Facultad de Derecho

EL DERECHO AL OLVIDO EN EL CONTEXTO DE BLOCKCHAIN Y DEL RGPD

Autor: Lucía López López
5º E-3 B

Tutor: Javier Wenceslao Ibáñez Jiménez

Área de Derecho Mercantil

MADRID | 2024

RESUMEN

Este estudio examina la compatibilidad de la tecnología blockchain con el Reglamento General de Protección de Datos, enfocándose en el derecho al olvido. Analiza las características de la blockchain y las dificultades que presenta para cumplir con este principio, especialmente debido a su inmutabilidad y la dificultad para determinar al responsable en una red descentralizada. En proceso, se analizan y proponen métodos para alcanzar la compatibilidad desde enfoques normativos y técnicos. El trabajo concluye destacando la necesidad de una colaboración estrecha entre juristas y tecnólogos para desarrollar una solución integral que equilibre el avance tecnológico con la adaptación a la normativa.

Palabras clave: DLT, blockchain, derecho al olvido, RGPD.

ABSTRACT

This study examines the compatibility of blockchain technology with the General Data Protection Regulation, focusing on the right to be forgotten. It analyzes the characteristics of blockchain and the difficulties it presents in complying with this principle, particularly due to its immutability and the challenge of identifying the responsible party in a decentralized network. In this process and methods are proposed to achieve compatibility from both normative and technical approaches. The study concludes by highlighting the need for close collaboration between legal experts and technologists to develop a comprehensive solution that balances technological advancement with regulatory compliance.

Key words: DLT, blockchain, right to be forgotten, GDPR.

ÍNDICE

LISTADO DE ABREVIATURAS

AEPD	Agencia Española de Protección de Datos
ARCO	Derechos de acceso, rectificación, control y oposición
CCITT	Comité Consultivo Internacional Telegráfico y Telefónico
CNIL	Comission Nationale de l'Informatique et de Libertés
DAO	Organización Autónoma Descentralizada
DLT	Distributed Ledger Technology (tecnología de registro distribuido)
EDPB	European Data Protection Board (Comité Europeo de Protección de Datos)
ITU	International Telecommunication Union (Unión Internacional de Telecomunicaciones)
ITU-T	Sector de normalización de las comunicaciones
(ITU –T) FG DLT	Focus Group on Application of Distributed Ledger Technology
ISO TC	International Organization for Standardization - Technical Committee (Organización Internacional de Normalización - Comité Técnico)
LOPD	Ley Orgánica de Protección de Datos
LOPGDD	Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales
PCH	Policy- based Chameleon Hash
PKI	Public Key Infraestructure (Infrestructura de clave pública)
RGPD/GRPD	Reglamento General de Protección de Datos
SNS	Social Networking Services (servicio de red social)
STOA	Science and Technology Options Assestment (Panel del Parlamento Europeo para la Ciencia y la Tecnología

CAPÍTULO I. INTRODUCCIÓN.

1. JUSTIFICACIÓN DEL TEMA Y OBJETIVOS DEL TRABAJO.

La tecnología de registros distribuidos — *distributed ledger technology*; en adelante, DLT — ha desarrollado gran importancia en la última década, prometiendo revolucionar la forma en que se gestiona la información. Sin embargo, sus características intrínsecas también presentan desafíos significativos.

La relevancia de investigar estos aspectos radica en dos factores clave[1]: primero, el impacto abarcador de esta tecnología, que influye en todos los sectores comerciales e industriales, además de las interacciones entre individuos y empresas; segundo, debido a que su implementación trasciende los principios y regulaciones vigentes del derecho de internet[2].

Este estudio aborda una de las esferas más desafiantes para el legislador: los derechos de protección de datos. A medida que avanzamos hacia una sociedad donde la tecnología desempeña un papel cada vez más central, es imperativo revisar y adaptar nuestras leyes y regulaciones para asegurar que protejan adecuadamente los derechos individuales eficazmente, sin obstaculizar el progreso tecnológico.

Este trabajo se sustenta en el marco del Reglamento General de Protección de Datos[3] (en adelante, RGPD) y los derechos ARCO[4], explorando cómo la característica distintiva de la blockchain —la inalterabilidad— puede entrar en conflicto con las expectativas y necesidades de privacidad y olvido en la era digital.

---

[1] Ibáñez Jiménez, J. W, *Derecho de blockchain y de la tecnología de registros distribuidos*, Aranzadi, Navarra, 2018, p. 19.

[2] Barrio Andrés, M. *Fundamentos del derecho de internet*, Centro de Estudios Políticos y Constitucionales, Madrid, 2020

[3] 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 (DOUE, núm. 119, de 4 de mayo de 2016, pp. 1-88)

[4] El RGPD amplía los derechos ARCO tradicionales (acceso, rectificación, cancelación, oposición) con la inclusión del derecho a la portabilidad, la limitación del tratamiento y el derecho al olvido, introduciendo la nueva nomenclatura ARCO-POL.

Ante el ritmo acelerado de la evolución tecnológica, un conocimiento profundo del ordenamiento jurídico actual debe incluir no solo las normas vigentes, sino también las tecnologías emergentes y los desafíos que estas representan. De este modo, el trabajo incorpora el estudio de estrategias legales que permitan la coexistencia armoniosa entre derecho y tecnología, además de otras técnicas alternativas que permitan el ejercicio del derecho sin conflictos.

En definitiva, este trabajo presenta un análisis exhaustivo orientado a asegurar que el desarrollo tecnológico beneficie a la sociedad en su conjunto, sin comprometer los derechos y libertades fundamentales. Los objetivos específicos del trabajo son los siguientes:

- Analizar la normativa aplicable a la tecnología de registros distribuido desde la perspectiva del tratamiento de datos personales y, en particular, el derecho al olvido. A este efecto, considerar el encaje de los datos tratados en el blockchain bajo el ámbito de aplicación del RGPD y la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPGDD)[5].

- Explorar la tensión existente entre la inmutabilidad de la cadena de bloques y las exigencias del derecho al olvido, identificando los desafíos legales y técnicos implicados.

- Contribuir al debate académico y legislativo sobre la necesidad de adaptar el marco legal existente para abordar las nuevas realidades tecnológicas, asegurando un equilibrio entre innovación y protección de derechos fundamentales.

2. METODOLOGÍA EMPLEADA.

La metodología de este trabajo ha sido cuidadosamente diseñada para analizar de manera detallada y precisa la compleja relación entre la tecnología de registros distribuidos y el derecho al olvido.

El trabajo se cimienta sobre las normativas de la Unión Internacional de Telecomunicaciones (ITU) y Organización Internacional de Normalización (ISO), que establecen estándares

[5]Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (BOE, núm. 294, de 6 de diciembre de 2018).

internacionales para esta tecnología, a través del Grupo de Trabajo de Aplicación de Tecnología de Registros Distribuidos (ITU-T FG DLT) y el Comité Técnico ISO/TC 307, respectivamente. Estos estándares proporcionan un marco esencial para asegurar la precisión técnica y la correcta interpretación de términos, facilitando una adecuada comprensión de las implicaciones legales y tecnológicas.

Asimismo, este enfoque se beneficia de la supervisión y orientación del Prof. Dr. Ibáñez Jiménez, fundador de Alastria —primera blockchain pública permisionada nacional— y participante activo en la estandarización global de la tecnología blockchain.

Este estudio aplica un método exegético para interpretar de manera detallada y sistemática legislaciones vigentes relacionadas con el derecho al olvido: el RGPD y la LOPGDD. Este enfoque permite alcanzar una comprensión efectiva de los textos legales y entender su alcance y limitaciones en el contexto de la aplicación a tecnologías emergentes como la DLT.

En el análisis de las soluciones propuestas para alcanzar la compatibilidad tecnológica y legislativa, se adopta una perspectiva socioeconómica que priorice la eficiencia. Mediante la evaluación de las consecuencias reales de las normas existentes, se busca predecir los posibles efectos de las soluciones proyectadas. Así, se consideran las repercusiones económicas de cada alternativa, buscando, en consonancia con la protección de los derechos humanos, la optimización de recursos y el mayor bienestar social a largo plazo. De esta forma, el derecho se convierte en una herramienta proactiva para impulsar el progreso social y económico y se asegura la adopción de los medios más idóneos para su implementación[6].

Este enfoque multidisciplinario permite una exploración holística de la interacción entre tecnología y ley. Así, el estudio no solo busca identificar los retos y tensiones actuales, sino también explorar soluciones viables y estrategias de conciliación entre la innovación tecnológica y los derechos individuales a la privacidad y al olvido.

[6] Posner, R. A. *Economic analysis of law*. Aspen Publishing, 2014.

CAPÍTULO II. LA TECNOLOGÍA DLT Y LA BLOCKCHAIN.

1. DEFINICIÓN, PUNTOS CLAVE Y FUNDAMENTO.

Los estándares globales ITU e ISO describen desde una perspectiva técnica en qué consiste la DLT y cómo opera por medio de sus principales componentes[7].

Así, se configura como un sistema registral que, distribuido y sincronizado, produce una base de datos compartidos sin necesidad de intervención de una autoridad central. El núcleo de la DLT radica en su arquitectura descentralizada, valiéndose de una red de nodos independientes que, por medio de un mecanismo de consenso[8], permiten que se registre la información de manera simultánea y uniforme en toda la red. La responsabilidad y el mantenimiento de la información son colectivos, dando lugar a la creación de un "sistema de registros"[9] en el que la información es confiable y segura[10].

La DLT comprende diversas tecnologías de registros distribuidos, siendo la blockchain la más destacable. Esta constituye una forma específica de DLT que estructura la información en bloques que se enlazan cronológicamente y de forma consecutiva al bloque anterior mediante un hash criptográfico único. De esta manera, se forma una secuencia continua por la cual solo se podría agregar información a la cadena. Este proceso se logra mediante la inclusión, en cada nuevo bloque, del hash identificativo del bloque anterior. El resultado es la obtención de un historial de transacciones trazable e irreversible, dado que cualquier

[7] ITU-T Focus Group on Application of Distributed Ledger Technology: *Technical Specification FG DLT D1.1. Distributed ledger technology terms and definitions*, International Communication Union (ITU), 3 de marzo de 2024 (disponible en https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d11.pdf; última consulta 1/03/2024).

[8] Los mecanismos de consenso son protocolos que establecen el proceder de los miembros del colectivo que usa la DLT, asegurando que se pongan de acuerdo sobre la validez de las entradas en el ledger y el estado actual del mismo.

[9] La función registral deviene real y adquiere una función jurídica por cuanto supone la anotación y el almacenamiento de datos en internet permitiendo su acceso posterior en lo que adquiere una función probatoria (Cfr. Ibáñez Jiménez, J. W., *Op. cit.*, p. 16).

[10] La DLT combina una arquitectura descentralizada que mejora la resistencia a fallos en el sistema y ataques cibernéticos (ya que el punto central se sustituye por varios componentes independientes), una descentralización política elimina el riesgo de manipulación por parte de la autoridad central que ejerce el control y una centralización lógica por cuanto la existencia de un consenso dota al registro de coherencia e integridad. (Buterin, V., "The Meaning of Decentralization". *Medium*, vol. 6, 2017 (disponible en https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274; última consulta 3/03/2024).

intento de alterar bloques anteriores sería detectado por la red, sin superar el protocolo de consenso establecido[11].

La exposición de los principales caracteres de DLT y blockchain revelan su potencial revolucionario, resaltando una diversidad de beneficios. Su aptitud para garantizar la autenticidad y la trazabilidad de los datos tiene el potencial de aumentar significativamente la eficiencia y minimizar los costos en numerosos campos. Pronto se hizo evidente el potencial de esta tecnología para redefinir profundamente las prácticas comerciales y las interacciones sociales, impulsando su evolución en alcance y complejidad, lo que permite diferencia distintas fases de desarrollo.

En sus comienzos, la Blockchain 1.0 se ocupó de las monedas digitales como Bitcoin, simplificando las transacciones financieras. La fase de Blockchain 2.0 amplió el uso de la tecnología a la formación de contratos inteligentes habilitando un espectro más amplio de aplicaciones económicas, abarcando todo desde el manejo de valores hasta el de hipotecas o préstamos. Por su parte, Blockchain 3.0 representa la incursión en esferas no financieras, impactando áreas como el gobierno, la salud y la cultura, promoviendo la regulación y la gobernanza de procesos descentralizados[12].

