El derecho al olvido en la Unión Europea y su relevancia en relación con la tecnología Blockchain

Amalia Balaguer Pérez
Doctora en Derecho por la UNED

1. Introducción

Blockchain es una tecnología, relativamente reciente, mediante la que se almacenan datos. Se trata de "una tecnología que permite a grandes grupos de gente y organizaciones alcanzar un acuerdo sobre registrar información y registrarla permanentemente, sin ninguna autoridad central (...) es simplemente una base de datos compartida (...) todos los participantes de la red tienen su propia copia de la base de datos"[1].

Tras la entrada en vigor del Reglamento General de Protección de Datos han surgido dudas sobre la posible colisión entre esta tecnología y el llamado "derecho al olvido" recogido en el Reglamento. Esta comunicación analiza el derecho al olvido y esta posible colisión del derecho con la tecnología Blockchain (en adelante BC).

De acuerdo con ØLNES, S., UBACHT, J., y JANSSEN, M., mediante esta tecnología, "pueden añadirse transacciones nuevas, pero la información previa no puede eliminarse"[2]. Sin embargo, también afirman que "esto no significa que el BC sea inalterable. Las partes controladoras que establecen el BC (que van desde ciudadanos hasta organizaciones públicas o privadas) pueden decidir alterar la historia de un BC"[3].

Varias opiniones han afirmado que hay una colisión entre la tecnología BC y el derecho al olvido[4].

1 EU BLOCKCHAIN. OBSERVATORY AND FORUM, *FAQ*: "A technology that allows large groups of people and organizations to reach agreement on and permanently record information without a central authority (...) a blockchain is simply a shared database (...) all participants on the network have their own copy of the database". Disponible en: https://www.eublockchainforum.eu/faq

2 ØLNES, S., UBACHT, J., y JANSSEN, M., "Blockchain in government: Benefits and implications of distributed ledger technology for information sharing", Editorial, *Government Information Quarterly* 34, 2017, 355-364, p. 355: "New transactions can be added, but previous information cannot be removed enabling all nodes to track the history".
También: SATER, S., Blockchain and the European Union's General Data Protection Regulation: A Chance to Harmonize International Data Flows, 6 de Noviembre de 2017, p. 20, citando a NAKAMOTO: "Because of the transaction process, the blockchain is an append-only, immutable, and timestamped chain of information. In order for someone to change a transaction, they would have to redo all of the previous miner's work to produce a different winning nonce and redo the work for all the subsequent blocks to keep the chain intact".

3 Íbidem, p. 356: "However, this does not mean that the BC is unalterable. The controlling parties that set up the BC (ranging from citizens to public or private organizations) can decide to alter the history of a BC".
También se argumenta que "BCs que funcionan por el protocolo de consenso Prueba de Trabajo (PdT) han sido vulnerables a ataques 51%, p.ej. los mineros que controlan más de la mitad de los recursos PdT pueden controlar la inclusión de nuevos bloques y también posiblemente reescribir la historia del BC", ØLNES, S., UBACHT, J., y JANSSEN, M., "Blockchain in government: Benefits and implications of distributed ledger technology for information sharing", Editorial, *Government Information Quarterly* 34, 2017, 355-364, p. 360: "BCs powered by the consensus protocol Proof of Work (PoW) have been susceptible to 51% attacks, e.g. the miners that control more than half of the PoW resources can control the inclusion of new blocks and also possibly rewrite the BC history".

