a nivel de la Unión, falsear la competencia e impedir que las autoridades cumplan las funciones que les incumben en virtud del Derecho de la Unión.

Además de lograr la homogeneización de la regulación aplicable entre los países miembros, el RGPD ha aprovechado para introducir toda una serie de novedades entre las que destacamos:

a) **Ámbito de aplicación.**

El RGPD amplía el ámbito de aplicación territorial a los responsables y a los encargados del tratamiento no establecidos en la Unión Europea cuando las actividades de tratamiento estén relacionadas con la oferta de bienes o servicios o con el control del comportamiento de las personas que se encuentran en la Unión[9].

b) **Delegado de protección de datos (DPD).**

Una de las novedades estrella del RGPD es la creación de la figura del delegado de protección de datos, nuevo cargo que debe formar parte de la plantilla del responsable o del encargado del tratamiento o bien actuar en el marco de un contrato de servicios suscrito con cualquiera de ellos[10].

El delegado de protección de datos tiene, como principales funciones la de: a) informar y asesorar al responsable o al encargado del tratamiento y a los trabajadores sobre las obligaciones que impone la normativa de protección de datos; b) supervisar el cumplimiento de la normativa; c) asesorar en relación con la evaluación de impacto relativa a la protección de datos; d) cooperar con la AEPD, y e) actuar como punto de contacto para cuestiones relativas al tratamiento.

El delegado actuará siempre con plena autonomía en el ejercicio de sus funciones y el responsable o el encargado del tratamiento deberán facilitarle todos los recursos que precise para el ejercicio de su cargo.

c) **Principios.**

El RGPD incorpora los principios de «responsabilidad proactiva» y «enfoque de riesgo», que obligan a los responsables del tratamiento a llevar a cabo una labor activa en el cumplimiento de sus obligaciones.

---

9 El propósito de esta medida es la de evitar que compañías establecidas fuera de la UE y que estén realizando tratamiento de datos personales de residentes en la Unión queden fuera del marco regulador del RGPD.

10 Será necesario designar un delegado de protección de datos en los casos siguientes:

- Cuando el tratamiento lo lleve a cabo una autoridad o un organismo público (excepto juzgados y tribunales). En este caso, se puede designar un único delegado de protección de datos para diversas de estas autoridades u organismos.
- Cuando el tratamiento requiere la observación habitual y sistemática de personas interesadas a gran escala.
- Cuándo el tratamiento tiene por objeto categorías especiales de datos personales o datos relativos a condenas o infracciones penales.

d) **Nuevas categorías especiales de datos.**

Se introducen, además de los ya existentes bajo la Directiva, las siguientes nuevas categorías de datos: genéticos[11] y biométricos[12].

e) **Consentimiento.**

En esta materia se introduce una notabilísima novedad que es la de que el RGPD requiere que la persona interesada preste el consentimiento mediante una declaración inequívoca o una acción afirmativa clara. *A los efectos del RGPD, la utilización de casillas para prestación del consentimiento ya marcadas, el consentimiento tácito o la inacción no constituyen un consentimiento válido*.

El RGPD contempla algunas situaciones en las que el consentimiento ha de ser explícito.

f) **Derechos de las personas interesadas.**

El RGPD incorpora el derecho al olvido como un derecho vinculado al derecho de supresión, al derecho a la limitación del tratamiento y al derecho a la portabilidad.

g) **Medidas de seguridad.**

En el régimen anterior se establecían una serie de medidas de seguridad que debían aplicarse en función de los distintos tipos de datos que fueran objeto de tratamiento (de contacto, información bancaria, salud, etc.). Pues bien, ahora el RGPD, de acuerdo con el nuevo principio de «responsabilidad proactiva», obliga a que sean el responsable y el encargado del tratamiento quienes decidan, tras realizar la correspondiente evaluación de los riesgos asociados a cada tratamiento, las medidas técnicas y organizativas adecuadas de conformidad con el riesgo que conlleve el tratamiento[13].

---

11 Aquellos datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionan una información única sobre la fisiología o la salud de esta persona, obtenidas en particular del análisis de una muestra biológica.

12 Aquellos datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física, que permiten o confirman la identificación única de esta persona (imágenes faciales, datos dactiloscópicos, etc.).

13 En las grandes organizaciones, como norma general, este análisis de riesgos y la determinación de las medidas/controles a implantar puede llevarse a cabo utilizando alguna de las metodologías o estándares de análisis de riesgo existentes: Magerit, ISO, etc. En organizaciones de menores dimensiones que lleven a cabo tratamientos de poca complejidad, este análisis puede ser el resultado de una reflexión documentada sobre las implicaciones de los tratamientos en los derechos y las libertades de las personas interesadas. Esta reflexión debe analizarse en el contexto en que se lleva a cabo el tratamiento (medios, instalaciones, usuarios etc.) y tiene que dar respuesta a una serie de cuestiones básicas relativas al tipo de datos, su utilización y amenazas plausibles.

Son muchas las cuestiones que pueden impactar de forma negativa en los derechos y libertades de las personas si se tratan inadecuadamente los datos. Por lo tanto, es muy importante que, si no se

h) **Notificación de violaciones de seguridad**.

Otra de las novedades estrella del RGPD. No nos detendremos mucho porque nos referiremos a ella en el apartado relativo a la ciberseguridad.

i) **Inscripción y notificación de ficheros**.

El RGPD ha suprimido la necesidad de crear formalmente los ficheros y notificarlos a los respectivos registros de protección de datos de las autoridades de control (*i. e.* AEPD).

j) **Encargo del tratamiento**.

El RGPD amplía el contenido mínimo del contrato de encargo de tratamiento entre responsable y encargado, a la par que establece algunas obligaciones específicas para los encargados del tratamiento que no se circunscriben al ámbito del contrato que los vincula al responsable y que las autoridades de protección de datos tienen que supervisar separadamente. Por ejemplo, los encargados tienen que mantener un registro de actividades de tratamiento.

k) **Mecanismos de certificación**.

El reglamento promueve los mecanismos de certificación como instrumentos útiles para demostrar el grado de cumplimiento de la normativa.

l) **Consentimiento de los menores**.

De acuerdo con el RGPD, en el ámbito de los servicios de la sociedad de la información (principalmente las operaciones realizadas a través de internet), el consentimiento de los menores solo es válido si tienen más de 16 años. No obstante, se permite que los Estados miembros de la Unión Europea rebajen la edad hasta los 13 años. En España se ha fijado esta edad en los 14 años, pero no solo en el ámbito de los servicios de la sociedad de la información, sino para cualquier tratamiento de datos de menores, excepto que una norma con rango de ley exija la asistencia de los titulares de la potestad parental o tutela.

m) **Documentación de las operaciones de tratamiento: registro de actividades de tratamiento.**

Los responsables y encargados del tratamiento tienen que llevar un registro de las actividades de tratamiento que lleven a cabo. Este registro debe contener, respecto de cada actividad, la información que establece el artículo 30 del RGPD.

---

utiliza una metodología estándar, fácilmente auditable y objetivable, se documenten detalladamente las cuestiones que se han tenido en cuenta a la hora de determinar el nivel de riesgo existente y concretar las medidas de seguridad que hay que aplicar. Eso nos servirá para cumplir con el principio de responsabilidad proactiva.

n) **Derecho de información**.

El reglamento configura la información como un derecho de las personas afectadas y amplía las cuestiones sobre las que es necesario informarlas.

o) **Ventanilla única**.