2. CARACTERES GENERALES DE LA BLOCKCHAIN Y SU IMPACTO REGULATORIO.

Las diversas aplicaciones de la blockchain resaltan su importancia en el manejo de datos y la sensibilidad de los mismos en lo que respecta a las operaciones y la privacidad de los individuos. Mientras la DLT se presenta como un mecanismo altamente seguro y transparente, algunos de estos caracteres presentan desafíos regulatorios. Desde la perspectiva de la ITU, estos se analizan agrupándolos según las propiedades clave de la DLT[13].

[11] Ibáñez Jiménez, J. W., *Op. cit.,* pp. 22-23.
[12] Swan, M., *Blockchain. Blueprint for a new economy*, O'Reilly, 2015.
[13] ITU-T Focus Group on Application of Distributed Ledger Technology: *Technical Specification FG DLT D 4.1 Distributed ledger technology regulatory framework*, International Communication Union (ITU), 10 de marzo de 2024 (disponible en https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d14.pdf; última consulta 30/05/2024)

Aunque algunas propiedades están relacionadas de una manera más directa con los desafíos del RGPD, conviene abordar todas ellas para obtener una comprensión completa y detallada desde la óptica del derecho al olvido que posteriormente nos permita desarrollar las estrategias o mecanismos que adecuados para asegurar una compatibilidad legal y técnica.

1) La primera propiedad hace referencia al carácter distribuido y compartido de la red. Cada nodo integrante de la red se comunica con los demás directamente en un modo *peer-to-peer* (P2P). En ausencia de una autoridad central, los nodos están gobernados por reglas que emergen de las operaciones de la red. Esto complica la identificación de un único responsable del tratamiento de los datos, a la vez que la distribución transfronteriza de los datos plantea dificultades para la determinación de la ley aplicable y el cumplimiento de estándares, especialmente cuando leyes locales puedan entrar en conflicto entre sí o ser inconsistentes.

2) Autonomía y responsabilidad conforman la segunda propiedad. Las transacciones en sistemas de DLT pueden ejecutarse de manera autónoma bajo condiciones predefinidas en el sistema. Los contratos inteligentes permiten automatizar procesos que típicamente requieren acuerdos legalmente vinculantes, integrando decisiones humanas a partir de los activos registrados en la blockchain. Sin embargo, la tradición jurídica ha evidenciado como la redacción de reglas que prevean todas las contingencias futuras es imposible, surgiendo situaciones que pueden no reflejar la intención de los autores. Esta limitación es extrapolable a los códigos de los contratos inteligentes, cuya ejecución automatizada podría ignorar nuevos elementos externos a la cadena y resultar en acciones que, en ausencia de un juicio interpretativo humano, podrían contravenir a las leyes[14].

   Los retos regulatorios relacionados con esta característica remiten de nuevo a abordar la responsabilidad en casos de infracción de la protección de datos y la autenticidad del consentimiento, factores que están estrechamente conectados con la facultad de eliminar esos datos del sistema.

[14] Yeung, K., Regulation by Blockchain: The Emerging Battle for Supremacy between the Code of Law and Code as Law, *The Modern Law Review*, vol. 82, n. 2, pp. 207-209.

3) Resistencia a la manipulación. La DLT utiliza técnicas criptográficas avanzadas, incluyendo la firma digital de entradas y el encadenamiento de datos mediante hashes criptográficos, lo que implica que cualquier intento de modificar una entrada exige alterar todas las entradas subsiguientes. Esto permite crear un registro prácticamente inalterable en el que ningún nodo individual contiene un conjunto completo de transacciones, fortaleciendo la resistencia al sabotaje al distribuir la responsabilidad entre múltiples nodos descentralizados, impidiendo con los mecanismos de consenso que una sola entidad convenza a todos de modificar sus registros.

Uno de los principales desafíos que presenta esta tecnología en relación con el derecho al olvido es la dificultad técnica para eliminar datos, presupuesto esencial de la regulación legal de este derecho.

Asimismo, las técnicas criptográficas desempeñan un papel crucial en la determinación del cumplimiento con los altos estándares de protección de datos que establece el Reglamento.

4) Mecanismos de incentivos y activos digitales. La encriptación de los datos conlleva unos costes asociados y motiva la dotación de incentivos por su ejecución[15]. La incentivación juega un papel crucial en la gobernanza de las redes de DLT, siendo esencial para alinear los objetivos de los participantes con el funcionamiento eficiente de la red. Al mismo tiempo, no solo estimulan la participación activa en la DLT, sino que también promueven la responsabilidad social. Esto amplía el impacto de los incentivos más allá de los beneficios económicos, generando efectos sociales positivos.

Los incentivos generalmente toman la forma de tokens[16], lo cual pueden complicar la transparencia y el manejo del consentimiento, así como requerir especificidades en su tratamiento bajo el RGPD.

[15] Son costes asociados al procedimiento de cifrado de datos, además del coste eléctrico y la amortización del equipo informático, el coste asociado a la supervisión humana de las operaciones. Ibáñez Jiménez, J. W., *Op. cit.*, p. 16.

[16] Representación de cualquier valor o activo sobre una cadena de bloques que, siendo fungible y negociable, refleja una forma de riqueza en dicho sistema. Boar, A., "Efectos de la tecnología blockchain en el sector financiero" en Profit (ed.), ACCID (coord.), *Blockchain, bitcoin y criptomonedas: bases conceptuales y aplicaciones prácticas*, Bresca, Barcelona, 2018, pp. 19-20.

5) La última propiedad hace referencia a naturaleza de las plataformas DLT en términos de manejo de la validación de transacciones y participación en la red: transparencia, confianza y anonimato.

Estas plataformas tienen desafíos inherentes en equilibrar la transparencia (entendida como apertura y visibilidad) con la privacidad. La naturaleza abierta de la DLT contrasta con las exigencias de privacidad establecidas por regulaciones como el RGPD, que prioriza el control individual sobre la información personal. Sin embargo, la reducción de esta visibilidad en aras de mayores niveles de privacidad puede constituir un tema delicado en materia de auditoría o para el seguimiento de actividades ilícitas[17].

Ante esta situación, se deben mencionar los trabajos en el desarrollo de técnicas de anonimización y tecnologías que mejoran la privacidad, cuyo análisis es objeto de este trabajo.

El alcance de los principios de transparencia, confianza y anonimato varía considerablemente según se trate de redes permisionadas o sin permiso, de acuerdo con el tipo de control y acceso que cada red implementa. Mientras que en las primeras la toma de decisiones se deriva de un tercero de confianza (TTP) que otorga acceso al contenido a los participantes en la red, en las redes sin permiso todos los participantes pueden actuar libremente sin necesidad de una autentificación formal. Esta distinción evidencia la existencia de diferentes niveles de confidencialidad y confianza, así como plantea cuestiones adicionales en materia de responsabilidad que se abordarán más adelante.

CAPÍTULO III. REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

1. OBJETO Y PRINCIPIOS FUNDAMENTALES

La evolución tecnológica ha propiciado la redefinición de conceptos legales fundamentales, como la noción de datos personales.

La creciente capacidad de vigilancia y control ofrecida por las nuevas tecnologías ha motivado la necesidad de una revisión normativa, culminando en la aprobación del

[17] En este sentido, la FATF (*Financial Action Task Force*) ha expresado reiteradamente su preocupación de que las criptomonedas, debido a su gran anonimato, puedan ser usadas en actividades criminals, instando a los países a implementar sistemas de supervisión que armonicen la privacidad con las demandas legales.

Reglamento (UE) 2016/679, comúnmente conocido como el Reglamento General de Protección de Datos (RGPD).

Esta normativa deroga la Directiva 95/46/CE[18], que sentaba las bases para la libre circulación de datos en la Unión Europea en beneficio del mercado interior[19]. A pesar del éxito de la Directiva en implementar un sistema uniforme de protección de datos, su enfoque armonioso a menudo ponía en segundo plano la protección efectiva. Esto resultaba en debilidades, como el amplio margen de discrecionalidad otorgado a los Estados miembros, lo que conducía a la fragmentación nacional de la normativa de protección de datos, particularmente en lo que respecta a las transferencias internacionales, esenciales en una economía global[20]. Además, el progreso de la economía digital y la penetración social de las nuevas tecnologías han subrayado la necesidad creciente de un marco de protección de datos robusto y coherente.

A nivel nacional, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) adapta la legislación al RGPD derogando la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD)[21] [22].

El RGPD retoma y amplía muchos de los conceptos, principios y obligaciones que ya establecía la Directiva europea y las legislaciones nacionales correspondientes, añadiendo a su vez obligaciones adicionales. Incorpora dos enfoques fundamentales: los principios del tratamiento[23] y la obligación del responsable y del encargado[24].

---

[18] 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 respeta al tratamiento de datos personales y a la libre circulación de estos datos (DOCE, núm. 281, de 23 de noviembre de 1995, pp. 31-50.)

[19] Rallo Lombarte, A. V. "El nuevo derecho de protección de datos". *Revista Española de Derecho Constitucional*, n. 116, pp. 45-74 (disponible en https://doi.org/10.18042/cepc/redc.116.02; última consulta 7/03/2024)

[20] *Íbid.*

[21] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (BOE núm. 298, de 14 de diciembre de 1999).

[22] La aplicabilidad directa del reglamento desplaza con su entrada en vigor la normativa nacional la normativa incompatible, pero el principio de seguridad jurídica requiere que esta sea explícitamente derogada por normas internas de igual rango legal, asegurando la coherencia legal conforme a precedentes del TJUE Sentencia del Tribunal de Justicia (Sala Segunda), Comisión v. España, C-546/03, de 23 de febrero de 2006 [versión electrónica - base de datos Eur-Lex. Ref. EU:C: 2006:132]. Fecha de la última consulta: 15 de abril de 2024.

[23] *Vid.* Artículo 5 RGPD. *Principios relativos al tratamiento.*

[24] Troncoso Reigado, A. "Del Principio de seguridad de los datos al derecho a la seguridad digital", *Economía industrial*, n 410,2018, p. 127.

Estas dos dimensiones servirán como marco en este trabajo para explorar la integración de la tecnología DLT dentro de este reglamento.

2. ÁMBITO DE APLICACIÓN TERRITORIAL

El RGPD adopta un enfoque amplio y detallado en relación con su ámbito de aplicación.

El artículo 3 del RGPD define su ámbito de aplicación territorial con una óptica extensa que trasciende las fronteras de la Unión Europea a través de dos criterios principales.

Primero, utiliza un enfoque funcional basado en la presencia de un "establecimiento" en la UE[25]. De acuerdo con este, si las operaciones de una entidad o responsable se llevan a cabo dentro del ámbito de la Unión, independientemente de si el procesamiento de datos tiene lugar dentro o fuera de ella, quedan sometidas al ámbito de aplicación del Reglamento[26].

Segundo, el criterio de *"targeting"* expande el alcance del RGPD enfocándose en el procesamiento de datos personales de individuos que residen en el territorio de la UE. Este criterio se refiere a entidades y responsables que, operando desde fuera de Europa, dirigen sus actividades hacia residentes de la UE, ya sea ofreciendo bienes y servicios (art. 3.2 a)[27] o monitoreando el comportamiento de los individuos dentro de la UE por internet o por cualquier medio habilitado para ello (art. 3.2 b)[28].

Por último, el RGPD también se extiende a entidades que, sin estar establecidas en la UE, están sujetas a la legislación de los Estados miembros por obligaciones derivadas del derecho internacional público (art. 3.3).

---

[25] Considérese un enfoque flexible para determinar un establecimiento, donde no se requiere le presencia física o registro formal. En su lugar, se evalúan factores como el grado de estabilidad y la efectividad con la que una empresa desarrolla sus actividades económicas (Considerando 22 RGPD). *Vid*. STJUE C- 230/14 Weltimmo.