4 SMITH., J., TENNISON, J., WELLS, P., FAWCETT, J., HARRISON, S., *Applying blockchain technology in global data infrastructure*, Open Data Institute, 2016, p. 16: "The irreversibility and transparency of public blockchains mean they are probably unsuitable for personal data. We need to be careful when designing blockchain systems not

Ya que una de las características de la tecnología BC es que no pueden modificarse los datos almacenados con esta tecnología, el derecho a la supresión o a la modificación de los datos no es "posible en blockchains, que son, en teoría, inmutables"[5].
En cuanto a la tecnología BC en la UE, recientemente se ha firmado la Declaración "Cooperation on a European Blockchain Partnership", en la que no se menciona esta posible colisión, pero, por otra parte se establece que los firmantes trabajarán para apoyar los objetivos entre los que se incluyen "asistir a la Comisión a preparar las especificaciones técnicas de esta iniciativa, definir el modelo de gobernanza apropiado e identificar otras condiciones de infraestructura que son esenciales para su éxito (incluyendo el cumplimiento de los requisitos regulatorios)"[6].

2. El derecho al olvido

El derecho al olvido es el derecho que tienen las personas a que se eliminen determinados datos, tanto los que han sido cedidos voluntariamente, como aquellos que se han publicado, por ejemplo, por los medios.
De acuerdo con SARRIÓN ESTEVE, "el derecho al olvido tiene su origen o fuente en el derecho fundamental a la protección de datos, aunque sin duda podemos considerar que goza de una sustancia o entidad autónoma con respecto a aquél, siendo diferente a una mera proyección de la facultad de cancelación de datos que forma parte del haz de facultades que conforman el derecho fundamental a la protección de datos"[7].
Por otra parte de, según MANTELERO, "la noción europea del derecho al olvido tiene Su orígenes en el *droit à l'oubli*, reconocido por diferentes decisiones en Francia y otros países europeos"[8]. No obstante, también afirma el autor que "la representación diferente del derecho al olvido como el derecho a que los datos personales se borren completamente es consistente con la noción del droit à l'oubli, pero en este caso tiene un alcance más amplio, porque la eliminación de los datos no está relacionada sólo con la perdida de interés en eventos pasados, sino también con otras situaciones (p. ej. procesamiento de datos ilícito o arbitrario) que no conciernen al equilibrio entre los medios y la vida individual"[9]. Efectivamente, se trata de un derecho que cubre no sólo información publicada en

---

to infringe on people's privacy, and to account for a world in which we have doxing, identity theft and the right to be forgotten".
También: SATER, S., Blockchain and the European Union's General Data Protection Regulation: A Chance to Harmonize International Data Flows, 6 de Noviembre de 2017, p, 37: "The right to erasure is an obstacle for blockchain technology" y ZETZSCHE, D. A., BUCKLEY, R. P., ARNER, D. W., The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain, University of New South Wales Law Research Series, 2017, p. 15:"Another interference with privacy rights stems from the fact that data once stored on the ledger cannot be erased: this is the immutability feature of DLT. This may have devastating consequences to an individual or entity. (...)This is at odds with the 'right to be forgotten'granted in some jurisdictions".

5 LYONS, T., *Workshop Report - GDPR*, EU Blockchain Observatory and Forum, Bruselas, 8 de junio de 2018, p. 5: "Right to amendment/erasure: not possible in blockchains, which are in theory immutable and tamper proof".

6 Declaration. *Cooperation on a European Blockchain Partnership*, 2018, III, 7. b: "By the end of 2018, assisting the Commission in preparing the technical specifications of this initiative, defining the appropriate governance model and identifying other framework conditions which are essential to its success (including compliance with regulatory requirements)".

7 SARRIÓN, J., "La cuestión territorial en el derecho al olvido tras Google Spain", en COTINO HUESO, L., SAHUQUILLO OROZCO, J.L., CORREDOIRA ALFONSO, L. (eds.), *El paradigma del Gobierno Abierto. Retos y oportunidades de la participación, transparencia y colaboración*, Universidad Complutense de Madrid, pp. 161-170, p. 163.

8 MANTELERO, A., "The EU Proposal for a General Data Protection Regulation and the roots of the 'right to be forgotten'", *Computer law & security review* 29, 2013, 229-235, p. 229: "The European notion of the right to be forgotten draws its origins from *droit à l'oubli*, recognized by different decisions in France and in other European countries".