Este sistema permite ahora que los ciudadanos y también los responsables establecidos en diferentes Estados miembros o que hagan tratamientos que afecten a diferentes Estados miembros tengan como interlocutora una única autoridad de protección de datos.

p) **Régimen sancionador.**

La Directiva permitía a los Estados miembros[14] decidir acerca del régimen de sanciones que debía aplicarse en caso de incumplimiento[15]. Cada Estado miembro procedió a establecer un régimen sancionador diferente[16]. El RGPD ha dado un paso de gigante en esta materia y ha establecido un régimen sancionador muy gravoso en el que, como en la normativa de derecho de la competencia, se tiene en cuenta el volumen de facturación de las empresas que infringen la normativa de protección de datos.

Destacaremos aquí que las sanciones por conductas graves pueden llegar a ser de hasta 10 millones de euros o un 2 % del volumen de negocio del ejercicio anterior (la que sea mayor) y, para los casos muy graves, de hasta 20 millones de euros o un 4 % del volumen de negocio del ejercicio anterior (la que sea mayor).

Sin perjuicio de que el RGPD es directamente aplicable a todos los Estados miembros, España aprovechó para aprobar la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y garantía de los derechos digitales (LOPDGDD), que no solo ha adaptado el ordenamiento jurídico nacional al RGPD, sino que también ha introducido aclaraciones con vocación de servir de ayuda a responsables y encargados de tratamiento a la hora de llevar a cabo operaciones de tratamiento con mayor seguridad jurídica. A su vez la LOPDGDD

14 Lo que en la práctica podía significar que las empresas pudiesen llevar sus tratamientos de datos a Estados miembros con un régimen sancionador más laxo, en una suerte de «data forum shopping».

15 Decía su artículo 24 que: «Los Estados miembros adoptarán las medidas adecuadas para garantizar la plena aplicación de las disposiciones de la presente Directiva y determinarán, en particular, las sanciones que deben aplicarse en caso de incumplimiento de las disposiciones adoptadas en ejecución de la presente Directiva».

16 En el caso español el sistema era gradual de sanciones leves, graves y muy graves, con infracciones que podían alcanzar, en los casos más graves, la imposición de multas de hasta 600.000 euros (régimen que se matizó por la Ley 2/2011, de 4 de marzo, de Economía Sostenible). El sistema italiano podía alcanzar sanciones de hasta 300.000 euros, pero podía duplicar o cuadruplicar esta cantidad en el caso de que concurriesen ciertas circunstancias, estableciéndose además incluso responsabilidad penal y penas de privación de libertad en algunos supuestos. En el Reino Unido el Data Protection Act de 1998 preveía sanciones de hasta 500.000 libras esterlinas.

ha aprovechado para incorporar, entendemos que por su cercanía con la materia que nos ocupa, 17 nuevos «derechos digitales» con el objetivo de dar respuesta a cuestiones derivadas de la incorporación de las nuevas tecnologías en el día a día de los ciudadanos[17].

Como señala Barrio (2018), toda esta regulación presenta defectos, insuficiencias y algunos contenidos son una mera reiteración de otros mandatos ya en vigor en diferentes normas del ordenamiento jurídico. También a veces reconoce derechos inespecíficos o normas promocionales o programáticas, que no cuentan con garantías precisas para su cumplimiento (para. 9).

Ejemplo de esto último es el derecho a la portabilidad en las redes sociales al que se refiere el artículo 95. Este derecho permite, siempre que sea técnicamente posible, que los usuarios tengan derecho a recibir y transmitir los contenidos que hubieran facilitado a una red social a otra plataforma. Sin embargo, en la práctica este derecho solo será posible en la medida en la que los usuarios dispongan de los contenidos que hayan facilitado a dicha red social, de acuerdo con las normas de participación en las mismas (*i. e.* pueden haber renunciado previamente a este derecho[18], etc.).

Mayor problemática plantean ciertos derechos directamente relacionados con la protección de datos: el derecho de rectificación y actualización de informaciones en medios digitales en internet (arts. 85 y 86) y el derecho al olvido en internet (arts. 95 y 96).

Entendemos aquí que merecen una reflexión más detallada por la problemática que plantean: aunque su nacimiento viene propiciado por el protagonismo indiscutible de internet en la sociedad actual, su cumplimiento se plantea un tanto difícil en el entorno difuso de internet; y, por el otro, son susceptibles de colisionar con el derecho fundamental a la información.

3. El derecho al olvido en el nuevo entorno tecnológico

3.1. Concepto

A pesar de que el término ha sido acuñado de esa manera, más que del «derecho al olvido» deberíamos de hablar del «derecho a ser olvidado» es decir: el derecho a que un dato o contenido relativo a una persona deje de ser asequible para terceras personas en internet.

---

17 En este sentido la norma reconoce el derecho a acceder a internet, a la seguridad digital, al denominado testamento digital (acceso al contenido digital de una persona una vez fallecida), el derecho a la educación digital, el derecho a la intimidad y uso de dispositivos digitales en el entorno laboral, el de desconexión digital, los derechos en relación con la videovigilancia, etc.

18 Siempre y cuando claro está, la renuncia sea válida y no contraríe el interés o el orden público ni perjudique a terceros.

La AEPD atina al definirlo como aquel derecho que tiene un ciudadano a impedir la difusión de información personal a través de internet cuando su publicación no cumple con los requisitos de adecuación y pertinencia previstos en la normativa.

Ningún sentido tendría que los particulares pudiesen ejercitar sus derechos ante las empresas e instituciones responsables del tratamiento de sus datos si luego estos permanecieran reproducidos en sitios web *sine die*, accesibles a cualquier persona.

El derecho al olvido no es más que una extensión de los tradicionales derechos a la rectificación, oposición y cancelación de datos personales con la diferencia de que, mientras que los primeros se ejercitan ante un responsable del tratamiento en particular, el derecho al olvido pretende lo mismo en relación con la información o perfil que de una persona se haya podido elaborar y sea susceptible de ser encontrado en internet. Pongamos un ejemplo claro: una persona podría solicitar la rectificación o cancelación de sus datos personales que apareciesen en una web concreta. Sin embargo, todas las reproducciones, *links* y contenidos de la misma que hayan podido reproducirse en otros entornos de internet quedarían al margen del ejercicio de ese derecho frente al responsable, y la finalidad de dicho ejercicio quedaría del todo frustrada.

El derecho al olvido no puede ejercitarse al mero arbitrio de cualquier particular: requiere que concurran los presupuestos legales para su ejercicio. De otra manera se imposibilitaría el derecho a la información y a la libertad de prensa, derechos fundamentales con los que siempre está en riesgo de colisionar[19].

Su primera formulación fue jurisprudencial. El caso paradigmático, la sentencia del caso Google. Merece la pena que nos detengamos a analizar este caso porque ha sentado las bases de su ejercicio.

3.2. La sentencia Google

Antes del RDPG el derecho al olvido era un derecho que no tenía un claro reconocimiento legal, pero que se desprendía del espíritu y finalidad de la normativa.

---

[19] Al que se refiere el artículo 20 de la CE:

> Se reconocen y protegen los derechos:
>
> a) *A expresar y difundir libremente los pensamientos, ideas y opiniones* mediante la palabra, el escrito o cualquier otro medio de reproducción.
>
> […]
>
> d) *A comunicar o recibir libremente información veraz por cualquier medio de difusión*. La ley regulará el derecho a la cláusula de conciencia y al secreto profesional en el ejercicio de estas libertades.