[26] *Vid.* Art. 3.1 RGPD

[27] Voluntad de dirigir esa oferta a residentes europeos como elemento delimitador del supuesto de hecho ponderando indicios como uso de la lengua, mención de clientes en la UE o uso de moneda local (Considerando 23 RGPD). *Vid*. STJUE C-585/08 Pammer and Hotel Alpenho.

[28] Domenech, J. J. G., "La aplicación del nuevo RGPD en el contexto del tratamiento de datos en la UE", *Revista Lex Mercatoria,* n. 6, 2017, pp. 37-42 (disponible en https://doi.org/10.21134/lex.vi.53; última consulta 16/04/2024).

La aplicabilidad territorial del Reglamento no representa un desafío para las redes privadas permisionadas que operan a través de entidades específicas o consorcios, ya que su estructura controlada permite determinar claramente su sujeción al mismo[29]. En contraste, las redes no permisionadas enfrentan mayores complicaciones debido a la descentralización de sus nodos operativos. La flexibilidad interpretativa del concepto de establecimiento y la capacidad de estas tecnologías para crear una presencia virtual facilitan la justificación de la aplicabilidad del RGPD, bastando la realización de actividades como transacciones o la ejecución de contratos inteligentes por medio de la infraestructura de blockchain. Este argumento se fortalece con el criterio de "*targeting*", que minimiza la importancia de la ubicación del responsable del tratamiento[30].

3. ÁMBITO DE APLICACIÓN MATERIAL.

El RGPD aborda la gestión de datos personales, estableciendo una clara separación con los datos no personales, que son regulados bajo el Reglamento 2018/1807 en el contexto del mercado digital de la Unión Europea[31].

La normativa del RGPD, recogida en el artículo 2, contempla varias excepciones en su aplicación, como son las operaciones fuera de la UE, determinadas actividades gubernamentales, usos estrictamente personales o domésticos, y las funciones de las autoridades en cuanto a la prevención y detección de delitos. Además, cabe indicar que el RGPD se aplicará exclusivamente a individuos, excluyendo a las personas jurídicas y los datos de personas ya fallecidas, cuyo tratamiento queda a discreción de las leyes particulares de cada Estado miembro[32].

---

[29] El binomio privado-público hace referencia quién puede acceder a la DLT, mientras que permisionada-sin permiso se refiere a la necesidad de obtener permisos específicos para mantener y operar un nodo en dicho sistema**.** Op. Cit. ITU-T Focus Group on Application of Distributed Ledger Technology: *Technical Specification FG DLT D1.1*

[30] Hernández Peña, J. C., "Tecnologías de registro distribuido y protección de datos personales. Compatibilidad y conflictos al hilo del Reglamento general de Protección de Datos" Valpuesta, E. & Hernández Peña, J. C (coord.), Blockchain: aspectos jurídicos de su utilización, Wolters Kluwer, Madrid, 2022, p. 75

[31] Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo de 14 de noviembre de 2018 relativo a un marco para la libre circulación de datos no personales en la Unión Europea (DOUE, núm. 303, de 28 de noviembre de 2018, pp. 59 a 68).

[32] *Vid*. considerandos 14 y 27

El artículo 4.1. del RGPD establece que los datos personales comprenden "toda información sobre una persona física identificada o identificable", ya sea directa o indirectamente, sin importar el medio o formato en el que esta se presente. Por su parte, el considerando 26 aclara que la información que no pueda vincularse o no permita identificar a un individuo, es decir, información anónima, no está sujeta a las disposiciones del RGPD.

Asimismo, el nuevo Reglamento introduce el concepto de seudonimización, un método de gestión de datos en el que la información almacenada se sustituye por un identificador (seudónimo). El RGPD fomenta esta práctica como una medida para mitigar los riesgos en el tratamiento de datos[33]. Sin embargo, incluso cuando los datos personales están seudonimizados, pueden vincularse a una persona específica mediante el uso de información adicional o de terceros. Por lo tanto, estos datos están sujetos a la regulación del RGPD.

A diferencia de los datos que se consideran anónimos, los cuales están protegidos únicamente por la necesidad de un proceso de anonimización robusto para prevenir la averiguación de la identidad, los datos seudonimizados cuentan con cuatro tipos de garantías bajo el RGPD. La primera de ellas es la exigencia de un proceso de seudonimización diseñado para prevenir la identificación sin información adicional. Además, el RGPD impone restricciones en cuanto a los objetivos del tratamiento, la duración de la conservación de los datos y su divulgación. Se añaden garantías adicionales según el riesgo que el tratamiento pueda representar para los derechos y libertades individuales. Por último, se establecen medidas técnicas y organizativas para evitar violaciones de datos, abarcando tanto los datos seudonimizados como cualquier información adicional involucrada[34].

Debido a la complejidad de los estándares establecidos por el Reglamento, la incorporación de los registros distribuidos dentro de su marco normativo puede no ser tan clara ni directa. Los datos pueden estar almacenados en formato de texto plano, en cuyo caso su sujeción al RGPD sería indiscutible, o bien pueden estar protegidos mediante la implementación de técnicas y medidas de seguridad avanzadas[35]. En este último caso, es relevante mencionar el

[33] *Vid*. considerandos 28 y 29.
[34]AEDP, "Anonimización y seudonimización", 2021 (disponible en https://www.aepd.es/prensa-y-comunicacion/blog/anonimizacion-y-seudonimizacion; última consulta 15/04/2024).
[35] Hernández Peña, J. C., *Op. cit*. p. 84.

uso de métodos criptográficos y funciones hash como parte de las estrategias de protección de datos empleadas.

La tecnología blockchain emplea criptografía doble, también denominada criptografía asimétrica (en contraposición la criptografía simétrica)[36]. En este sistema se utilizan dos claves distintas: una pública, que se comparte con otros usuarios de la red para identificar al emisor y verificar su firma; y una privada, empleada por el usuario para realizar operaciones en la blockchain, incluyendo la inserción de datos[37]. Cuando un usuario transmite un mensaje, utiliza la clave pública del destinatario para cifrarlo. Solo el destinatario, utilizando su clave privada única, puede descifrar este mensaje, lo que garantiza que únicamente la persona designada para ello tenga acceso al contenido[38].

En muchas situaciones, las claves públicas son emitidas por entidades externas dentro de las infraestructuras de clave pública (PKI)[39]. Esto implica que terceras partes llevan a cabo la identificación del usuario y registran esta información junto con datos personales en un certificado digital, un procedimiento que, en algunos casos, es obligatorio por ley. Aunque no se puede derivar directamente la clave privada de la pública, sí es posible establecer una conexión entre ambas: únicamente la clave privada correspondiente puede descifrar el dato cifrado con la clave pública. Esta dinámica permite que terceros puedan llegar a identificar al usuario vinculado a una clave pública específica[40].

En lo que respecta al proceso de hashing, se utiliza para convertir cualquier tipo de entrada de datos, independientemente de su formato, en una secuencia alfanumérica de longitud fija. Más adelante en este estudio se analizará con mayor detalle la función hash y su naturaleza

[36]En la criptografía simétrica, se emplea una única clave que tanto el emisor como el receptor deben conocer para cifrar y descifrar mensajes de manera segura, sin que terceros tengan conocimiento o intervengan en el proceso. Puig Pascual, A. "Identidad Digital Sobre «Blockchain» a Nivel Nacional". *ICADE. Revista De La Facultad De Derecho*, n. 101, 2018 (disponible en https://doi.org/10.14422/icade.i101.y2017.006; última consulta 16/04/2024).
[37] Ibáñez Jiménez, J. W, *Op. cit.* p. 27.
[38] Puig Pascual, A. *Op. cit*.
[39] La PKI es un sistema diseñado para facilitar el uso seguro del cifrado de claves públicas en transacciones digitales. Opera verificando las identidades de las partes involucradas mediante la firma digital de certificados digitales por una entidad reconocida como autoridad de certificación (CA) de confianza.
[40]AEPD, "Cifrado y Privacidad (V): la clave como dato personal", 2021 (disponible en https://www.aepd.es/prensa-y-comunicacion/blog/cifrado-privacidad-iv-la-clave-como-dato-personal; última consulta 16/04/2024).

irreversible, la cual es de particular interés debido a su conflicto con el derecho al olvido. Por ahora, es pertinente determinar si esta técnica, a menudo considerada como un método de anonimización, cumple con los altos estándares de protección establecidos por el RGPD para obtener esta categorización.

El Grupo de Trabajo del artículo 29, en su Dictamen 5/2014[41], ha concluido que el proceso de hashing no convierte los datos personales en anónimos, una afirmación que ha encontrado respaldo en un informe de STOA preparado para el Parlamento Europeo, así como en las posiciones de la Agencia Española de Protección de Datos (AEPD) y el Comité Europeo de Protección de Datos (EDPB). En este contexto, los datos hash se clasifican y tratan como otros identificadores únicos, tales como las direcciones IP o los códigos SWIFT[42]. La justificación de este tratamiento se basa en los criterios estrictos que el RGPD establece para considerar que un dato es verdaderamente anónimo. Para alcanzar este estatus, debe ser prácticamente imposible revertir la información a su forma original o averiguar la identidad de la persona a la que pertenece, criterios que el hashing no cumple completamente debido a la posibilidad teórica de que esto suceda, aunque sea compleja[43].

Por lo tanto, se concluye que tanto la criptografía asimétrica como el hashing actúan como métodos de seudonimización. Aunque no logran desasociar completamente los datos de la persona a la que pertenecen[44], estas técnicas son valoradas por ofrecer una protección de datos personales adecuada y por reducir los riesgos asociados con su procesamiento[45].

---

[41] 2014 Article 29 Data Protection Working Party, Opinion 05/2014 on "Anonymisation Techniques", 2014 (disponible en http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm; última consulta 20/04/2024).

[42] *Cfr*. Hernández Peña, J. C., Op. cit. pp. 86-87. *Vid*. AEDP, "Introducción al hash como técnica de seudonimización de datos personales", 2019 (disponible en https://www.aepd.es/prensa-y-comunicacion/blog/anonimizacion-y-seudonimizacion; última consulta 16/04/2024). STOA, "Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law?", 2019.

[43] *Id.*

[44] Necesidad de realizar un análisis casuístico que verifique que la técnica empleada cumple con los criterios necesarios para minimizar los riesgos de individualización, vinculación e inferencia. Article 29 Working Party *id*. Hernández Peña plantea que el uso temporalmente restringido del tratamiento de datos mediante hash podría justificar su irreversibilidad en situaciones específicas. Argumenta que "un «hash» que se tratara por un período breve de tiempo cuenta con mayores posibilidades de que se llegue a considerar anónimo si se aplican capas y técnicas criptográficas adicionales". Hernández Peña, J.C., *Op. cit*. p. 87.

[45] *vid.* considerando 83 y artículo 32.1.a del RGPD

4. LA RESPONSABILIDAD EN EL TRATAMIENTO DE DATOS

Otro debate clave en torno al test de identificabilidad del Reglamento se centra en determinar desde qué perspectiva debería evaluarse el riesgo o la probabilidad de identificación[46]. ¿Quién es responsable de la categorización de los datos y, de este modo, de garantizar su protección? De manera más amplia, confirmada la sujeción de estos datos a los derechos salvaguardados en el Reglamento, ¿quién se encarga de garantizar su tratamiento adecuado y hacerlo cumplir?

El Capítulo IV del RGPD presenta las figuras de responsable y encargado del tratamiento de datos. Mientras que asume el rol de responsable quien determina los fines y medios del tratamiento, el encargado es el tratante por cuenta del responsable[47], rigiendo entre ambos un contrato[48].

El responsable del tratamiento debe cumplir su función mediante la implementación de medidas efectivas y apropiadas para asegurar la conformidad con el Reglamento. Este compromiso forma parte del principio de responsabilidad proactiva[49], que implica el uso de diversas herramientas diseñadas para proteger los derechos de los titulares de los datos de manera integral. Así, el RGPD va más allá de meramente establecer metas de cumplimiento; desarrolla y adapta los medios necesarios para alcanzarlas.

En este proceso añade la nota de flexibilidad en la aplicación, reconociendo que los diferentes responsables y encargados pueden necesitar adaptar sus medidas de protección de datos ante los diversos niveles de riesgos que enfrenten[50].