9 Íbid., p. 233: "The different representation of the right to be forgotten as the right to have personal data completely removed is consistent with the notion of droit à l'oubli, but in this case it has a wider scope, because the erasure of the data is not only related to the loss of interest in past events, but also to other situations (e.g.wrongful or illicit

los medios sino también datos personales cedidos de manera voluntaria.
Se trata de un derecho no absoluto cuya mayor relevancia se pone de manifiesto en relación con Internet, puesto que gran parte de datos personales se ceden en este medio o aparecen en este medio (ya sea información personal cedida voluntariamente, fotos publicadas por la persona interesada, o, por otra parte, noticias en periódicos digitales concernientes a una persona). La información en Internet significa, además, una mayor difusión, por lo que el derecho al olvido cobra mayor importancia.
En relación con la tecnología BC ha de decirse que el aspecto más importante de este derecho surge con aquellos datos almacenados, más que aquellos publicados en medios, pues, como hemos dicho, la tecnología BC tiene como utilidad el almacenamiento de datos.
Este derecho ha sido recientemente recogido y regulado en el Artículo 17 del Reglamento General de Protección de Datos (Reglamento 2016/679), pero ya en la Directiva de Protección de datos (Directiva 95/46/CE) aparecía un derecho al olvido, si bien no era así denominado y tenía una aplicación mucho más limitada.
En el año 2012, Vivian Reding, la vicepresidenta de la Comisión Europea, en un discurso sobre la reforma de la protección de datos mencionó también este derecho, al afirmar que "las personas deben poder, de manera fácil, llevar sus datos a otro proveedor o hacer que se borren si ya no quieren que se usen (...) Otro modo importante de dar a las personas control sobre sus datos: el derecho a ser olvidado. Quiero clarificar de manera explícita que las personas tendrán el derecho - y no sólo la "posibilidad" - de retirar su consentimiento al procesamiento de los datos personales que han dado (...) Si un individuo ya no quiere que un controlador de datos procese o almacene sus datos, y si no hay una razón legítima para mantenerlos, los datos deberían eliminarse de su sistema. El derecho a ser olvidado no es, por supuesto, un derecho absoluto. Hay casos en los que hay un interés legítimo y legalmente justificado de mantener datos en una base de datos"[10]. Destaca, también, la necesidad de reforma puesto que "en 1993, Internet portaba sólo un 1% de la información telecomunicada"[11].
Efectivamente, el derecho al olvido no se ha regulado como un derecho absoluto y se han establecido disposiciones para la libertad de información y expresión, como veremos posteriormente.

3. La protección de datos en la Unión Europea

Hasta la entrada en vigor del Reglamento General de Protección de Datos, la protección de los datos personales se encontraba en la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995. Posteriormente, la Carta de Derechos Fundamentales de la Unión Europea, que entró en vigor el 1 de diciembre de 2009, incorpora en su artículo 8 un derecho fundamental a la protección de datos de carácter personal[12].

---

data processing) that do not concern the balance between media and individual life".

10 REDING, V., The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age, *Innovation Conference Digital, Life, Design*, Munich, 22 de enero de 2012, p. 5: "People must be able to easily take their data to another provider or have it deleted if they no longer want it to be used. (...) Another important way to give people control over their data: the right to be forgotten. I want to explicitly clarify that people shall have the right – and not only the 'possibility' – to withdraw their consent to the processing of the personal data they have given out themselves (...) If an individual no longer wants his personal data to be processed or stored by a data controller, and if there is no legitimate reason for keeping it, the data should be removed from their system.
The right to be forgotten is of course not an absolute right. There are cases where there is a legitimate and legally justified interest to keep data in a data base".

11 Íbidem, p. 2: "In 1993, the Internet carried only 1% of all telecommunicated information. Today, the figure has risen to more than 97%".