El 13 de mayo de 2014, el Tribunal de Justicia de la Unión Europea (TJUE) dictó una importantísima sentencia contra el buscador de internet Google en materia de protección de datos personales (en adelante, la Sentencia)[20].

El proceso tuvo su origen en la reclamación planteada por D. Mario Costeja Fernández ante la AEPD contra La Vanguardia Ediciones, SL, Google Spain y Google Inc. En dicha reclamación el Sr. Costeja pretendía la eliminación de cierta información sobre un embargo contra su persona acaecido en 1998, información que había quedado absolutamente desactualizada en la fecha de la reclamación. En efecto, cuando introducía sus datos en el motor de búsqueda de Google, el resultado que obtenía se vinculaba a dos páginas del periódico *La Vanguardia*, del 19 de enero y del 9 de marzo de 1998, en las que aparecía un anuncio de una subasta de inmuebles a causa de un embargo por deudas a la Seguridad Social.

Mediante esta reclamación, el Sr. Costeja González solicitaba a la AEPD que:

- Obligase a La Vanguardia a eliminar o modificar su publicación para que no apareciesen sus datos personales.
- Obligase a Google Spain o a Google Inc. a que eliminasen u ocultasen sus datos para que dejasen de estar ligados a los enlaces de La Vanguardia.

La AEPD entendió que la reclamación contra La Vanguardia no procedía puesto que la publicación había tenido lugar por orden del Ministerio de Trabajo y Asuntos Sociales y tenía por objeto dar la máxima publicidad a la subasta para conseguir la mayor concurrencia de licitadores. Sin embargo, en los casos de Google Spain y Google Inc. el desenlace fue distinto: ordenó la eliminación en sus buscadores de la información desactualizada acerca del Sr. Costeja. La AEPD consideró que quienes gestionan motores de búsqueda están sometidos a la normativa en materia de protección de datos, dado que llevan a cabo un tratamiento de datos del que son responsables y actúan como intermediarios de la sociedad de la información.

Google Spain y Google Inc. interpusieron sendos recursos contra dicha resolución ante la Audiencia Nacional, que decidió acumularlos y plantear una cuestión prejudicial al Tribunal de Justicia europeo.

No interesan aquí las cuestiones que se dilucidaron acerca de la aplicación de la Directiva a un responsable situado fuera de la Unión Europea (Google Inc.), puesto que además es una cuestión que ha resuelto ya el RGPD al establecer su ámbito de aplicación[21].

[20] STJUE (Gran Sala) de 13 mayo de 2014. TJCE 2014\85 (NCJ058436).

[21] En el caso de esta sentencia el TJUE entendió que sí resultaba aplicable la Directiva.

Sin embargo, la segunda parte de la Sentencia resuelve precisamente la cuestión de si la actividad de los buscadores como proveedores de contenidos[22] supone un «tratamiento de datos» a los efectos de la Directiva, y también la de si el interesado puede tener derecho a ejercitar sus derechos ante el buscador.

El TJUE resolvió en favor del Sr. Costeja al entender:

- Que el gestor de un motor de búsqueda debe considerarse «responsable» de dicho tratamiento, en el sentido de la Directiva.
- Que debe distinguirse en este terreno la responsabilidad del motor de búsqueda de la del editor de un contenido en una web. Mientras que el primero puede verse obligado a retirar la «indexación» de búsquedas, el segundo puede tener un interés legítimo en que la publicación se mantenga al amparo de otro derecho fundamental (*i. e.* derecho de información y libertad de prensa)[23].
- Que los interesados deben poder ejercitar sus derechos cuando los datos sean inexactos, inadecuados, no pertinentes y excesivos en relación con los fines del tratamiento, no estén actualizados o se conserven durante un período superior al necesario, a menos que se imponga su conservación por fines históricos, estadísticos o científicos.

No obstante el TJUE entendió que en estos casos se debe evaluar primero si concurren los requisitos necesarios para que el derecho al olvido pueda reconocerse y posteriormente sopesar si debe prevalecer sobre el derecho a la información. En efecto, la supresión de vínculos de la lista de resultados de un buscador podría, en función de la información de que se trate, tener repercusiones en el interés legítimo de los internautas potencialmente interesados en tener acceso a la información en cuestión.

Por lo tanto resulta preciso buscar, en dichas situaciones, un justo equilibrio. Para ello se debe atender a la naturaleza de la información de que se trate y al carácter más o menos sensible que tenga para la vida privada de la persona afectada, y sopesar el interés del público en disponer de esta información, que puede variar, en particular, en función del papel que esta persona desempeñe en la vida pública.

---

22 En concreto, actividad que consiste en localizar la información publicada o incluida en la red por terceros, indexarla de forma automática, almacenarla temporalmente y finalmente ponerla a disposición de los internautas con un cierto orden de preferencia, cuando dicha información contenga datos personales de terceras personas.

23 El tratamiento por parte del editor de una página web, que consiste en la publicación de información relativa a una persona física, puede, en su caso, efectuarse con fines exclusivamente «periodísticos» y beneficiarse, de este modo, en virtud del artículo 9 de la Directiva, de las excepciones a los requisitos que esta establece, mientras que ese no es el caso en el supuesto del tratamiento que lleva a cabo el gestor de un motor de búsqueda.

En este sentido el TJUE en la Sentencia de 24 septiembre de 2019, C-136/2017 resuelve un caso en el que los interesados ven desestimadas sus solicitudes dirigidas a Google para la retirada de varios enlaces que dirigían a páginas web publicadas por terceros, en las que se incluían datos personales especialmente protegidos.

El Tribunal de Justicia europeo recuerda que en estos casos debe tenerse en cuenta la gravedad de la injerencia en los derechos fundamentales del interesado y ponderar si la inclusión de dichos enlaces resulta estrictamente necesaria para proteger la libertad de información de los internautas potencialmente interesados en acceder a dicho contenido.

En dicha sentencia el TJUE entiende además que para poder conciliar el derecho a la libertad de información de los internautas con los derechos fundamentales de una persona cuyos datos personales salen como resultado de búsquedas en internet, el gestor de un motor de búsqueda debe estimar la solicitud de retirada de enlaces que dirigen a páginas web en las que figuran datos personales referidos a procedimientos judiciales *cuando los datos se refieran a una etapa anterior del procedimiento judicial, de forma que ya no se ajusten a la situación actual*.

Como colofón, el Tribunal europeo declara que aunque *a priori* los derechos del interesado prevalecen sobre la libertad de información de los internautas, debe valorarse siempre, y caso por caso, la naturaleza de la información, el carácter sensible de esta para la vida privada del interesado y el interés público de los internautas en disponer de la información.

3.3. El derecho al olvido en registros públicos

Tres años después de la sentencia del caso Google, el TJUE[24] tuvo ocasión de matizar el alcance del derecho al olvido en el caso de que se pretenda ejercitar contra datos personales que aparecen en el Registro Mercantil.

El origen de la cuestión era la pretensión de un ciudadano italiano de que la Cámara de Comercio de Lecce hiciera anónimos los datos que le vinculaban con un procedimiento concursal de una sociedad en la que se había visto involucrado años atrás como liquidador. El interesado argumentaba que había transcurrido un tiempo suficiente como para que no existiese interés en mantener dicha información accesible al público y que dicha información estaba perjudicando su reputación de cara a futuras operaciones mercantiles.