---

[46]Recuero, M. "La identificabilidad de los datos de carácter personal: una incertidumbre latente en tiempos del Reglamento general de protección de datos", *Derecho digital y nuevas tecnologías*, Thomson Reuters – Aranzadi, 2022.

[47] *Vid.* artículo 4.7 y 4.8 RGPD, relativos a la definición de responsable y encargado de datos.

[48] *Vid.* artículo 28 relativo a la relación responsable – encargado.

[49] *Vid.* artículos 5.2 y 24.1. RGPD

[50] Martínez Vázquez, F. "El reciente marco de la protección de datos personales (RGPD y nueva LOPDP): las obligaciones del responsable y del encargado, el Delegado de Protección de Datos y el régimen sancionador". *Revista Universidad, Ética y Derechos – Rueda*, n. 3-4, 2019, p. 47. A su vez, reconoce en su artículo la naturaleza de los datos, alcance subjetivo de la aplicación, métodos de tratamiento o número de operaciones sujetas a la misma organización son factores clave para interpretar el riesgo existente.

La figura del responsable y el encargado del tratamiento de datos adquiere una relevancia particular al considerar la diversidad de actores involucrados en los sistemas de registro distribuido. En principio, podríamos encontrarnos con múltiples responsables en términos de protección de datos personales, sin poder identificar claramente quién entre ellos tendría la obligación de garantizar, por ejemplo, el derecho de rectificación de los datos personales contenidos en el blockchain. La posibilidad de asignar a los distintos actores estos roles específicos será analizada en el apartado 4.3 de este trabajo.

La identificación del responsable del tratamiento de datos personales es un pilar fundamental para la aplicación efectiva del RGPD y el ejercicio de los derechos individuales, como el derecho al olvido. Esta figura desempeña un rol esencial al actuar como nexo entre los individuos y sus datos personales**.** En este sentido, el responsable del tratamiento se convierte en el punto de contacto principal al que los individuos pueden dirigirse para solicitar el ejercicio de sus derechos, incluyendo, en el caso específico del derecho al olvido, la supresión de sus datos.

CAPÍTULO IV. EL DERECHO AL OLVIDO: ARTÍCULO 17 RGPD.

1. RELEVANCIA Y ALCANCE DEL DERECHO AL OLVIDO

No existe un consenso doctrinal sobre los orígenes del derecho al olvido, pues se debate sobre la preexistencia de este concepto vinculado a los derechos de la intimidad, la reputación y la imagen, así como su amplia aplicación en el ámbito del Derecho Penal[51]. A pesar de que la Directiva 95/46 no reconoce explícitamente el derecho al olvido, algunos autores identifican vestigios fragmentados de este derecho en diferentes preceptos relacionados con el derecho de oposición y cancelación, y en la referencia a la no conservación de los datos por un tiempo mayor al necesario[52].

[51] Muchos autores se atribuyen al caso Melvin v. Reid (The California Court of Appeal, 1931) el origen del derecho al olvido, reconduciendo la resolución a través de las figuras del derecho al honor y a la intimidad. Cfr. López García, M. "Derecho a la información y derecho al olvido en internet", *La Ley Unión Europea*, n. 17, 2014, pp. 41-42.

[52] Ambrose, M.L. y Auloos, J. "The right to be forgotten across the pond", *Journal of Information Policy*, vol 3, 2013, p.7 (disponible en https://doi.org/10.5325/jinfopoli.3.2013.0001; última consulta 10/05/2024)

En este contexto, la sentencia del Tribunal de Justicia de la Unión Europea en el caso Google supone un cambio significativo al introducir la definición de la "noción moderna del derecho al olvido"[53]. El caso surgió debido a unas deudas del Sr. Costeja con la Seguridad Social, que resultaron en la subasta pública de su propiedad ordenada por el Ministerio de Trabajo y Asuntos Sociales, y su publicación en un periódico digital. Años después, al buscar el nombre del Sr. Costeja en Google, este artículo seguía resultando accesible. La cuestión a resolver suponía, por tanto, determinar si Google estaba obligada a eliminar de internet todos los datos personales relacionados con este suceso del pasado privado del Sr. Costeja[54].

Finalmente, el Tribunal resuelve reconociendo que los ciudadanos tienen el derecho a solicitar la eliminación de sus datos personales de internet cuando su tratamiento sea inapropiado, irrelevante o excesivo en relación con los fines y el tiempo transcurrido[55]. A esta sentencia le sigue la constatación del contenido obsoleto de la Directiva 95/46[56], lo que lleva a la incorporación de estas novedades en el RGPD.

El nuevo Reglamento establece el derecho al olvido de forma explícita, tanto como un derecho del interesado como una obligación del responsable del tratamiento de los datos[57]. Este derecho, detallado en el artículo 17, establece que la necesidad de borrar información personal puede deberse a varias circunstancias. Los interesados pueden solicitar la eliminación de sus datos personales cuando estos ya no sean necesarios desde una perspectiva

[53] Pazos Castro, R. "El mal llamado <<derecho al olvido>> en la era de Internet, Boletín del Ministerio de Justicia, vol. 69, n. 2183, 2015 (disponible en https://dialnet.unirioja.es/descarga/articulo/5342701.pdf; última consulta 15/05/2024).

[54] Sentencia del Tribunal de Justicia (Gran Sala), Google Spain y Google Inc. v. AEDP y Mario Costeja, C-131/12, de 13 de mayo de 2014 [versión electrónica - base de datos Eur-Lex. Ref. EU:C:2014:317]. Fecha de la última consulta: 13 de mayo de 2024.

[55] Moreno Bobadilla, A. "Los derechos digitales en Europa tras la entrada en vigor del Reglamento de Protección de Datos Personales: Un antes y un después para el derecho al olvido digital", *Estudios Constitucionales*, vol. 18, n.2, 2020 (disponible en: http://dx.doi.org/10.4067/S0718-52002020000200121; última consulta 13/05/2024).

[56] La nueva definición dista de las posibilidades de resolución de estos conflictos como una concreción de los derechos de oposición y cancelación. (1) Que un buscador cancele los datos de una persona no significa su total desaparición. Cfr. Piñar Mañas, J. L. "Caso google ¿una mejor privacidad?", *El País*, 15 de mayo de 2014 (disponible en https://elpais.com/elpais/2014/05/14/opinion/1400086304_243572.html; última consulta 12/05/2024). Pazos (*Op. cit*. pp. 43) añade otras dos diferencias: (2) no parece admitirse la identificación de la búsqueda como un acceso a datos personales por quién conoce los datos indexados y su disponibilidad, pues este acceso resulta posible para cualquier persona, (3) la posibilidad de que el motor de búsqueda siga mostrando la página web fuente si se accede con otros términos de búsqueda ajenos a los datos personales del afectado.

[57] Moreno Bobadilla, A., *Op. cit.*

empresarial, cuando retiren su consentimiento y no haya una necesidad imperiosa de retener los datos, o cuando la información haya sido obtenida o procesada ilegalmente.

De lo expuesto se deduce que el derecho al olvido adquiere un carácter más complejo, derivado de la variabilidad de las situaciones a las que intenta de dar respuesta. Supone una extensión del derecho de supresión que conlleva la obligación de intentar eliminar los datos que se hayan hecho públicos. El responsable del tratamiento que haya publicado estos datos debe informar a otros responsables del tratamiento para que eliminen todos los enlaces a dichos datos, así como sus copias o réplicas[58]. De este modo, no se corresponden con un borrado temporal de los mismos, sino que requiere la eliminación efectiva. Si bien, tampoco implica una supresión total y permanente por cuanto los datos tratados pueden seguir estando disponibles, asimilándose a una limitación de su difusión por cuanto solo se exige la "eliminación del enlace"[59].

El surgimiento de nuevas tecnologías ha añadido una capa adicional de complejidad a la implementación del derecho al olvido. En particular, las tecnologías de registro distribuido plantean desafíos únicos para la eliminación efectiva de datos. A continuación, se explorarán las problemáticas específicas del derecho al olvido en el contexto de la cadena de bloques, analizando cómo la naturaleza inmutable de esta tecnología y las características propias de su funcionamiento pueden dificultar su implementación.

2. PROBLEMÁTICA ASOCIADA A LA INMUTABILIDAD DE LA CADENA DE BLOQUES.

Al explorar las características esenciales y el funcionamiento de la blockchain, se destacaba su notable resistencia a la manipulación y se ofrecía una visión preliminar sobre el encadenamiento de datos. A continuación, se realizará un análisis más detallado de estas

[58] *Vid.* Considerando 66 RGPD.

[59] La resolución del caso Google Spain y Google Inc. v. AEDP y Mario Costeja establece que el derecho al olvido afecta únicamente a los resultados obtenidos al buscar por el nombre de la persona, sin requerir la eliminación de la página de los índices del buscador ni de la fuente original. El enlace dejará de ser visible solo en las búsquedas realizadas con el nombre de la persona que ejerció su derecho. Las fuentes no se modifican, y el resultado seguirá apareciendo en búsquedas realizadas con cualquier otra palabra o término diferente al nombre del afectado.

cuestiones y la problemática asociada a las mismas con respecto al cumplimiento del derecho al olvido.

El funcionamiento básico de una blockchain implica la adición de nuevos bloques, que contienen datos, a la red descentralizada, funcionando como un registro único. Las transacciones se registran y validan mediante un mecanismo de consenso y, una vez validados, los datos se integran a la cadena utilizando técnicas criptográficas. Todos los bloques están interconectados, desde el primer bloque de la red (conocido como bloque génesis) hasta el bloque más reciente, lo que garantiza la inmutabilidad de la cadena[60]. Cada bloque contiene el hash del bloque anterior, asegurando así la continuidad de la cadena y permitiendo únicamente la inclusión de bloques válidos.

En un sistema centralizado, la manipulación de la información puede ser relativamente sencilla. Sin embargo, en un sistema descentralizado, alterar los datos es prácticamente imposible. La inmutabilidad del sistema se mantiene porque cualquier intento de enviar una transacción inválida o con datos falsos será detectado y rechazado por el mecanismo de consenso, preservando así la integridad y la confiabilidad del sistema[61].

Cuanto más larga sea la cadena de bloques en una blockchain, mayor será su resistencia a los intentos de manipulación de sus datos. La alteración de cualquier dato comprometería todo el sistema, ya que las blockchains consisten en una serie de bloques interconectados, y un solo bloque corrupto afectaría a toda la cadena[62]. Una modificación en cualquier punto de la blockchain haría que el hash del siguiente bloque fuese incorrecto, por lo que obligaría a recalcular los hashes de todos los bloques subsiguientes, resultando extremadamente costoso[63]. Esto "rompería la cadena de bloques" haciendo que toda la blockchain devenga inútil.

[60]Llamas Covarrubias, J. Z. "Transparencia y protección de datos personales en la cadena de bloques (blockchain)", *Estudios En Derecho A la Información*, vol. 1, n. 11, 2020, pp. 34-35 (disponible en https://doi.org/10.22201/iij.25940082e.2021.11.15299; última consulta 17/05/2024).
[61] *Ibid.* p. 36
[62] Ibáñez, J., *Op. cit.* p. 22
[63]Politou, E., Casino, F., Alepis, E. & Patsakis, C. "Blockchain Mutability: Challenges and Proposed Solutions". *IEEE Transactions On Emerging Topics In Computing*, vol. 9, n.4, 2021, p. 1977 (disponible en https://doi.org/10.1109/tetc.2019.2949510; última consulta 17/05/2024).

Además, se ha hecho mención de la función crucial que la blockchain desempeña como registro, incluyendo la procedencia de los ítems que rastrea. Permitir que alguien sea "olvidado" crearía un vacío en la cadena de custodia de los elementos que la blockchain está monitoreando, lo que atentaría contra el valor fundamental que ofrecen las tecnologías blockchain[64].

La inmutabilidad de la tecnología blockchain aporta ventajas significativas en términos de transparencia y trazabilidad de las transacciones. Sin embargo, también presenta consecuencias indeseadas, como la persistencia de contenidos erróneos o ilegales en la cadena de bloques, así como de aquellos datos personales de un individuo cuando este solicita su eliminación en virtud del derecho recogido en el artículo 17 del RGPD.