12 "1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.
2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona

La Directiva no establecía de manera expresa un derecho al olvido así formulado, pero sí existía una disposición relacionada, en el artículo 12. b (derecho de acceso), en la que se establecía que "los Estados miembros garantizarán a todos los interesados el derecho de obtener del responsable del tratamiento: (...) b) en su caso , la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la presente Directiva, en particular a causa del carácter incompleto o inexacto de los datos".

Aunque no puede considerarse un derecho al olvido, debido a sus limitaciones y condiciones y a que no depende de la simple voluntad de la persona interesada de eliminar sus datos, sí implica la obligación de eliminar los datos en ciertos supuestos. Efectivamente, como indican FOSCH VILLARONGA, KIESEBERG y LI "el Derecho al Olvido no es cien por cien nuevo. La Directiva 95/46/EC de protección de datos ya contenía el "derecho de acceso" en su Artículo 12, lo que ya, de algún modo, contemplaba la posibilidad de imponer la eliminación de datos ilegales, inexactos o incompletos por parte del controlador de datos"[13].

Posteriormente, este derecho se ha desarrollado jurisprudencialmente, concretamente en la Sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014 (C-131/12), conocida como "caso Google". En esta sentencia, el Tribunal afirmó, respecto a la supresión de datos, que "en el supuesto en el que se aprecie, tras una solicitud del interesado en virtud del artículo 12, letra b), de la Directiva 95/46, que la inclusión en la lista de resultados obtenida como consecuencia de una búsqueda efectuada a partir de su nombre, de vínculos a páginas web, publicadas legalmente por terceros y que contienen datos e información verídicos relativos a su persona, es, en la situación actual, incompatible con dicho artículo 6, apartado 1, letras c) a e)[14], debido a que esta información, habida cuenta del conjunto de las circunstancias que caracterizan el caso de autos, es inadecuada, no es pertinente, o ya no lo es, o es excesiva en relación con los fines del tratamiento en cuestión realizado por el motor de búsqueda, la información y los vínculos de dicha lista de que se trate deben eliminarse"[15]. La persona interesada "puede, habida cuenta de los derechos que le reconocen los artículos 7 y 8 de la Carta, solicitar que la información de que se trate ya no se ponga a disposición del público en general mediante su inclusión en tal lista de resultados, estos derechos prevalecen, en principio, no sólo sobre el interés económico del gestor del motor de búsqueda, sino también sobre el interés de dicho público en acceder a la mencionada información en una búsqueda que verse sobre el nombre de esa persona. Sin embargo, tal no sería el caso si resultara, por razones concretas, como el papel desempeñado por el interesado en la vida pública, que la injerencia en sus derechos fundamentales está justificada por el interés preponderante de dicho público en tener, a raíz de esta inclusión, acceso a la información de que se trate"[16]. Ya antes del Reglamento se reconocía, por tanto, en la Directiva de protección de datos, un derecho al olvido más limitado, relacionado principalmente con la pertinencia de la información, que, a su vez, se relaciona con el paso del tiempo: "se deduce de estos requisitos, establecidos en el artículo 6, apartado 1, letras c) a e), de la Directiva 95/46, que incluso un tratamiento inicialmente lícito de datos exactos puede devenir, con el tiempo, incompatible con dicha Directiva cuando estos datos ya no sean necesarios en relación con los fines para los que se recogieron o trataron. Éste es el caso, en

---

afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación.

3. El respeto de estas normas estará sujeto al control de una autoridad independiente".

13 FOSCH VILLARONGA, E., KIESEBERG, P., LI, T., "Humans forget, machines remember: Artificial intelligence and the Right to Be Forgotten", *Computer Law & Security Review* 34 (2018) 304-313, p. 306: "Indeed, the Right to Be Forgotten is not hundred percent new. The data protection directive 95/46/EC already contained the "right of access" on its Article 12, which somehow already contemplated the possibility to enforce the erasure of incomplete, inaccurate or illegal data from the data controller."

14 El artículo 6.1, letras c) a e) establece que los datos personales deben ser adecuados, pertinentes, no excesivos, exactos y actualizados, y conservados durante un tiempo no superior al necesario.