Los tribunales italianos plantearon la cuestión prejudicial ante el TJUE acerca de si los datos personales que figuran en los registros de sociedades deben estar disponibles de forma ilimitada para destinatarios indeterminados o si, por el contrario, el acceso a los mis-

[24] STJUE (Sala Segunda) de 9 marzo de 2017. TJCE 2017\76.

mos debe limitarse en el tiempo, restringirse a determinadas personas según cada caso o incluso eliminarse según los criterios del responsable de los datos.

El TJUE entendió que debía realizarse una ponderación entre el derecho al respeto de la vida privada manifestado en limitar el acceso a los datos personales contenidos en los registros de sociedades y el derecho de publicidad e información que tienen los operadores en el mercado.

En este sentido, señaló el TJUE que la publicidad de los registros de sociedades tiene por objeto garantizar la seguridad jurídica en las relaciones entre las sociedades y los terceros y proteger, en particular, los intereses de los terceros en relación con las sociedades anónimas y las sociedades de responsabilidad limitada, ya que dichas sociedades solo ofrecen su patrimonio social como garantía respecto a ellos. El TJUE observó que pueden producirse situaciones en las que se necesita disponer de datos personales recogidos en el registro de sociedades, incluso muchos años después de la situación que generó su inscripción (*i. e.* liquidación de una empresa), dado que existen multitud de derechos y relaciones jurídicas que pueden vincular a una sociedad con distintos actores en varios Estados miembros. Asimismo existe una auténtica heterogeneidad en los plazos de prescripción previstos por las diferentes normativas de los Estados miembros, por lo que resulta imposible identificar un plazo único desde el cual la inscripción de estos datos en el registro y su publicidad ya no sea necesaria.

Ponderando este derecho a la publicidad e información de terceros con el derecho a la protección de datos personales, el TJUE consideró que debe prevalecer la necesidad de proteger los intereses de terceros en relación con las sociedades mercantiles y garantizarse la seguridad jurídica y la lealtad de las transacciones comerciales.

No obstante, resulta interesante destacar que el propio TJUE dejó abierta la posibilidad de que los Estados miembros puedan limitar la publicidad de los datos que consten en los registros mercantiles una vez que transcurra un plazo suficientemente largo y cuando existan razones excepcionales y justificadas que así lo aconsejen.

3.4. El ejercicio del derecho al olvido

Hemos visto como se ha ido construyendo el derecho al olvido en la jurisprudencia del TJUE. El vigente artículo 17 del RGPD ya lo ha incorporado y lo reconoce como un derecho específico y autónomo, a la par que establece unas pautas para su ejercicio. Toda aquella persona que pretenda ejercitar su derecho al olvido deberá justificar ante el responsable del tratamiento que concurre alguna de las circunstancias siguientes:

a) Los datos personales ya no son necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo.

b) El tratamiento no se base en otro fundamento jurídico.

c) El interesado se oponga al tratamiento y no prevalezcan otros motivos legítimos para el tratamiento.

d) Los datos personales hayan sido tratados ilícitamente.

e) Los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento.

f) Los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1.

El responsable del tratamiento podrá denegar el ejercicio del derecho cuando el tratamiento resulte necesario para: ejercer el derecho a la libertad de expresión e información; cumplir con alguna obligación legal que requiera dicho tratamiento; cumplir una misión realizada en interés público; el interés público o en el ámbito de la salud; fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos; o para la formulación, el ejercicio o la defensa de reclamaciones.

Como consecuencia de la sentencia Google, el buscador habilitó un formulario en el que los interesados pueden exponer las razones para el ejercicio de su derecho al olvido, y el buscador atenderla cuando concurran causas justificadas[25].

El propio formulario señala que a la hora de estudiar la reclamación se buscará un equilibrio entre los derechos a la privacidad de los usuarios afectados, el interés público que pueda tener esa información y el derecho de otros usuarios a distribuirla[26].

En caso de que Google no diera respuesta a una reclamación o fuera denegada, los interesados pueden interponer una reclamación ante la AEPD para que resuelva. Esta decisión será recurrible ante los tribunales.

Llegados a este punto hemos señalado que el derecho al olvido no es infalible y que su ejercicio puede verse constreñido en la práctica por la existencia de otros derechos fundamentales. Existen voces contrarias al mismo que entienden que el que lo ejercita (piénsese en el caso de políticos en casos de corrupción) se olvida en ocasiones de que la reputación no es exactamente algo que le pertenece. La reputación no deja de ser el conglomerado de

[25] Puede consultarse el formulario en el siguiente enlace: <https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf&visit_id=636856772235123441-2995422405&rd=1>.

[26] Y, en previsión ante la avalancha de ejercicio del derecho en casos de personas implicadas en casos de corrupción, Google ya adelanta que «es posible que rechacemos retirar cierta información sobre estafas financieras, negligencias profesionales, condenas penales o conductas de funcionarios».

cosas que la gente piensa de una persona y no se puede proceder a borrar el cerebro de las personas de la noche a la mañana. En este sentido, no debe olvidarse, como muchos asesores de imagen bien saben, que en ocasiones puede ser más útil para cualquier persona hacer pública una rectificación de sus palabras o acciones antes que proceder, bajo la mayor de las sospechas posibles, a borrar su historial online bajo la atenta mirada de los internautas. En cualquier caso, cuando se decida su ejercicio deberán cumplirse las condiciones y requisitos mencionados anteriormente.

4. La tecnología *blockchain* y la protección de datos

4.1. ¿Qué es *blockchain*?

La tecnología *blockchain* está en boga. Se trata de una nueva disrupción tecnológica que ha sido calificada por algunos como una nueva revolución industrial[27]. Su afianzamiento plantea interesantes retos al derecho a la protección de datos personales.

A pesar de la sofisticación que el empleo de todo anglicismo sugiere, la idea de la tecnología blockchain es teóricamente tan simple como la crear una base de datos descentralizada, distribuida y enlazada mediante una serie de cadenas que unen bloques.

Apuntaremos que no existe una sola red blockchain, sino tantas como decidan crearse. Además las redes de este tipo pueden ser públicas o privadas en función de quiénes puedan participar en las mismas, hecho al que posteriormente haremos referencia por sus implicaciones en materia de protección de datos.

Una red blockchain funciona en la mayoría de los casos de la siguiente manera: cada uno de sus usuarios participantes en la misma cuenta con una clave pública (un código alfanumérico) que le identifica ante los demás usuarios. Esta clave pública se encuentra correlacionada matemáticamente con una clave privada, conocida únicamente por el usuario, que le permite revelar todos aquellos datos que se encuentran encriptados bajo su clave pública. De esta manera los usuarios actúan en blockchain en principio anónimamente, salvo que existan otros elementos que les permitan identificarse (por ejemplo, en el caso en el que se revelasen las claves).

Mediante la utilización de estas claves se producen intercambios. El objeto del intercambio puede ser de muy variada naturaleza. En la fecha de realización de este trabajo el

[27] Calificación que casi resulta un mantra para los numerosos defensores de esta tecnología. Entre otros podemos citar a Pollock (2018).

principal intercambio que se produce en las redes existentes a nivel mundial es el de las polémicas criptomonedas[28].

Sin embargo, en un futuro próximo los intercambios que se producirán en este tipo de redes apuntan a dar ambiciosas soluciones a problemas de la vida real: una red blockchain puede documentar verdaderos contratos inteligentes con cláusulas autoejecutables y verificables por todos sus participantes[29], utilizarse para habilitar un sistema de votación fiable, emplearse para realizar todo tipo de intercambios financieros o utilizarse para crear y documentar registros de todo tipo (civil, de la propiedad, de propiedad intelectual etc.).