En este contexto, parece inevitable hablar de una confrontación, si no de una incompatibilidad, tanto a nivel legal como técnico, entre el RGPD y la tecnología blockchain. Esto es comprensible si se considera la reciente expansión de blockchain a nivel global, ya que durante el largo proceso de debate y redacción del RGPD, no era tan prevalente como lo es hoy. Además, cabe la posibilidad de que los reguladores hayan optado deliberadamente por un enfoque neutral en cuanto a tecnología, para no atar las disposiciones de la ley a tendencias tecnológicas específicas y avanzadas[65].

Aunque en principio las blockchains son inmutables y la única forma de actualización sería mediante la adición de una nueva transacción a la cadena, algunos expertos argumentan lo contrario. En este debate, es crucial partir de la premisa de que alinear la tecnología blockchain con las necesidades del RGPD y el derecho al olvido requiere desarrollar una solución que permita eliminar datos personales de los registros de blockchain sin comprometer la integridad de la cadena, es decir, manteniendo intactas las funciones hash que interconectan los bloques.

Los argumentos principales en este contexto subrayan que la inmutabilidad de la blockchain es una propiedad emergente y no una característica intrínseca de su estructura de datos. Esto

[64] Tatar, U., Gokce, Y., & Nussbaum, B. (2020). "Law versus technology: Blockchain, GDPR, and tough tradeoffs", *Computer Law And Security Report/Computer Law & Security Report*, vol. *38*, 2020, p. 5 (disponible en https://doi.org/10.1016/j.clsr.2020.105454; última consulta 17/05/2024).
[65] Politou, E. et al., *Op. Cit.* p. 1978

significa que un agente o grupo de agentes con suficiente poder computacional podría alterar la blockchain[66].

En el caso de las blockchains permisionadas, donde el número de nodos está limitado, la manipulación de datos no debería considerarse imposible. Un análisis de los diversos mecanismos de consenso disponibles revela que siempre existe la posibilidad de que la mayoría del consorcio o los nodos dominantes (51%) se organicen de manera que impongan su versión de la realidad y modifiquen el libro mayor en consecuencia[67]. Aunque este escenario es más bien una posibilidad teórica, ya que un ataque de este tipo es complicado y costoso de ejecutar.

En las redes públicas, debido a su naturaleza más descentralizada y a la falta de confianza absoluta entre los participantes, parece aún más improbable la posibilidad de alterar la información. Sin embargo, se ha argumentado que incluso en las blockchains públicas no existe una inmutabilidad perfecta, ya que bajo ciertas condiciones específicas, una blockchain particular puede ser modificada[68]. Eventos como la bifurcación del DAO en la blockchain pública Ethereum en junio de 2016, llevada a cabo para revertir un fraude y devolver fondos robados por valor de unos 70 millones de dólares, sustentan esta teoría[69].

Estas perspectivas deben ser evaluadas en función de la distinción entre una eliminación total de datos de la cadena y el empleo de técnicas que tornen el contenido prácticamente inaccesible, una posible solución que se discute en términos de su compatibilidad con el RGPD y que requeriría un previo análisis casuístico que logre pasar exitosamente la prueba de identificabilidad[70].

---

[66] *Ibid*. p. 1977.

[67]Sayeed, S. & Marco-Gisbert, H. (2019). "Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack", *Applied Sciences*, vol. *9*, n. 1788, 2019 (disponible en https://doi.org/10.3390/app9091788; última consulta 18/05/2024).

[68]Greenspan, G., "The blockchain inmutability myth", 2017 (disponible en https://www.multichain.com/blog/2017/05/blockchain-immutability-myth; última consulta 19/05/2024).

[69] Romero Ugarte, J. L., "Tecnología de registros distribuidos (DLT): una introducción", *Boletín Económico/Banco de España, 4/2018*, 2018.

[70]Según la Autoridad Francesa de Protección de Datos (CNIL), es técnicamente imposible aprobar una solicitud de borrado de datos una vez encriptados en la cadena de bloques. Sin embargo, admite la existencia de técnicas criptográficas que pueden reducir la accesibilidad a niveles prácticamente nulos, pero cuestiona si la persistencia de estos datos en la cadena implica un incumplimiento con el RGPD.

De lo mencionado, se puede inferir que, a primera vista, blockchain no está diseñado para ser compatible con el RGPD, o que el RGPD en su forma más pura no es compatible con blockchain tal como se ha redactado hasta ahora. No obstante, a continuación se analizarán las diversas soluciones aportadas para ajustarse a esta compatibilidad.

El principal desafío reside en cómo proceder. Para abordar esto, consideraremos soluciones a través de dos enfoques: mediante estrategias legales que impliquen un ajuste de la regulación para este tipo de tecnologías, y mediante el desarrollo de técnicas que cumplan con los principios establecidos por el Reglamento.

2.1. Estrategias legales.

La primera vía para abordar la compatibilidad entre el RGPD y la tecnología blockchain consiste en abandonar una visión agnóstica en términos tecnológicos. Reconocer la relevancia y proliferación de la tecnología blockchain en el panorama actual y futuro requiere desarrollar marcos regulatorios específicos que se ajusten a sus particularidades, en lugar de aplicar reglas generales inapropiadas para su naturaleza.

En el contexto actual el problema puede abordarse, *prima facie*, por medio de dos alternativas: la exclusión del ámbito de aplicación del reglamento o la flexibilización del contenido del mismo para acomodarlo a las sus características. La primera opción implicaría directamente no incluir datos personales o reconocer el carácter anónimo y, como tal, no necesitado de mayor protección, de los datos incluidos en la blockchain.

Sin embargo, la esencia misma de la blockchain, especialmente en su uso como infraestructura de identidad digital, necesariamente implica el tratamiento de datos personales. Por ello, con el objetivo de adecuar los fines de la tecnología al tratamiento regulado por el Reglamento, se propone el almacenamiento off-chain de los datos personales que esta precisa para su operatividad. Bajo esta solución, los datos personales se separan de los demás datos de transacción y se almacenan fuera de la blockchain, mientras que en la cadena solo se recoge una marca de tiempo y un hash que hace referencia a la información

real guardada externamente[71]. Esto permite verificar la autenticidad de los datos sin necesidad de su almacenamiento directo. Así, una vez que la información original se elimina del almacenamiento externo, los datos restantes en la blockchain se vuelven inútiles para la identificación personal, cumpliendo de este modo con los requerimientos del derecho al olvido.

Sin embargo, esta solución contraviene los beneficios de almacenar datos en una blockchain en términos de transparencia, seguridad y resistencia a manipulaciones. Además, no está exenta de críticas e incertidumbre legal. En primer lugar, este intento de compatibilidad con el RGPD expone la blockchain a las vulnerabilidades del almacenamiento externo y, potencialmente, a la necesidad de terceros confiables, algo que la blockchain busca evitar. En segundo lugar, incrementa la complejidad y el riesgo, ya que cada empresa tiene su propia infraestructura y al distribuir los datos personales entre distintas compañías, aumenta el riesgo de que parte de esta información pueda ser robada en caso de una brecha de seguridad. Asimismo, el uso de la blockchain se reduciría a una simple tabla de consulta, desperdiciando muchos de los beneficios inherentes a esta tecnología[72]. Unos riesgos que cuestionan la robustez y eficacia de una solución que ni siquiera garantiza una compatibilidad total habida cuenta de que el carácter seudónimo de los datos encriptados podría ser susceptible de revelar información sensible en combinación con otra información disponible.

El otro enfoque mencionado consiste en tratar de convertir la información almacenada en verdaderamente anónima, eliminando cualquier probabilidad razonable de identificación del usuario mediante técnicas como *Zero-Knowledge proofs* (en adelante ZKP) o las denominadas *ring signatures* (firmas de anillo).

La ZKP engloba un conjunto de técnicas que permite a un verificador confirmar la veracidad de una declaración hecha por una parte (el probador) sin tener acceso a ningún conocimiento

[71] Belen-Saglam, R., Altuncu, E., Lu, Y., & Li, S. "A systematic literature review of the tension between the GDPR and public blockchain systems", *Blockchain. Research And Applications*, vol. *4*, n. 2, 2023 (disponible en https://doi.org/10.1016/j.bcra.2023.100129; última consulta 22/05/2024).

[72] Van Humbeeck, A., "The Blockchain-GDPR paradox",*CodeMine*, 2017 (disponible en https://blog.codemine.be/posts/20171121-blockchain-gdpr-paradox/; última consulta 23/05/2024).

sobre la declaración, excepto su veracidad[73]. La ZKP, en su funcionamiento básico, consta de un proceso por el cual el probador busca persuadir al verificador de que está al tanto de cierta información confidencial utilizando su firma digital identificadora. La ausencia de exposición del mensaje en su procesamiento garantiza la privacidad, pero a su vez lo hace costoso en recursos y tiempo de procesamiento[74].

Las *ring signatures*, por su parte, parten de la formación de anillos con las claves públicas de varios usuarios. Su beneficio consiste en ocultar la identidad del firmante al mezclar su firma con la de otros miembros del grupo, haciendo imposible para terceros identificar a título individual cuál de los posibles firmantes es el real[75]. Rivest y otros defienden la capacidad de esta herramienta para filtrar secretos pues, a título de ejemplo, podría utilizarse para proporcionar una firma anónima de un funcionario gubernamental, sin revelar la identidad concreta del firmante.

Sin embargo, estas alternativas no constituyen más que técnicas de encriptación y, al menos en su estado de desarrollo actual, no parecen garantizar una anonimización total a la altura del elevado estándar exigido por el Reglamento. La posibilidad de averiguar la identidad del titular de los datos persiste con la ZKP porque opera asociando al sujeto con una dirección URL, mientras que las firmas de anillo permiten saber que la información proviene de un miembro del grupo conocido. No obstante, estas técnicas avanzadas cumplen con dos principios clave del diseño de privacidad recogidos en el artículo 25 del RGPD: minimización de datos y limitación de la accesibilidad[76].

En cuanto a la flexibilización legislativa, el RGPD introducía un criterio de riesgo para determinar las obligaciones de los encargados y responsables del tratamiento de datos,

[73] Goldwasser, S., Micali, S., & Rackoff, C. (1989). "The Knowledge Complexity of Interactive Proof Systems", *SIAM Journal On Computing*, vol. 18, n. 1, pp. 186-208, 1989 (disponible en https://doi.org/10.1137/0218012; última consulta 22/05/2024).

[74] Júnior, T. A. F., Vasconcelos, R. O., & De Ribamar Lima Ribeiro, A. "Um estudo comparativo entre zero-knowledge proof (ZKP) e ring signatures visando as implicações legais e regulatórias com a lei geral de proteção de dados (LGPD) e general data protection regulation (GDPR)", *Revista Observatorio de la Economía Latinoamericana*, vol. 22, n. 2, 2024 (disponible en https://doi.org/10.55905/oelv22n2-015; última consulta 23/05/2024).

[75] Rivest, R. L.; Shamir, A.; Tauman, Y. "How to leak a secret." In: Advances in Cryptology — ASIACRYPT, Berlin, 2001 (disponible en https://iacr.org/archive/asiacrypt2001/22480554.pdf; última consulta 7/06/2024).

[76] AEPD, "Cifrado y Privacidad (IV): Pruebas de conocimiento cero", 2020 (disponible en https://www.aepd.es/prensa-y-comunicacion/blog/cifrado-privacidad-iv-pruebas-conocimiento-cero; última consulta 23/05/2024).

basándose en la razonabilidad de la identificación. Varios autores han propuesto diferentes clasificaciones en atención a esta posibilidad de identificación, destacando la hecha por Polonetsky sugiriendo un espectro de seis niveles: desde datos personales explícitos hasta anónimos[77].

En este sentido, podría explorarse la posibilidad de introducir una categoría específica que, dado el reducido riesgo de revelación de la identidad asociado con técnicas como las mencionadas anteriormente, permita una aplicación más flexible del RGPD para los datos cifrados en una blockchain que cumplan con este estándar (el cual deberá ser definido previamente).