15 Sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014, 94.

16 Íbidem, 99.

particular, cuando son inadecuados, no pertinentes o ya no pertinentes o son excesivos en relación con estos fines y el tiempo transcurrido"[17].

De acuerdo con SARRIÓN ESTEVE, "Google Spain es el último eslabón dentro de una jurisprudencia tuteladora de la protección de datos por parte del TJUE que ha conseguido dar carta de naturaleza al derecho al olvido en la Unión Europea"[18].

Podríamos decir que ya existía un posible conflicto con la tecnología BC desde el momento en el que la Directiva se encontraba en vigor, puesto que, aunque esta no recogía un derecho al olvido así denominado, si recogía el derecho a que los datos se eliminasen en ciertos supuestos. Sin embargo, en el nuevo Reglamento este derecho se incluye de manera explícita y detallada.

Por otra parte, según BUNN, "la decisión Google ha confirmado que la referencia a la inconclusión o inexactitud de los datos es sólo a modo de ejemplo y no es exhaustiva"[19].

No obstante, limitado como era, este derecho ya habría colisionado con una tecnología en la que la eliminación de datos no fuera posible, puesto que en ciertos casos la persona interesada podía pedir la supresión de los datos. Sin embargo, esto no era un problema en el año 1995, ya que no existía la tecnología BC.

En el ámbito nacional, en la STC 58/2018 el Tribunal Constitucional afirma que "la prohibición de indexar los datos personales, en concreto los nombres y los apellidos de las personas recurrentes, para su uso por el motor de búsqueda interno de "El País" debe ser considerada una medida limitativa de la libertad de información idónea, necesaria y proporcionada al fin de evitar una difusión de la noticia lesiva de los derechos invocados"[20], de manera que establece que los datos, además de no aparecer en los buscadores generales si así lo exige la persona interesada, no deben aparecer tampoco en los motores de búsqueda internos de los medios de comunicación.

4. El derecho al olvido en el RGPD

El reglamento se aplica, salvo algunas excepciones, "al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero" en el ejercicio de actividades comprendidas en el ámbito de aplicación del Derecho de la Unión[21].

El derecho al olvido se regula en el artículo 17, que establece unas condiciones para el ejercicio de este derecho, entre las que se encuentran, que "los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo", la persona interesada haya retirado su consentimiento, la persona interesada se oponga (excepto si prevalecen motivos legítimos para el tratamiento), los datos hayan sido tratados de manera ilícita, los datos deban suprimirse debido a una obligación legal del responsable del tratamiento, o se hayan obtenido en relación con una oferta directa de servicios de la sociedad de la información a niños[22].

17 Íbidem, 94.

18 SARRIÓN, J., "La cuestión territorial en el derecho al olvido tras Google Spain",en COTINO HUESO, L., SAHUQUILLO OROZCO, J.L., CORREDOIRA ALFONSO, L. (eds.), *El paradigma del Gobierno Abierto. Retos y oportunidades de la participación, transparencia y colaboración*, Universidad Complutense de Madrid, pp. 161-170, p. 170.

19 BUNN, A., "The curious case of the right to be forgotten", *Computer Law & Security Review* 31, 2015, 336-350, p. 342: "the Google decision has confirmed that reference to the incompleteness or inaccuracy of the data is by way of example only and is not exhaustive".

20 STC 58/2018, FJ 8.

21 Reglamento (ue) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). *Artículo 2.*

22 *Artículo 17.*

Derecho de supresión («el derecho al olvido»)

1. El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales

En principio, el único requisito que hay para que alguien pueda pedir la supresión de sus datos es que retire el consentimiento o se oponga (cumpliéndose los requisitos establecidos). Se establecen también una serie de excepciones, entre las que se encuentran que el tratamiento sea necesario "para ejercer el derecho a la libertad de expresión e información". Debe notarse que este artículo regula la supresión de los datos, es decir, no basta, en principio, con que los datos no sean públicos o que nadie pueda acceder a ellos, sino que deben eliminarse.
En todo caso, la regulación de este derecho difiere de la regulación anterior, que exigía que el tratamiento de datos no se ajustase "a las disposiciones de la presente Directiva, en particular a causa del carácter incompleto o inexacto de los datos" para ejercer el derecho a suprimir los datos. Se amplían, por tanto, los supuestos en los que se puede exigir que se eliminen los datos, pero, respecto a la tecnología BC, la regulación anterior también era problemática.