Sea como fuere, toda la información que se intercambia en una red blockchain por sus participantes es almacenada en bloques de datos enlazados, como una cadena, que se encriptan para que no puedan ser modificados ni alterados en el futuro de ningún modo[30]. Los bloques se ordenan de forma cronológica. Cada bloque se une al siguiente bloque formando una cadena gracias a que cuenta con un guarismo (denominado hash)[31] del bloque que le precede. Esta característica impide que un bloque que tuviese hash erróneo pudiera introducirse violentamente en la cadena y ser replicado. Para verificar las operaciones los

---

28 De carácter y naturaleza jurídica controvertida (se ha dicho que son un medio de pago, títulos valores, dinero digital o bienes muebles digitales, entre otras muchas cosas), las criptomonedas se intercambian en las redes blockchain entre sus usuarios que pueden verificar, en todo momento, la fecha y valor efectivamente transmitido en cada transacción. Plantea interesantes problemas de tributación, como recientemente ha señalado en un magnífico estudio González de Frutos (2018).

29 La idea de un contrato inteligente no es ni mucho menos nueva, pero la tecnología blockchain supone un avance que posibilita que pase del mundo de las ideas a la realidad cotidiana. Ya aventuró esta posibilidad en un interesante estudio Szabo (1997).

Hoy día ya con esta tecnología de cuerpo presente existen interesantísimos estudios, entre los que citamos el de Werbach y Cornell (2017), o el también interesante desarrollado por Kaulartz y Heckmann (2016).

30 En realidad sí puede modificarse, lo único que dicha modificación entrañaría la dificultad de ser consensuada por la mayoría simultánea de los nodos de la red, hecho que en la práctica dificulta muchísimo cualquier alteración. En el caso de las redes abiertas, alcanzar un consenso para producir una alteración será muchísimo más difícil que en una red privada en la que los participantes se conozcan y puedan llegar a este tipo de arreglos. Por otro lado, no son ajenas a los piratas informáticos, conocidos como *hackers*, como se demostró en múltiples ciberataques que se han producido hasta la fecha a las distintas redes con el objetivo de robar criptomonedas. Piénsese que en el futuro estos mismos *hackers* tendrán incentivos para sustraer cualquier tipo de información interesante que sea susceptible de ser transmitida a través de una red blockchain.

31 Un hash es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. Independientemente de la longitud de los datos de entrada, el valor hash de salida tendrá siempre la misma longitud. Este tipo de función hash no puede ser revertida (como sí sucede con la técnica de encriptación) para obtener información acerca de la fuente de información original. Esta cualidad de la función hash permite a cualquiera verificar la información que contiene sin necesidad de compartirla: una vez que el hash relativo a cierta información se graba en una red blockchain, puede verificarse si otra parte tiene esos mismos datos haciendo una comparación entre los hashes sin necesidad de comprobar la fuente de origen.

nodos u ordenadores del sistema desglosan los datos de las transacciones y los convierten en bloques de datos enlazados en forma de cadena.

Todos los participantes en una red blockchain tienen una copia de las transacciones que en la misma se verifican, de tal manera que la veracidad de la información cuenta con el aval de que todos los participantes tienen la misma información. Esta circunstancia permite que no se requieran terceros ajenos a la red para verificar las transacciones que en la misma se producen: todos los participantes cuentan en todo momento con la misma información, la misma versión y un medio seguro para transmitirla y conocerla (la criptografía).

4.2. Colisión entre la normativa de protección de datos y *blockchain*

La legislación de protección de datos ha sido diseñada para un mundo en el que los datos se recopilan, almacenan y procesan de manera centralizada por aquellos que realizan un tratamiento de datos en ficheros físicos o automatizados, ya sea como encargados o como responsables del tratamiento. Sin embargo venimos diciendo que blockchain parte de varios axiomas, entre los que destaca precisamente el axioma contrario, el de la descentralización.

Lo cierto es que en la filosofía de blockchain subyace la idea de que los individuos mantengan siempre el control de su actuación y que se relacionen entre sí evitando la intervención de terceras partes: los propios individuos validan estas actuaciones mediante el consenso existente entre los operadores de su red. Existen estudios que señalan las bondades que la consolidación de la tecnología blockchain traerá al mundo de la protección de datos[32].

No obstante, en el estado actual de las cosas la compatibilidad de blockchain con la normativa de protección de datos plantea serios interrogantes.

Dejaremos a un lado la compleja casuística que puede derivarse de la ley aplicable para decir aquí que una red blockchain puede interferir con varias jurisdicciones[33].

---

[32] Recomendamos a estos efectos la interesante lectura del artículo de Mainelli (2017).

[33] Simplemente mencionaremos la vocación expansiva con la que se ha planteado el RGPD. Su ámbito de aplicación territorial viene regulado en el artículo 3, que señala:

> Artículo 3. *Ámbito territorial*
>
> 1. El presente Reglamento se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no.
>
> 2. El presente Reglamento se aplica al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con:

Abordaremos la cuestión asumiendo que hablamos de una red blockchain sujeta al RGPD. En este caso los principales interrogantes a los que se debe dar solución para poder cumplir con la normativa son:

- La identificación de quiénes asumen los roles de responsables y encargados del tratamiento en un sistema por definición descentralizado.
- El ejercicio de los derechos por parte de los particulares (acceso, rectificación, cancelación, olvido…) toda vez que el talón de Aquiles de blockchain es precisamente el que los datos que se incorporan a su red se sellan y convierten en inmutables.
- La cuestión de cómo limitar el plazo de conservación de los datos: de acuerdo con la normativa, los datos personales deben mantenerse solo durante el tiempo necesario para cumplir con los fines para los que fueron recabados.
- Cómo garantizar la integridad y confidencialidad: en blockchain, por definición, todos los nodos participantes tienen acceso a los datos almacenados en la red (todos los nodos poseen una copia exacta de cada transacción realizada).

Estos interrogantes, y otros de menor importancia que nos dejamos en el tintero, deben ser resueltos para garantizar la coexistencia de la normativa con una tecnología cuyos principales atributos son precisamente la inmutabilidad de la información y la descentralización[34].

---

a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o

b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión.

3. El presente Reglamento se aplica al tratamiento de datos personales por parte de un responsable que no esté establecido en la Unión sino en un lugar en que el Derecho de los Estados miembros sea de aplicación en virtud del Derecho internacional público.

Con el fin de garantizar que las organizaciones no europeas puedan evitar la aplicación de la normativa de protección de datos simplemente por encontrarse fuera de la UE, el RGPD introduce una nueva disposición para considerar aplicable el mismo a las organizaciones o empresas extranjeras que ofrezcan productos o servicios a ciudadanos europeos. De esta manera se reemplaza el antiguo criterio de «medios» por el de «servicios».

El nuevo ámbito de aplicación conlleva el que una organización no establecida en la UE que esté procesando los datos personales de ciudadanos de la UE en actividades relacionadas con la oferta de productos o servicios a dichas personas o realizando un seguimiento, monitorización y estudio del comportamiento (como por ejemplo el seguimiento a través de cookies) deberá cumplir plenamente con el contenido del RGPD.

Será por tanto aplicable el RGPD a toda empresa extranjera que, aunque no tenga «equipos informáticos o medios» situados en la UE (como se requiere en virtud de la Directiva de protección de datos), realice una actividad real orientada de forma deliberada a personas o ciudadanos ubicados en la UE. Por lo tanto, cuando se entienda que a través de una red blockchain se está realizando una actividad de estas características, le será aplicable el RGPD.