Las características de esta medida sugieren cierto carácter de provisionalidad, pues no resuelve por completo el problema de la inmutabilidad o el borrado de datos, pero podría garantizar la compatibilidad del tratamiento. La minimización de las posibilidades de identificación a través de estas técnicas y la seguridad inherente a la estructura de la blockchain podrían ser argumentos suficientes para justificar la creación de una ficción de "dato olvidado" cuando aún persista en la cadena vestigio de la existencia del mismo[78]. Además, esta clasificación ad hoc no requeriría una modificación legislativa completa.

Asimismo, resulta adecuado establecer sandboxes regulatorios donde los proyectos de blockchain puedan operar con mayor flexibilidad bajo supervisión y evaluación continua. Esto permitiría a los reguladores observar el impacto de estas tecnologías y ajustar las normativas según sea necesario. La Comisión Europea ya ha dado sus primeros pasos en esta dirección con el comienzo en 2023 de este proyecto, buscando crear un marco para que reguladores, autoridades supervisoras y emprendedores de blockchain colaboren en un

[77] 1) dato personal explícito, 2) dato personal potencialmente identificable, 3) dato personal no inmediatamente identificable, 4) dato personal codificado, 5) dato personal no identificado (disociado) y 6) dato personal anónimo. Polonetsky, J., Tene, O., & Finch, K. "Shades of Gray: Seeing the Full Spectrum of Practical Data De-Identification", *Santa Clara Law Review*, vol. 56, n.3, 2016 (disponible en https://ssrn.com/abstract=2757709; última consulta 24/05/2024).

[78] Entiéndase la propuesta de una categoría con requisitos preestablecidos para garantizar un estándar de seguridad al mismo nivel que el establecido por el Reglamento, considerando como vestigios una señal de existencia de contenido tan ofuscado y difuso que la acerque a la inutilidad y, en todo caso, el desconocimiento del contenido que pretende ser olvidado.

diálogo regulatorio, identifiquen obstáculos y puedan llegar a un desarrollo colaborativo de un informe de buenas prácticas[79].

2.2. Estrategias técnicas.

El principal desafío en relación con la inmutabilidad de la blockchain es que, una vez que los datos se ingresan en ella, no pueden ser revocados. Esto se debe a reglas arquitectónicas del entorno digital construido, no a una cuestión normativa y, como tal, modificable[80]. Por ello, es crucial desarrollar soluciones técnicas que permitan la rectificación de datos en la blockchain.

La discusión tecnológica no se encuentra en el ámbito de desarrollo del presente trabajo, limitándose a analizar desde una perspectiva legal las principales soluciones propuestas: modelos de blockchain editable, eliminación de claves y poda de la blockchain.

La primera solución propone eliminar directamente la inmutabilidad desarrollando las blockchains editables, campo que aún se encuentra en prematuro desarrollo. Diversos modelos han sido propuestos de manera sucesiva desarrollando las deficiencias de sus predecesores.

Ateniese y otros introdujeron uno de los primeros modelos de arquitectura editable mediante la introducción de funciones hash camaleón. Estas funciones extienden las capacidades de las funciones hash tradicionales al incluir claves trampa, lo que permite a cualquiera que posea estas claves generar la función y encontrar colisiones en su dominio a la vez que la blockchain se mantiene resistente a aquellas colisiones ajenas a las claves trampa[81]. Con la clave trampa, se pueden identificar colisiones y reemplazar el contenido de los bloques, permitiendo así la redacción de la blockchain. Este sistema deja una cicatriz inmutable para indicar cuándo se ha modificado un bloque, haciendo compatible esta posibilidad de alteración con los beneficios asociados a la inmutabilidad de la blockchain: auditabilidad y

[79] The European Blockchain Services Infrastructure (EBS), "Sandbox Project", 2024 (disponible en https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/Sandbox+Project; última consulta 23/05/2024)
[80] Tatar, U., Gokce, Y., & Nussbaum, B., Op cit. p. 7.
[81]Khalili, M., Dakhilalian, M., & Susilo, W. "Efficient chameleon hash functions in the enhanced collision resistant model", *Information Sciences*, vol. 510, pp. 155-164, 2020 (disponible en https://doi.org/10.1016/j.ins.2019.09.001; última consulta 23/05/2024).

transparencia[82]. La idea es que la clave trampa se comparta secretamente entre un grupo de usuarios, haciéndolos responsables de redactar el contenido de la blockchain.

Posteriormente, se introdujo el concepto de *policy - based chameleon hash* (PCH). Estos permiten asociar políticas de acceso a los hashes generados, controlando los permisos de redacción según los atributos de los participantes. Cualquier usuario con permisos adecuados puede encontrar colisiones y modificar transacciones[83]. Diversos equipos de investigación han trabajado en el desarrollo de otros modelos de blockchain editable basada en PCH, implementando mecanismos de responsabilidad y autogestión de datos.

Sin embargo, se ha criticado esta propuesta por la posibilidad de que un usuario malicioso en una blockchain pública evite incluir una mutación en su transacción o configure una política que solo él pueda modificar. Además, los anteriores modelos presentan dificultades para su implementación en blockchains sin permiso, donde se desconocen los participantes. En respuesta, Deuber y sus colaboradores presentan un nuevo modelo consistente en un esquema de redacción a nivel de bloque que se basa en la votación por consenso. Si la propuesta de redacción de un usuario recibe suficientes votos, el bloque modificado reemplaza al original. Este sistema no depende de herramientas criptográficas complejas y permite a cualquier usuario verificar la legitimidad de la redacción comprobando los resultados de la votación en la cadena[84]. Este sistema asume que la mayoría de los nodos validadores son honestos y actúan de manera racional al votar para aceptar o rechazar las solicitudes de edición. Sin embargo, los validadores podrían optar por una actuación deshonesta y no revisar el grupo de bloques candidatos para aumentar sus oportunidades de ser seleccionados.

En términos generales, cabe concluir que la investigación sobre esquemas de blockchain editable ha demostrado que ninguno de ellos aborda la protección de la privacidad de los datos. La necesidad de avanzar en esta área se refleja en estudios posteriores, pero un análisis

[82] Ateniese, G., Magri, B., Venturi, D. & Andrade, E. "Redactable blockchain–or–rewriting history in bitcoin and friends", I*EEE European Symposium on Security and Privacy (EuroS&P)*, 2017, pp. 111–126 (disponible en 10.1109/EuroSP.2017.37; última consulta 23/05/2024).

[83]Dong, Y., Li, Y., Cheng, Y., & Yu, D. (2024). "Redactable consortium blockchain with access control: Leveraging chameleon hash and multi-authority attribute-based encryption", *High-confidence Computing*, vol. 4, n. 1, 2024 (disponible en https://doi.org/10.1016/j.hcc.2023.100168; última cosnsulta 24/05/2024).

[84] Deuber, D., Magri, B., & Thyagarajan, S. "Redactable blockchain in the permissionless setting," I*EEE European Symposium on Security and Privacy (EuroS&P)*, pp. 124–138, 2019 (disponible en https://doi.org/10.1109/SP.2019.00039; última consulta 24/05/2024).

comparativo de cada una de estas aproximaciones técnicas más complejas y concretas queda fuera del alcance de este estudio.

Otra solución alternativa para cumplir con el derecho al olvido es almacenar los datos en la blockchain de manera encriptada y así, cuando el usuario solicita la eliminación de su información personal, simplemente olvidar o eliminar la clave de cifrado haría que los datos se vuelvan inaccesibles[85]. Esto plantea la cuestión de si la referencia a la "tecnología disponible" en el artículo 17.2 RGPD podría interpretarse de manera que permita soluciones alternativas en lugar de la eliminación completa, dadas las limitaciones técnicas de la blockchain[86]. Pese a la aplicabilidad directa del RGPD, la ausencia de una definición precisa de en lo referente a "eliminación", abre la posibilidad de interpretaciones distintas a la eliminación absoluta. Algunas leyes nacionales ya han adoptado una versión más flexible del derecho al olvido, lo que sugiere que podría haber espacio para interpretaciones que consideren la inmutabilidad del libro mayor y la necesidad de soluciones alternativas[87]. Sin embargo, otros Estados miembros no han previsto esta opción[88], lo que podría llevar a una fragmentación de las reglas aplicables, contraviniendo el objetivo del RGPD de unificar estas normativas[89].

Por último, se debe mencionar la técnica de poda de la blockchain, que se desarrolla inicialmente para mejorar el rendimiento al reducir el tamaño de la cadena. No obstante, su operativa llamó la atención sobre las ventajas que estas técnicas ofrecen para cumplir con los requisitos del derecho al olvido[90]. La poda implica eliminar transacciones y bloques antiguos después de un período predefinido, manteniendo solo los bloques que contienen la versión hash de los datos eliminados, lo que garantiza la integridad y seguridad de los datos. Aunque esta solución presenta concesiones significativas y puede reducir el tamaño del nodo de archivo, toda la información necesaria para recrear el estado anterior todavía se almacena en

[85] Politou, E., Casino, F., Alepis, E. & Patsakis, C., *Op. cit*. p. 1979.
[86] Finck, M. "Blockchains and Data Protection in the European Union", *Max Planck Institute for Innovation & Competition Research Paper*, p. 24, 2017 (disponible en http://dx.doi.org/10.2139/ssrn.3080322; última consulta 24/05/2024).
[87] Es el caso de Alemania, cuya Ley de adaptación al Reglamento hace una valoración de las capacidades tecnológicas al aceptar la falta de eliminación absoluta cuando estas lo hagan imposible.
[88] Este es el posicionamiento, anteriormente comentado, de la CNIL.
[89] Finck, M. *Op. cit*. p. 25.
[90] The European union Blockchain Observatpory and Forum, "Blockchain and the GDPR", p. 31, 2018.

cada nodo. Esto hace improbable que esta técnica cumpla con las medidas de anonimización desde la perspectiva del RGPD, ya que las blockchains podadas conservan más estados históricos que el bloque más reciente[91]. Esto es necesario en caso de una reorganización de la blockchain, cuando una versión de la cadena con una mayor dificultad acumulativa aparece y revierte varios bloques[92].

3. DETERMINACIÓN DEL RESPONSABLE DEL TRATAMIENTO DE DATOS.

En el apartado 3.3 se señalaba cómo el RGPD pone un énfasis especial en los responsables del tratamiento de datos, identificándolos como los principales responsables de los deberes y obligaciones establecidos en su texto normativo. La necesidad de una entidad centralizada responsable según la ley y la eliminación de una autoridad central por parte de la tecnología blockchain son otro de los principios conflictivos entre el RGPD y blockchain. La arquitectura de red distribuida peer-to-peer significa que a menudo no está claro qué parte determina los fines y medios del tratamiento[93].

En la determinación del responsable se hace esencial diferenciar entre los agentes que establecen el propósito del tratamiento de datos en la capa de aplicación y aquellos involucrados en la capa de infraestructura[94]. *Prima facie*, los participantes que envían datos personales a la plataforma blockchain son más propensos a ser considerados responsables, ya que deciden el propósito y los aspectos técnicos y organizativos del tratamiento en la capa de aplicación. Por otro lado, los nodos y mineros que simplemente procesan datos en nombre de los usuarios en la capa de infraestructura probablemente sean encargados en lugar de responsables, ya que facilitan el funcionamiento de la red sin determinar los fines del tratamiento[95]. Si bien las dificultades que rodean este entramado hacen necesario un análisis casuístico.

---

[91] STOA, *Op. cit.* p. 35

[92] Roberto, J. "Dispelling Myths: How a Pruned Ethereum Node Can Fully Verify the Blockchain", 2018 (disponible en https://medium.com/coinmonks/how-a-pruned-ethereum-node-can-fully-verify-the-blockchain-bbe9f29663ed; última consulta 25/05/2024).

[93] *Cfr*. art. 4.7 RGPD.

[94] Winston, M. & Salmon, J. "A guide to blockchain and data protection", *Hogan Lovells*, p. 10, 2018 (disponible en https://engagepremium.hoganlovells.com/_uploads/blockchain-insights/5649DataProtection-BlockchainPaperARTWORKSTAGE3Low-res-gumfy.pdf; última consulta 30/05/2024).