4.1.*Excepciones*

Hay que examinar las excepciones, en cualquier caso, en las que no se aplica el derecho al olvido, que se encuentran recogidas en el artículo 17.3. La primera excepción del derecho al olvido es que el tratamiento de datos sea necesario para ejercer el derecho a la libertad de expresión e información. Sin embargo, debido a la subjetividad de lo que pueda considerarse necesario para ejercer este derecho a la libertad de expresión, es difícil que puedan almacenarse datos con BC asumiendo en principio que son datos necesarios para ejercer este derecho. Se trata, más bien, de una disposición que podría aplicarse cuando ya se haya solicitado la supresión de los datos, si bien está previsto el desarrollo legal en el artículo 85.1 del Reglamento: "Los Estados miembros conciliarán por ley el derecho a la protección de los datos personales en virtud del presente Reglamento con el derecho a la libertad de expresión y de información, incluido el tratamiento con fines periodísticos y fines de expresión académica, artística o literaria".
Otra excepción al derecho al olvido es que el tratamiento sea necesario "para el cumplimiento de

---

cuando concurra alguna de las circunstancias siguientes:
a) los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;
b) el interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico;
c) el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2;
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.
2. Cuando haya hecho públicos los datos personales y esté obligado, en virtud de lo dispuesto en el apartado 1, a suprimir dichos datos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.
3. Los apartados 1 y 2 no se aplicarán cuando el tratamiento sea necesario:
a) para ejercer el derecho a la libertad de expresión e información;
b) para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable;
c) por razones de interés público en el ámbito de la salud pública de conformidad con el artículo 9, apartado 2, letras h) e i), y apartado 3;
d) con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, en la medida en que el derecho indicado en el apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o
e) para la formulación, el ejercicio o la defensa de reclamaciones.

una obligación legal que requiera el tratamiento de datos". En este caso, y con la existencia de una obligación legal definida, los datos en cuestión podrían almacenarse con la tecnología BC, puesto que no podría exigirse la eliminación de estos. El mismo apartado recoge como excepción que el tratamiento sea necesario "para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable", para lo que aplica lo mismo.
Lo mismo puede decirse de las últimas tres excepciones: por razones de interés público en el ámbito de la salud pública cuando el tratamiento es necesario para los fines citados en el artículo 9.2.h o por las razones de interés público citadas en el artículo 9.2.i[23] y se cumplen las condiciones del apartado 9.3[24]; con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, cuando el derecho al olvido pudiera hacer imposible u obstaculizar gravemente los objetivos del tratamiento; y para la formulación, el ejercicio o la defensa de reclamaciones; supuestos que pueden establecerse legalmente.
Como puede verse, las excepciones son muchas y, por tanto, hay muchos casos en los que el tratamiento de datos mediante la tecnología BC podría no suponer un conflicto con el Reglamento.

4.2.*Posibles soluciones*

Una de las soluciones que se han propuesto para resolver los posibles conflictos con el derecho a la protección de datos es la de un BC editable. En este sentido, ATENIESE, MAGRI, VENTURI y ANDRADE han "formado equipo con Accenture [Acc] para desarrollar un prototipo" en el que "entidades de confianza pueden editar bloques siempre y cuando estén actuando según normas de gobernanza acordadas"[25].
Otro factor a tener en cuenta es la "seudonimización", que el Reglamento define como "el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se

23 "Artículo 9
Tratamiento de categorías especiales de datos personales
1. Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física.
2. El apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes:
(...)
h) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3;
i) el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional".