[34] Recomendamos aquí la lectura del brillante artículo escrito por Finck (2017).

Para ello en primer lugar entendemos que deben distinguirse las redes blockchain «abiertas» de aquellas que son «cerradas». Una red abierta permite participar a cualquiera, mientras que una red privada solo admite la participación de un número discriminado de individuos. En los sistemas completamente cerrados existe un único propietario de la red blockchain que tiene competencia para dictar las normas de uso.

Desde el punto de vista de la privacidad, cada tipo de red presenta una serie de ventajas e inconvenientes.

Para proteger la confidencialidad de la información almacenada, sin duda el mejor de los esquemas posibles es el del sistema cerrado. En un sistema de este tipo siempre existirá una autoridad central (responsable del tratamiento) que permitirá identificar y proteger la confidencialidad, tanto de la información que se almacena como la de los individuos que en ella participan. Sin embargo, una red de este tipo será la menos habitual, puesto que su configuración es contraria a la filosofía de «no intermediación» de terceros que preside blockchain.

Los sistemas abiertos, mucho más frecuentes[35] en la actualidad, no permiten este control sobre los participantes ni sobre la información que se intercambia. Garantizar la confidencialidad y privacidad de lo que en ellos sucede presenta una mayor complicación.

El segundo problema que se puede presentar es el de determinar si las claves utilizadas para operar en una red blockchain, así como otros datos que se vuelcan en la misma, pueden ser considerados o no como datos personales.

Si partimos de la definición que da el RGPD:

> «Datos personales»: 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.

En principio podríamos decir que en la medida en la que no se pueda identificar a una persona a través de cierta información no estaremos ante un dato personal. Sin embargo, la interpretación de cuándo se considera que no es «identificable» una persona se ha endurecido mucho en la legislación reciente.

[35] Al que se adscribe el célebre bitcóin.

Para el Grupo de Trabajo del Artículo 29[36] solo estamos ante un verdadero dato anónimo y no personal cuando, una vez protegido mediante uno de los medios existentes, se previene irreversiblemente la identificación (Article 29 Working Party, 2014, p. 3).

En este sentido, las fórmulas más usuales utilizadas para almacenar datos en una red blockchain son el *texto abierto*, el *texto encriptado* o la *utilización de una «función hash»* que una la información a la cadena.

Los datos personales almacenados en texto abierto permiten a cualquiera acceder a los mismos, por lo que el empleo de esta fórmula no respeta la protección de los datos personales. Además almacenar de esta manera los datos no resulta tampoco operativo a nivel técnico, porque se necesita una mayor capacidad de almacenamiento que en el caso de un dato comprimido o encriptado.

Los datos encriptados se encuentran mejor protegidos, pero podrán ser revelados para aquel que cuente con la clave de encriptación. También podrán relacionarse con un sujeto, en particular cuando se produzca una transacción fuera de la cadena o al transformar criptomonedas en moneda fiat. Esta circunstancia obliga a considerarlos como datos personales y a cumplir con la legislación vigente, que los considera como pseudoanonimizados.

Es por ello que el Grupo de Trabajo del Artículo 29 (Article 29 Working Party, 2014, pp. 23 y 24) ya dejó claro su criterio de que el concepto de dato personal incluye datos encriptados aunque se hayan utilizado algoritmos de hash, como los de las cadenas de bloques.

En el caso de que se utilice una función hash, esta técnica criptográfica permite generar, para cualquier tipo de documento, información o dato, un identificador (código alfanumérico) único. Mientras el dato no se modifique, este identificador resultante será siempre idéntico; en caso de la menor variación, el identificador será diferente. Por ello, el hash puede ser considerado como la huella digital de un dato específico.

Sin embargo no puede afirmarse que aun utilizando la función hash nunca pueda correlacionarse a un sujeto con los datos personales, pues pudiese darse el caso de que se conociese que determinadas funciones hash se corresponden con ciertos datos personales.

La técnica utilizada para convertir los datos en anónimos no solo debe ser lo suficientemente buena para que sea imposible identificar a una persona física, sino que también el proceso debe ser irreversible. Si no cumple con el requisito de la irreversibilidad, resultará de aplicación el RGPD.

[36] Se denomina así al grupo de trabajo europeo independiente que se creó a raíz del mandato establecido en el artículo 29 de la Directiva con el objetivo de estudiar y desarrollar cuestiones relacionadas con la protección de la privacidad y los datos personales.

4.3. Soluciones planteadas

Existen algunas propuestas para buscar la compatibilidad entre blockchain y la legislación de protección de datos, y solucionar algunos de los interrogantes que planteábamos en el apartado anterior.

Lamentablemente ninguna de ellas está exenta de controversia y parecen factibles para las cadenas de bloques privadas, pero no para las públicas.

Podríamos pensar, por ejemplo, en una blockchain que permitiese modificar los datos registrados manteniendo el cifrado de los mismos. Para llegar a esta solución sería necesaria la intervención de un tercero (responsable del tratamiento), pero sabemos que esta circunstancia comprometería el funcionamiento descentralizado de blockchain.

Se apunta también la posibilidad de utilizar la red blockchain únicamente para almacenar la información encriptada correspondiente a cada dato (los hashes), almacenando los datos personales en otra base de datos separada y gestionada por un responsable del tratamiento plenamente sujeto al RGPD. De este modo se garantizaría el principio de confidencialidad e integridad de los datos personales, puesto que los usuarios de la red solo tendrían acceso a hashes.

Adicionalmente, se podrían garantizar los derechos de las personas (acceso, rectificación, cancelación, olvido, etc.) sobre sus datos, que serían ejercitados modificando la base de datos personales separada, pero sin renunciar totalmente a los beneficios inherentes a la inmutabilidad que caracteriza la tecnología blockchain. Sin embargo, una solución así podría suponer mermas a la seguridad a la hora de manejar las dos bases de datos, si pensamos en el siguiente ejemplo: Si se produjera la circunstancia de que alguien conoce el conjunto de hashes utilizados por un sujeto o corporación y además dispusiera del conjunto de datos a los que dichos hashes se encuentran o pueden encontrarse asociados, podría intentar realizar operaciones de cruce con el resultado de que pudiese llegar a asociar un hash a ciertos datos personales. No se cumpliría con la exigencia de irreversibilidad y por lo tanto no quedaría garantizado el cumplimiento del RGPD. Con el objetivo de evitar lo anterior podría reforzarse la seguridad de los hashes acudiendo a técnicas de asociación con valores aleatorios (al modo al que se emplea un *token* en seguridad).

Otra solución pasaría por sofisticar la interactuación dentro de la propia red blockchain entre ciertos usuarios de los mismos, mediante la creación de un «canal privado». Este canal permitiría la transmisión de información creada por dos o más usuarios que quisieran compartir información en privado dentro la red blockchain, es decir, sin que los demás nodos sepan qué contenido comparten. El resto de nodos (los que se encuentran fuera del canal privado) solo podrán conocer el hash de la información que se comparta en el canal privado.

A través de este canal privado podría producirse el intercambio de datos personales cifrados entre los usuarios del mismo, cumpliendo con lo establecido en la legislación de protección de datos. El ejercicio de derechos por parte de los particulares se podría garan-

tizar mediante la eliminación por parte de los usuarios del canal privado de la clave de descifrado que corresponda a los datos personales, en concreto que sufran la correspondiente modificación, rectificación o cancelación. De esta manera, una vez ejercitados los derechos, el registro antiguo permanecería inidentificable e inaccesible para toda la red (incluyendo el canal privado), pudiéndose crear un nuevo registro actualizado, que recibiría una nueva clave de cifrado. El resto de participantes en la red solo tendría acceso a los hashes de información privada que es compartida en la red.