[95] *Id.*

La extrapolación del razonamiento del Grupo de Trabajo del Artículo 29 sobre el control de datos en servicios de redes sociales (SNS) a la tecnología blockchain puede arrojar luz sobre la responsabilidad en el tratamiento de datos en este contexto. La entidad que gestiona la blockchain podría ser vista como responsable de definir los "medios para procesar los datos del usuario", y por ende, sería responsable de que estos "medios" se diseñen y operen conforme a los principios de privacidad desde el diseño[96].

De este modo, las blockchains privadas ofrecen un escenario más claro. En estos sistemas, un operador central o un consorcio puede ser considerado responsable si tiene control sobre la blockchain, de manera similar a una estructura de sistema tradicional. Mientras que este operador central podría actuar como responsable del tratamiento, proporcionando la infraestructura necesaria y garantizando los medios para las transacciones[97], otros actores involucrados en la operación de la blockchain podrían asumir roles de encargados[98].

En contraposición, en las blockchains públicas los roles son más difusos y generalmente no hay un operador central con control sobre los participantes, lo que complica la asignación de las funciones tradicionales de responsable y encargado. Si no existe una entidad con control claro sobre los datos, los participantes podrían argumentar que no hay un responsable definido y, por lo tanto, no puede haber encargados[99]. No obstante, esta interpretación puede no alinearse con el RGPD, que exige una "atribución clara de responsabilidades" para el tratamiento de datos personales[100].

La determinación de quién asume el rol de responsable y encargado en estos casos complejos deriva en la discusión acerca de la compatibilidad de las funciones de cada uno de los actores que intervienen en el ecosistema de blockchain con las responsabilidades de estas figuras respecto al tratamiento de datos.

---

[96] Article 29 Data Protection Working Party, Opinion 5/2009 on "Online social networking", p.3, 2009 (disponible en http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm; última consulta 30/05/2024).
[97] Hernández Peña, J. C., *Op. cit.* p. 95
[98] Shah, P., Forester, D., Raspe, C., & Mueller, H. "Blockchain technology: Data Privacy issues and potential mitigation strategies", *Practical Law*, p. 5, 2019 (disponible en https://www.davispolk.com/sites/default/files/blockchain_technology_data_privacy_issues_and_potential_mitigation_strategies_w-021-8235.pdf; última consulta 31/05/2024).
[99] *Id.*
[100] *Cfr*. considerando 79 RGPD

En primer lugar, están los desarrolladores, que tienen un papel técnico, diseñando los protocolos y programas que sostienen el funcionamiento de los registros distribuidos[101]. En redes privadas permisionadas, los desarrolladores ajustan el software según las directrices de los agentes centralizados que gestionan la red. En redes públicas sin permiso, una comunidad de desarrolladores trabaja en programas y protocolos bajo modelos de software libre o de código abierto, permitiendo que cualquier persona pueda acceder al código y proponer cambios[102].

Los desarrolladores del código tienen un control significativo sobre el software central, lo que les da potencialmente un alto grado de control sobre cómo se procesan los datos. Sin embargo, no manejan datos personales a menos que operen nodos o minen bloques. Por ello, su consideración como responsables o encargados del tratamiento de datos debe excluirse, ya que no tienen influencia en la determinación de los fines del tratamiento; simplemente ponen el software a disposición de los usuarios[103]. Por esta razón, STOA los equipara con proveedores de infraestructura de comunicaciones, quienes no son responsables de la información transmitida a través de sus sistemas[104].

En lo que respecta a los nodos, el criterio predominante es no considerarlos ni responsables ni encargados[105]. En cuanto a los nodos validadores, su rol se define por la ejecución del protocolo de acuerdo con el diseño de la cadena y el modelo de gobernanza, recopilando las transacciones en nuevos bloques[106]. En atención a este ejercicio de adición de bloques a la cadena, podría argumentarse que mantienen cierto grado de responsabilidad sobre los medios de procesamiento, pero nunca de los fines de una transacción[107]. También se pueden entender como encargados del tratamiento de datos si se considera que en este ejercicio de validación

[101] ITU-T Focus Group on Application of Distributed Ledger Technology: *Technical Specification FG DLT D 4.1 Op. cit.* p. 11
[102] Hernández Peña, J. C., *Op. cit.* p. 98.
[103] Jiménez-Gómez, B. S. "Risks Of Blockchain For Data Protection: A European Approach", Santa Clara High Tech. Law Journal, vol. 36, n. 3, p. 313, 2020 (disponible en https://digitalcommons.law.scu.edu/chtlj/vol36/iss3/2; última consulta 30/05/2024).
[104] STOA, *Op. cit.* p. 46
[105]Hernández Peña, J. C., *Op. cit.* p. 97.
[106] ITU-T Focus Group on Application of Distributed Ledger Technology: *Technical Specification FG DLT D 4.1 Op. cit.* p. 11
[107] Ibáñez, L., O'Hara, K., & Simperl, E. "On Blockchains and the General Data Protection Regulation", p. 4, 2018 (disponible en http://eprints.soton.ac.uk/id/eprint/422879; última consulta 30/05/2024).

actúan siguiendo las indicaciones de alguien[108], o argumentar solo validan las transacciones enviadas por los participantes sin involucrarse en sus propósitos[109] [110].

En atención a los restantes nodos, el razonamiento es el mismo. No obstante, es digno de mención el argumento por el cual, ante la ausencia de un responsable concreto y determinado, todos los nodos de la red podrían ser responsables del tratamiento de datos. Al decidir unirse a la red, los nodos operan sin estar sujetos a instrucciones externas y establecen en qué condiciones lo hacen, lo que sugiere que cada nodo podría determinar sus propios fines y, en cierta medida, medios de procesamiento[111].

Sin embargo, muchos autores son reticentes a clasificar a cada nodo en la blockchain como corresponsable según el RGPD. Esto se debe a que la dispersión de los nodos dificulta determinar ante quién pueden ejercer sus derechos los interesados y cuál sería el efecto material de ejercer estos derechos ante cualquier nodo en particular[112]. Además, la capacidad individual de cada nodo para influir sobre los medios y tratamientos puede ser limitada[113].

Otro problema deriva de que los nodos no pueden ver los datos personales porque están encriptados, por lo que, de calificarse como responsables, puede resultar que en la práctica, no sean capaces de cumplir con todas las obligaciones inherentes a ese rol ni satisfacer los derechos de los sujetos de datos[114]. Para resolver esta aparente contradicción, el Grupo de Trabajo del Artículo 29 señala que la incapacidad de cumplir directamente con todas las obligaciones de un responsable no excluye a uno de ser considerado como tal[115].

---

[108] En este sentido su papel se puede asimilar al de los proveedores de servicios de almacenamiento en la nube, quien procesa datos personales en nombre del cliente (responsable). Jiménez-Gómez, B. S., *Op. cit.* p. 316.
[109] CNIL., *"Solutions for a responsible use of the blockchain in the context of personal data"*, p. 2, 2018
[110] Algunos autores consideran que el rol de los mineros en Bitcoin es meramente pasivo, ya que solo se encargan de procesar las direcciones del remitente y destinatario, las claves públicas y un hash criptográfico del contenido de la transacción, así como la cantidad de BTC. Su influencia en la inclusión de transacciones es nula, aunque si luye una transacción inválida en su bloque este será rechazado por los demás. Jiménez-Gómez, B. S. *Op. cit.* p. 314.
[111] Finck, M., *Op. cit.* p. 10
[112] Hernández Peña, J. C., *Op. cit.* p. 97.
[113] *Id.*
[114] Jiménez-Gómez, B. S., *Op. cit.* p. 324.
[115] Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", p. 22, 2010 (disponible en http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm; última consulta 31/05/2024).

Finalmente, es importante referirse a los participantes, quien tienen derechos plenos de escritura y acceso al registro[116]. La CNIL considera que un participante es responsable cuando se trata de una persona física cuya operación de procesamiento de datos personales está relacionada con una actividad profesional o comercial[117], así como cuando se trata de una persona jurídica que registra datos personales en una blockchain[118].

Además, varios participantes, actuando como grupo, pueden compartir la responsabilidad[119]. De acuerdo con la jurisprudencia reciente, simplemente optar por la DLT para procesar datos puede hacer que el usuario sea considerado responsable, sin necesidad de controlar los fines y medios del tratamiento, lo que entraña riesgos para la protección efectiva[120].

Al hacer a todos responsables (sean nodos o participantes), cabe el riesgo de que en realidad nadie lo sea de manera efectiva[121]. Para mitigar este riesgo, la CNIL recomienda designar a un participante como responsable cuando este toma decisiones por el grupo. Esto permitiría evitar supuestos de corresponsabilidad, pero ante la ausencia de identificación de uno, todos los participantes podrían serlo por igual[122].

Si bien es preciso señalar que la existencia de corresponsabilidad, ya sea entre usuarios, nodos u otros agentes, no implica que todos tengan la misma responsabilidad. Esta varía según la etapa y el grado de participación en el procesamiento de datos. Argumentar que todos los usuarios controlan los datos porque más de la mitad del poder de cómputo puede cambiar las reglas de la red implica que un usuario común podría ser considerado un responsable de datos[123]. Sin embargo, esto no es práctico ni razonable. Este hecho señala la

---

[116] ITU-T Focus Group on Application of Distributed Ledger Technology: *Technical Specification FG DLT D1.1*.

[117] La introducción de datos con carácter ajeno a una actividad comercial o profesional se excluye del ámbito de aplicación del RGPD: "actividad exclusivamente personal o doméstica" (art. 2.2.c).

[118] CNIL, *Op. cit.* p. 1

[119] *Vid.* art. 26. RGPD.

[120] En el caso Fashion ID, el TJUE concluyó que el administrador de una página web es responsable del tratamiento de datos personales simplemente por integrar un complemento, sin importar si puede controlar los datos transmitidos o las acciones del proveedor externo con esos datos. Esta responsabilidad surge del beneficio comercial que el operador obtiene al utilizar dicho complemento, lo que implica una influencia significativa sobre la recopilación y transmisión de los datos personales de los visitantes del sitio web. Sentencia del Tribunal de Justicia (Sala Segunda), Fashion ID GmbH & Co. KG, C-40/17, de 29 de julio de 2019 [versión electrónica - base de datos InfoCuria. Ref. EU:C: 2019:629]. Fecha de la última consulta: 2 de junio de 2024.

[121] Jiménez-Gómez, B. S., *Op. cit.* p. 324.

[122] CNIL, *Op. cit.* p. 2

[123] Jiménez-Gómez, B. S., *Op. cit.* p. 324.

importancia de distinguir entre diferentes roles y niveles de responsabilidad dentro de la red para asegurar el cumplimiento de las normativas de protección de datos de manera justa y eficiente, sin derivar en supuestos como la sobrecarga de los participantes comunes con obligaciones impracticables.

CAPÍTULO V. CONCLUSIONES

El estudio realizado ha identificado los desafíos en la convergencia entre tecnología y marco legal en el tratamiento de datos personales y registros distribuidos. Mientras el RGPD se redacta con el objetivo de devolver a los ciudadanos el control sobre sus datos personales, imponiendo regulaciones estrictas sobre su tratamiento, la blockchain redefine el modo en que se gestionan y verifican los datos. A partir de este análisis, se derivan las siguientes conclusiones:

- Las cuestiones relativas a cómo esta nueva tecnología se ajusta a las leyes existentes han sido abordadas con éxito mediante la introducción de criterios flexibles para determinar el alcance territorial del Reglamento y la clasificación de los datos encriptados en la cadena como datos seudónimos. Sin embargo, persiste la necesidad de encontrar soluciones efectivas para su aplicación práctica.

- La colisión entre la capacidad de la blockchain para descentralizar e inmutabilizar la información y el compromiso del RGPD de proteger la privacidad de los individuos a través de la designación de responsables de tratamiento y del derecho al olvido, plantea un dilema complejo. Dada la aparente incompatibilidad de ambos enfoques, expertos en tecnología blockchain y juristas tratan de abordar las soluciones desde perspectivas separadas.

- El carácter descentralizado de la blockchain y la variedad de sus formas organizativas pueden dificultar la determinación del responsable y del encargado del tratamiento de datos, haciendo que diferentes actores puedan asumir estos roles en atención a un análisis casuístico. Además, se da una falta de homogeneidad interpretativa que aumenta la complejidad para los individuos de identificar ante quién deben exigir el cumplimiento de sus derechos.