24 "Los datos personales a que se refiere el apartado 1 podrán tratarse a los fines citados en el apartado 2, letra h), cuando su tratamiento sea realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con el Derecho de la Unión o de los Estados miembros o con las normas establecidas por los organismos nacionales competentes, o por cualquier otra persona sujeta también a la obligación de secreto de acuerdo con el Derecho de la Unión o de los Estados miembros o de las normas establecidas por los organismos nacionales competentes".

25 Ateniese, G., Magri, B., Venturi, D., Andrade, E., "Redactable Blockchain– or –Rewriting History in Bitcoin and Friend", versión completa del artículo que apareció de manera abreviada en las actas del 2nd IEEE European Symposium on Security and Privacy – EuroS&P2017, 2017, p. 6: "We teamed up with Accenture [Acc] to develop a prototype (...) Trusted entities can edit blocks as long as they are acting on agreed rules of governance".

atribuyan a una persona física identificada o identificable" (artículo 4.5).
Esto podría permitir que se tratasen de manera separada los datos, de forma que aquellos que no permitan su atribución a una persona física podrían quizás almacenarse mediante BC. MOSER afirma que "generalmente, un modo de cumplir el RGPD es usar exclusivamente datos seudónimo en el blockchain y abstenerse de procesar información personalmente identificable en el blockchain. Esta última puede almacenarse y procesarse fuera del blockchain junto con, o de manera separada a, una tabla de referencia.
Si el controlador debe eliminar cualquier dato de un individuo, simplemente borra la información personalmente identificable clara, de manera que es incapaz de seguir creando una referencia al individuo"[26].
Sin embargo, sobre los seudónimos se ha dicho que "cuando los datos se dejan completamente anónimos, ya no equivalen a datos personales y, por tanto, no entran dentro del ámbito del marco legal. Sin embargo, cuando los datos se dejan seudónimos, siguen contando como datos personales ya que la identificación indirecta de una persona natural mediante un identificador sigue siendo posible"[27]. También la Opinión 05/2014 sobre las Técnicas de Anonimización, del Grupo de protección creado por la Directiva 95/46/CE afirma que la "seudonimización consiste en reemplazar un atributo (típicamente un atributo único) en un registro por otro. Es, por tanto, todavía probable que se identifique a la persona natural de manera indirecta"[28]. No obstante, MOURBY, M., MACKEY, E., ELLIOT, M., GOWANS, H., WALLACE, S.E., BELL, J., SMITH, H., AIDINLIS, S., KAYE, J., aunque dentro del contexto específico de la investigación administrativa de datos, opinan que "incluso los datos personales que se han sometido a un proceso de seudonimización del RGPD pueden no ser datos personales cuando se comparten con terceras partes" y "el hecho de que los individuos puedan ser seleccionados (i.e. diferenciados individualmente) dentro de "los datos seudonimizados" no es suficiente para volver estos datos personales"[29]. Los autores mencionados opinan que "el enfoque debería centrarse en la relación entre las partes y si esas relaciones permiten al investigador identificar los datos"[30], por lo que la solución propuesta podría aplicarse a un ámbito limitado.
Tanto en la aplicación del derecho como en la interpretación de las excepciones a este, algunas de ellas bastante indeterminadas (por ejemplo, misión de interés público, libertad de expresión...), debe utilizarse el principio de proporcionalidad para favorecer la aplicación del derecho fundamental y limitar el uso del BC en lo que suponga lesión de ese derecho, teniendo en cuenta los principios a

26 MOSER, J., "The Application & Impact of the European General Data Protection Regulation on Blockchains", *R3*, 2017, p. 8: "Generally, a way to comply with the GDPR is to exclusively use pseudonymous data in the blockchain and refrain from processing clear PII in the blockchain. The latter can be stored and processed outside the blockchain together with or separate from a reference table.
If the controller must delete any data of an individual, he simply deletes clear PII, so that he is unable to create a reference to the individual anymore".