No sabemos cuáles serán las diferentes soluciones que se irán adoptando conforme las redes blockchain se impongan como soluciones técnicas a problemas actuales. Sí que entendemos que ha merecido la pena apuntar aquí que en su planteamiento inicial suponen una colisión con la legislación de protección de datos, que debe evitarse mediante la adopción por parte de los desarrolladores de las soluciones pertinentes, en espera de que el legislador y los tribunales puedan apuntar otras soluciones *ad hoc*.

5. La creciente amenaza de los ciberataques y la protección de datos personales

Se calcula que el cibercrimen supone un 0,8 % del producto interior bruto mundial (Sánchez, 2018), y que es el tipo de delincuencia que más beneficio está generando a sus actores, solo por detrás del narcotráfico y la corrupción.

A través de internet y los dispositivos conectados los delincuentes buscan espiar, extorsionar y sustraer lo que se ha denominado como el «nuevo oro» de la economía: los datos, tanto personales como no personales.

En los últimos años ha tenido una tremenda repercusión la noticia del ciberataque a la compañía de información crediticia norteamericana Equifax, que tuvo que admitir en un comunicado que le habían sido sustraídos datos de 143 millones de personas en un ciberataque producido entre mayo y julio de 2017[37]. La información obtenida por los piratas informáticos incluyó números del seguro social, fechas de nacimiento, direcciones y, en algunos casos, números del carné de conducir, de tarjetas de crédito y otra documentación.

Frente a amenazas de semejante tipo, la nueva era digital en la que estamos inmersos no puede entenderse sin la ciberseguridad[38], herramienta que consiste en la adopción de

[37] La noticia fue publicada en numerosos medios de comunicación. Está disponible en Agencia EFE (2017).

[38] El término «ciberseguridad» no se encuentra aceptado por la RAE en la fecha de redacción de este trabajo. Se trata de una traducción literal del término anglosajón *cybersecurity*, y como tal es aceptado por todo el sector como todas aquellas medidas de defensa y políticas encaminadas a evitar la delincuencia en el entorno/espacio de la informática e internet.

una serie de mecanismos de salvaguarda, defensa y respuesta frente a las amenazas, que resulta necesaria para aportar confianza y estabilidad a todo el entorno digital y, en consecuencia, a empresas, gobiernos y ciudadanos por igual.

El incremento exponencial de los ciberataques ha obligado al legislador europeo a adoptar una normativa exigente para dar una respuesta ágil a un problema común.

En el caso español, desde hace unos meses se encuentra en vigor el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información (en adelante, el Real Decreto-Ley), cuyo objeto es precisamente la trasposición de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión Europea, conocida como Directiva de Ciberseguridad.

El Real Decreto-Ley establece mecanismos para mejorar la protección frente a las amenazas, riesgos e incidentes que afectan a las redes y sistemas de información[39], y que casi siempre implican un riesgo para los datos personales. Para lograrlo, se establece el principio de coordinación de las actuaciones realizadas a nivel nacional y europeo.

El Gobierno ha optado por extender el ámbito de aplicación a servicios tanto excluidos como no expresamente incluidos en la Directiva de Ciberseguridad, con el objetivo darle a la norma española un enfoque global.

Los sujetos obligados por el Real Decreto-Ley son:

a) *Los establecimientos permanentes situados en España*[40] *y los operadores establecidos*[41] *en España que presten servicios esenciales para la comunidad* y dependan de las redes y sistemas de información para el desarrollo de su actividad (OSE). En relación con las actividades de explotación de las redes y de prestación de servicios de comunicaciones electrónicas y recursos asociados, así como de los servicios electrónicos de confianza (expresamente excluidos de la directiva) el Real Decreto-Ley se aplicará únicamente en lo que se refiere a los operadores críticos.

---

39 Por redes y sistemas de información se entienden las 1) redes de comunicaciones electrónicas definidas en la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones; 2) dispositivos o grupo de dispositivos interconectados o relacionados entre sí, cuando uno o varios de ellos realicen tratamiento automático de datos digitales; 3) los datos digitales almacenados, tratados, recuperados o transmitidos mediante los elementos anteriores, incluidos los necesarios para el funcionamiento, utilización, protección y mantenimiento de dichos elementos.

40 De operadores residentes o domiciliados en otro Estado.

41 Cuando su residencia o domicilio social se encuentren en territorio español, siempre que estos coincidan con el lugar en que esté efectivamente centralizada la gestión administrativa y la dirección de sus negocios o actividades.

b) *Los proveedores de determinados servicios digitales que tengan su sede social en España (PSD).*

En relación con el primer tipo de sujetos obligados, los OSE se definen como aquellas entidades públicas o privadas que presten servicios esenciales[42] en alguno de los sectores estratégicos definidos en el anexo de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas[43], listado que deberá mantenerse actualizado con una frecuencia bienal.

El segundo tipo, los PSD, son un colectivo que abarca a un importante espectro de obligados: todas aquellas personas jurídicas que prestan un servicio digital de los recogidos en la letra a) del anexo de la Ley 34/2002 de 11 de julio, de servicios de la sociedad de la información y comercio electrónico. Es importante destacar que quedan excluidos del ámbito de aplicación del Real Decreto-Ley ciertos operadores de menor importancia en el sistema[44].

Una vez descritos los sujetos obligados, lo más importante es conocer a qué se ven obligados como consecuencia de la aplicación de esta nueva normativa. En este sentido podemos dividir las obligaciones en dos grupos:

a) *La necesidad de adoptar medidas técnicas y de organización adecuadas* y proporcionadas para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información utilizados en la prestación de servicios[45]. Se incluye el caso de que la gestión de los servicios esenciales o digitales se encuentre externalizada.

---

[42] Servicio esencial es aquel necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social económico de los ciudadanos o el eficaz funcionamiento de las instituciones del Estado y las Administraciones públicas, que dependa para su provisión de redes y sistemas de información.

[43] Se entiende por los mismos los que operan en el ámbito de la Administración, espacio, industria nuclear, industria química, instalaciones de investigación, agua, energía, salud, tecnología de la información y la comunicación, transporte, alimentación, *sistema financiero y tributario*.

[44] Quedan excluidos:

a) Los operadores de redes y servicios de comunicaciones electrónicas y los prestadores de servicios electrónicos de confianza *que no sean designados como operadores críticos* en virtud de la Ley 8/2011 de 28 de abril; y

b) Los PSD *cuando se trate de microempresas o pequeñas empresas*, de acuerdo con las definiciones recogidas en la Recomendación 2003/361/CE de la Comisión, de 6 de mayo de 2003, sobre la definición de microempresas, pequeñas y medianas empresas.

[45] Las medidas técnicas que deberán adoptar los OSE deberán ser desarrolladas reglamentariamente. En el caso de los PSD, deberán adoptar medidas de seguridad que tengan en cuenta los avances técnicos que se produzcan, así como los siguientes aspectos: a) la seguridad de los sistemas e instalaciones; b) la gestión de incidentes; c) la gestión de la continuidad de las actividades; d) la supervisión, auditorías y pruebas; e) el cumplimiento de las normas internacionales.

b) *La notificación de incidentes*[46] que sufran las redes y servicios de información que se emplean para la prestación de servicios esenciales y digitales a las autoridades competentes.

En todos los casos, los OSE y los PSD tienen la obligación de resolver los incidentes de seguridad que les afecten y de solicitar ayuda especializada cuando no puedan resolver por sí mismos los incidentes. De esta manera el legislador ofrece un doble sistema de garantía –sujeto/autoridades–, necesario ante una amenaza que pueda tener consecuencias muy serias para todos.

Debe señalarse que la obligación de notificar incidentes incluye además la notificación de aquellos que puedan haber afectado a datos personales.

En estos casos, tanto las autoridades competentes como los centros de respuesta de incidencias (CSIRT) de referencia comunicarán sin dilación a la AEPD los incidentes producidos y la mantendrán informada sobre su evolución, cooperando con la misma en todo lo que sea necesario para hacer frente a dichos incidentes.

Se establece aquí una obligación que supone una auténtica novedad y a su vez se coordina con una de las novedades más importantes del RGPD, *la que establece la obligación de reportar estos incidentes a cualquier responsable de un tratamiento de datos personales a la autoridad de control competente, que en el caso español es la AEPD*.

Antes de que entrara en vigor el RGPD, la normativa de protección de datos únicamente establecía la obligación de notificar las brechas de seguridad en las que se vieran afectados datos personales a los operadores de servicios de comunicaciones electrónicas y a los prestadores de servicios de confianza.

Por consiguiente, tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una violación de la seguridad de los datos personales deberá, sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, notificar la violación de la seguridad de los datos personales a la AEPD, a menos que el responsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de que la violación de la seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas. Si dicha notifi-

[46] Tanto los OSE como los PSD están obligados a notificar a la autoridad competente, a través del centro de respuesta de incidentes que se establezca en su caso, los incidentes que afecten a las redes y sistemas de información que utilicen en la prestación de sus servicios que puedan tener efectos perturbadores significativos en la prestación de los mismos, tanto en el caso de que se trate de redes y servicios propios como si lo son de proveedores externos.

Merece la pena destacar que las autoridades competentes, los CSIRT y el punto único de contacto, deberán salvaguardar la confidencialidad de la información recabada a través de las notificaciones, con el objetivo de garantizar la seguridad y los intereses comerciales de los OSE y PSD.

cación no es posible en el plazo de 72 horas, debe acompañarse de una indicación de los motivos de la dilación, pudiendo facilitarse información por fases sin más dilación indebida.

Tal y como sucede en el caso de la normativa de protección de datos personales, las infracciones del Real Decreto-Ley son de una cuantía muy considerable y se clasifican en muy graves, graves y leves. Las sanciones muy graves pueden acarrear sanciones de entre 500.000 y 1.000.000 de euros, las graves entre 100.000 y 500.000 y las leves de hasta 100.000 euros.

Para facilitar el cumplimiento de la obligación de notificación, la AEPD ha publicado una guía para el cumplimiento de notificaciones de brechas de seguridad[47].

Se atisba en este terreno por lo tanto una tendencia clara hacia la prevención y rápida cauterización de los problemas causados por los ciberataques, en los que la actuación conjunta de los responsables de tratamiento y las autoridades implicadas está llamada a cumplir un papel esencial en los próximos años.

No obstante debe tenerse en cuenta que la ciberseguridad deberá adaptarse continuamente, debido al cambiante ingenio empleado por los delincuentes y piratas de internet.

6. Conclusiones

Desde su nacimiento hasta la actualidad, el derecho a la protección de datos personales se enfrenta a numerosos retos. Hemos pretendido en estas líneas el objetivo muy ambicioso de abarcar un área muy extensa en la que podrían incluirse muchas otras observaciones y materias: las particularidades de las redes sociales, el entorno del *big data*, el coche autónomo, las aplicaciones de los teléfonos móviles, etc.

Por su importancia hemos creído conveniente trazar una evolución del derecho para poder analizar algunas cuestiones de rabiosa actualidad e importancia. El derecho al olvido, como nueva manifestación de un derecho que ya existía bajo formulaciones anteriores pero que debe ejercitarse ahora en ese océano sin límites que es internet y que se encuentra siempre en riesgo de entrar en colisión con el derecho fundamental a la información.

Han merecido también nuestro análisis los retos del nuevo entorno que parece estar creando la tecnología blockchain: son varias las industrias que han creado enormes consorcios y destinado fondos millonarios para su estudio y desarrollo común (financiera, aseguradora, tecnológica). Sin embargo, la falta de previsión de una correcta configuración técnica que permita a dichos desarrollos cumplir con la normativa de protección de datos puede comprometerlos y arrastrarlos a una muerte prematura.

[47] Puede consultarse en <https://www.aepd.es/media/guias/guia-brechas-seguridad.pdf>.

Por último, no podíamos dejar de mencionar, al hilo del nuevo RGPD, el importantísimo terreno de la ciberseguridad que ahora conecta el mundo de la seguridad informática y de sistemas con el de la protección de datos. Los sujetos implicados deben velar por el cumplimiento de una normativa cada día más exigente y protegerse de las amenazas del entorno en el que se mueven, el entorno conectado, para evitar que los ciberdelincuentes cometan millonarios robos y delitos en los que se vean involucrados además datos personales.

Referencias bibliográficas

Agencia EFE (2017). Un ciberataque masivo roba los datos de 143 millones de estadounidenses. *El País*. Recuperado de <https://elpais.com>. Acceso el 14 de enero de 2019.

Article 29 Working Party (2014). Opinion 05/2014 on Anonymisation Techniques. Recuperado de <https://www.pdpjournals.com>. Acceso el 24 de febrero de 2019.

Barrio, M. (2018). Los nuevos derechos digitales en España. *El País Retina*. Recuperado de desde <https://retina.elpais.com/retina>. Acceso el 20 de enero de 2019.

Finck, M. (2017). Blockchains and Data Protection in the European Union. *Max Planck Institute for Innovation and Competition Research Paper Series. Paper 18-01*. Recuperado de <https://papers.ssrn.com>. Acceso el 20 de noviembre de 2018.

González de Frutos, U. (2018). La fiscalidad en el mundo Blockchain. *Revista de Contabilidad y Tributación. CEF*, *425-426*, 5-36.

Kaulartz M. y Heckmann J. (2016). Smart Contracts – Anwendungen der Blockchain Technologie. *Computer und Recht*, *32*, 618-624.

Mainelli, M. (2017). Blockchain could help us reclaim control over our personal data. *Harvard Business Review*.

Pollock, D. (2018). The Fourth Industrial Revolution Built On Blockchain And Advanced With AI. *Forbes*. Recuperado de <https://www.forbes.com>. Acceso el 25 de enero de 2019.

Sánchez, J. M. (2018). El cibercrimen es incesante: provoca un agujero de 600.000 millones de dólares a las empresas. *ABC*. Recuperado de <https://www.abc.es>. Acceso el 8 de enero.

Szabo, N. (1997). Formalizing and Securing Relationships on Public Networks. *First Monday*. *2*(9). Recuperado de <http://firstmonday.org>. Acceso el 28 de enero de 2019.

Warren, S. y Brandeis, L. (1890). The Right to Privacy. *Harvard Law Review*, *IV*(5). Recuperado de <http://faculty.uml.edu>. Acceso el 23 de enero de 2019.

Werbach, K. y Cornell, N. (2017). Contracts Ex Machina. *Duke Law Journal*, *67*, 314-381. Recuperado de <https://scholarship.law.duke.edu>. Acceso el 28 de enero de 2019.