27 FINCK, M., "Blockchains and Data Protection in the European Union", *Max Planck Institute for Innovation and Competition Research Paper No. 18-01*, 2017, p. 10: "Where data is rendered completely anonymous, it no longer amounts to personal data and thus falls outside the scope of the legal framework. Where data is rendered pseudonymous, however, it continues to qualify as personal data as the indirect identification of a natural personal by an identifier remains possible".

28 DATA PROTECTION WORKING PARTY, ARTICLE 29, *Opinion 05/2014 on Anonymisation Techniques*, 0829/14/EN WP216, 2014, p. 20: "Pseudonymisation consists of replacing one attribute (typically a unique attribute) in a record by another. The natural person is therefore still likely to be identified indirectly".

29 MOURBY, M., MACKEY, E., ELLIOT, M., GOWANS, H., WALLACE, S.E., BELL, J., SMITH, H., AIDINLIS, S., KAYE, J., "Are 'pseudonymised' data always personal data? Implications of the GDPR for administrative data research in the UK", Computer Law & Security Review 34, 2018, 222–233, p. 227: "even data which have undergone a process of GDPR pseudonymisation may not be personal data when shared with third parties" y íbid., p. 228: "Therefore, the fact that individuals can be singled out (i.e. individually differentiated) within 'pseudonymised data' is not sufficient to render these data personal".

30 Íbid., p. 225: "the focus should be on the relationship between the parties, and whether these relationships enable the researcher to identify the data".

proteger y el objetivo que se persigue al utilizar BC, que era inicialmente más reducido y con menos potencialidad de vulneración del derecho, pero que está experimentando una creciente tendencia expansiva. Un mayor uso del BC, antes limitado a sectores más específicos, implica una mayor posibilidad de lesión del derecho a la protección de datos. Un interés puramente económico o la justificación basada en dificultades técnicas para cumplir con la regulación no pueden suponer la desprotección de los derechos fundamentales que protege el Reglamento.

5. Conclusiones

Como hemos visto, la tecnología BC parece colisionar con el derecho al olvido tal y como está regulado en el Reglamento General de Protección de Datos. Sin embargo, hemos argumentado que esta colisión no es nueva, sino que ya podía producirse con respecto a la Directiva 95/46/CE, durante su periodo de vigencia, ya que esta, aunque no establecía un derecho al olvido así denominado, sí establecía, bajo el derecho de acceso, la posibilidad de obtener la supresión o modificación de los datos en determinados supuestos, más limitados que aquellos recogidos en el Reglamento General de Protección de Datos. Este derecho fue posteriormente interpretado extensivamente en el caso Google por el Tribunal de Justicia de la Unión Europea.

Esta problemática no es, por tanto, nueva, si bien el derecho al olvido ha cobrado una mayor relevancia en los últimos años, debido a la expansión del Internet y a la mayor cesión de datos que se produce en este medio. Por otra parte, también la tecnología BC es relativamente nueva, por lo que sólo ahora cabe plantearse un conflicto entre esta y el derecho al olvido.

Hemos visto, sin embargo, que hay numerosas excepciones al derecho al olvido en la legislación, lo que permite que se utilice esta tecnología en diversos ámbitos.

Además, se han hecho varias propuestas para evitar esta colisión. En primer lugar, la de un BC editable. En segundo lugar, una solución menos evidente, puesto que hay opiniones que no la consideran posible, es la de utilizar seudónimos en el almacenamiento de datos, si bien se propone para un ámbito limitado o bien mediante el almacenamiento de la información que permita identificar a las personas fuera del BC, en el que se sólo se almacenarían datos seudónimos.

Por último, debe utilizarse el principio de proporcionalidad para favorecer la aplicación del derecho fundamental y limitar el uso del BC si este supone una lesión del derecho, tanto en la aplicación general del derecho al olvido como en la interpretación de sus excepciones.