- Las soluciones propuestas para solventar la problemática de la inmutabilidad en la cadena de bloques solo abordan parcialmente los desafíos existentes. Desde el punto de vista normativo, se han sugerido exclusiones o categorizaciones especiales de datos, sin lograr una solución que cumpla con los elevados estándares reglamentarios. Mientras tanto, las soluciones técnicas se desarrollan al margen de los requisitos de privacidad establecidos por la normativa. Esto refuerza la idea de una posible incompatibilidad y plantea la cuestión de qué se debe ajustar más: ¿la tecnología o la ley? Permitir excepciones para fomentar el potencial de la blockchain podría suponer un precedente para un desarrollo tecnológico sin límites que llegara a comprometer la protección de los derechos fundamentales. Por otro lado, adherirse estrictamente al RGPD podría limitar excesivamente el desarrollo tecnológico.

- El desarrollo legal y tecnológico comparten el objetivo de servir a la sociedad, pero la rápida evolución tecnológica crea una brecha entre ambas esferas. El derecho debe actuar como mediador, equilibrando el orden y el progreso. Es crucial que los juristas se comprometan en la creación de una teoría legal con conciencia tecnológica para abordar las demandas de la era digital. Además, es esencial que los desarrolladores técnicos colaboren estrechamente con los juristas para ayudar a adaptar el marco legal a las realidades tecnológicas, encontrando soluciones prácticas y legalmente viables.

- La creación de regulaciones más flexibles que no exijan un borrado total de los datos o la rebaja de los altos estándares protectores del reglamento podrían permitir el cumplimiento del derecho al olvido mediante técnicas criptográficas avanzadas diseñadas específicamente para cumplir con las exigencias legales. Sin embargo, esta solución es muy costosa, no solo en lo que respecta al procesamiento de datos bajo estas claves, sino también en cuanto a recursos necesarios. Además, conlleva el riesgo de que futuras innovaciones requieran ajustes normativos similares, derivando en la fragmentación del ordenamiento.

  La poda de la blockchain podría convertirse en una solución legítima si se rebajan estos estándares, mejorando la eficiencia de la cadena y reduciendo el coste del procesamiento de datos en comparación con la solución anterior.

No obstante, considero que el desarrollo de blockchains editables es la opción más prometedora, ya que permite abordar directamente la inmutabilidad de la cadena sin comprometer los estándares normativos. A pesar de la dificultad de su desarrollo, puede llegar a ofrecer una solución válida a largo plazo que permita alcanzar otros beneficios operativos. Si bien este campo requiere mayor desarrollo y, en este proceso, es fundamental incorporar las recomendaciones legales para alcanzar los estándares de privacidad establecidos por la normativa y seguir trabajando en el perfeccionamiento de modelos que no comprometan la integridad y la seguridad de la cadena.

En conclusión, la interacción entre la blockchain y el derecho al olvido no constituye ni debe verse como un obstáculo insuperable, sino como una oportunidad para explorar nuevas vías y desarrollar soluciones innovadoras que beneficien a la sociedad en su conjunto. A través de un enfoque multifacético y colaborativo que integre tanto las soluciones técnicas como las normativas se puede lograr un equilibrio en el que la blockchain pueda alcanzar su pleno potencial sin comprometer los principios fundamentales del RGPD.

CAPÍTULO VI. BIBLIOGRAFÍA Y OTROS RECURSOS

1. Legislación

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 respeta al tratamiento de datos personales y a la libre circulación de estos datos (DOCE, núm 281, de 23 de noviembre de 1995, pp. 31-50.)

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (BOE, núm. 298, de 14 de diciembre de 1999).

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 (DOUE, núm 119, de 4 de mayo de 2016, pp. 1-88).

Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, relativo a un marco para la libre circulación de datos no personales en la Unión Europea (DOUE, núm. 303, de 28 de noviembre de 2018, pp. 59 a 68).

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (BOE, núm. 294, de 6 de diciembre de 2018).

2. Jurisprudencia

Sentencia del Tribunal de Justicia (Sala Segunda), Comisión v. España, C-546/03, de 23 de febrero de 2006 [versión electrónica - base de datos Eur-Lex. Ref. EU:C: 2006:132]. Fecha de la última consulta: 15 de abril de 2024.

Sentencia del Tribunal de Justicia (Gran Sala), Google Spain y Google Inc. v. AEDP y Mario Costeja, C-131/12, de 13 de mayo de 2014 [versión electrónica - base de datos Eur-Lex. Ref. EU:C:2014:317]. Fecha de la última consulta: 13 de mayo de 2024.

Sentencia del Tribunal de Justicia (Sala Segunda), Fashion ID GmbH & Co. KG, C-40/17, de 29 de julio de 2019 [versión electrónica - base de datos InfoCuria. Ref. EU:C: 2019:629]. Fecha de la última consulta: 2 de junio de 2024.

3. Obras Doctrinales y Recursos De Internet

AEDP, "Anonimización y seudonimización", 2021 (disponible en https://www.aepd.es/prensa-y-comunicacion/blog/anonimizacion-y-seudonimizacion).

AEPD, "Cifrado y Privacidad (IV): Pruebas de conocimiento cero", 2020 (disponible en https://www.aepd.es/prensa-y-comunicacion/blog/cifrado-privacidad-iv-pruebas-conocimiento-cero; última consulta 23/05/2024).

AEPD, "Cifrado y Privacidad (V): la clave como dato personal", 2021 (disponible en https://www.aepd.es/prensa-y-comunicacion/blog/cifrado-privacidad-iv-la-clave-como-dato-personal; última consulta 16/04/2024).

AEDP, "Introducción al hash como técnica de seudonimización de datos personales", 2019 (disponible en https://www.aepd.es/prensa-y-comunicacion/blog/anonimizacion-y-seudonimizacion; última consulta 16/04/2024).

Ambrose, M.L. y Auloos, J. "The right to be forgotten across the pond", *Journal of Information Policy,* vol. 3, 2013, pp. 1- 23 (disponible en https://doi.org/10.5325/jinfopoli.3.2013.0001; última consulta 10/05/2024)

Article 29 Data Protection Working Party, Opinion 5/2009 on "Online social networking", 2009 (disponible en http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm; última consulta 30/05/2024).

Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", 2010 (disponible en http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm; última consulta 31/05/2024).

Article 29 Data Protection Working Party, Opinion 05/2014 on "Anonymisation Techniques", 2014 (disponible en http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm; última consulta 20/04/2024).

Ateniese, G., Magri, B., Venturi, D. & Andrade, E. "Redactable blockchain–or–rewriting history in bitcoin and friends", I*EEE European Symposium on Security and Privacy (EuroS&P)*, 2017 pp. 111–126 (disponible en 10.1109/EuroSP.2017.37; última consulta 23/05/2024).

Barrio Andrés, M. *Fundamentos del derecho de internet*, Centro de Estudios Políticos y Constitucionales, Madrid, 2020.

Belen-Saglam, R., Altuncu, E., Lu, Y., & Li, S. "A systematic literature review of the tension between the GDPR and public blockchain systems", *Blockchain. Research And Applications*, vol. *4*, n. 2, 2023 (disponible en https://doi.org/10.1016/j.bcra.2023.100129; última consulta 22/05/2024).

Boar, A., "Efectos de la tecnología blockchain en el sector financiero" en Profit (ed.), ACCID (coord.), *Blockchain, bitcoin y criptomonedas: bases conceptuales y aplicaciones prácticas*, Bresca, Barcelona, 2018, pp. 19-20.

Buterin, V., "The Meaning of Decentralization". *Medium*, vol. 6, 2017 (disponible en https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274; última consulta 3/03/2024)

CNIL., *"Solutions for a responsible use of the blockchain in the context of personal data"*, 2018

Deuber, D., Magri, B., & Thyagarajan, S. "Redactable blockchain in the permissionless setting," I*EEE European Symposium on Security and Privacy (EuroS&P)*, pp. 124–138, 2019 (disponible en https://doi.org/10.1109/SP.2019.00039; última consulta 24/05/2024).

Domenech, J. J. G., "La aplicación del nuevo RGPD en el contexto del tratamiento de datos en la UE", *Revista Lex Mercatoria*, n. 6, 2017, pp. 37-42 (disponible en https://doi.org/10.21134/lex.vi.53; última consulta 16/04/2024).

Dong, Y., Li, Y., Cheng, Y., & Yu, D. (2024). "Redactable consortium blockchain with access control: Leveraging chameleon hash and multi-authority attribute-based encryption", *High-confidence Computing*, vol. 4, n. 1, 2024 (disponible en https://doi.org/10.1016/j.hcc.2023.100168; última cosnsulta 24/05/2024).

Finck, M. "Blockchains and Data Protection in the European Union" (November 30, 2017). *Max Planck Institute for Innovation & Competition Research Paper*, 2017 (disponible en http://dx.doi.org/10.2139/ssrn.3080322; última consulta 24/05/2024).

Goldwasser, S., Micali, S., & Rackoff, C. (1989). "The Knowledge Complexity of Interactive Proof Systems", *SIAM Journal On Computing*, vol. 18, n. 1, pp. 186-208, 1989 (disponible en https://doi.org/10.1137/0218012; última consulta 22/05/2024).

Greenspan, G., "The blockchain inmutability myth", 2017 (disponible en https://www.multichain.com/blog/2017/05/blockchain-immutability-myth; última consulta 19/05/2024).

Hernández Peña, J. C., "Tecnologías de registro distribuido y protección de datos personales. Compatibilidad y conflictos al hilo del Reglamento general de Protección de Datos" Valpuesta, E. & Hernández Peña, J. C (coord.), Blockchain: aspectos jurídicos de su utilización, Wolters Kluwer, Madrid, 2022, pp. 65-99.

Ibáñez, L., O'Hara, K., & Simperl, E. "On Blockchains and the General Data Protection Regulation", 2018 (disponible en http://eprints.soton.ac.uk/id/eprint/422879; última consulta 30/05/2024).

Ibáñez Jiménez, J. W, *Derecho de blockchain y de la tecnología de registros distribuidos*, Aranzadi, Navarra, 2018.

ITU-T Focus Group on Application of Distributed Ledger Technology: *Technical Specification FG DLT D1.1. Distributed ledger technology terms and definitions*, International Communication Union (ITU), 1 de agosto de 2019 (disponible en https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d11.pdf; última consulta 1/03/2024)

ITU-T Focus Group on Application of Distributed Ledger Technology: *Technical Specification FG DLT D 4.1. Distributed ledger technology regulatory framework*, International Communication Union (ITU), 1 de agosto de 2019 (disponible en https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d14.pdf; última consulta 30/05/2024)

Jiménez-Gómez, B. S. "Risks Of Blockchain For Data Protection: A European Approach", Santa Clara High Tech. Law Journal, vol. 36, n. 3,.pp. 281-343, 2020 (disponible en https://digitalcommons.law.scu.edu/chtlj/vol36/iss3/2; última consulta 30/05/2024).

Júnior, T. A. F., Vasconcelos, R. O., & De Ribamar Lima Ribeiro, A. "Um estudo comparativo entre zero-knowledge proof (ZKP) e ring signatures visando as implicações legais e regulatórias com a lei geral de proteção de dados (LGPD) e general data protection regulation (GDPR)", *Revista Observatorio de la Economía Latinoamericana*, vol. 22, n. 2, 2024 (disponible en https://doi.org/10.55905/oelv22n2-015; última consulta 23/05/2024).

Khalili, M., Dakhilalian, M., & Susilo, W. "Efficient chameleon hash functions in the enhanced collision resistant model", *Information Sciences*, vol. 510, pp. 155-164, 2020 (disponible en https://doi.org/10.1016/j.ins.2019.09.001; última consulta 23/05/2024).

Llamas Covarrubias, J. Z. "Transparencia y protección de datos personales en la cadena de bloques (blockchain)", *Estudios En Derecho A la Información*, vol. 1, n. 11, 2020, pp. 27-63 (disponible en https://doi.org/10.22201/iij.25940082e.2021.11.15299; última consulta 17/05/2024).

López García, M. "Derecho a la información y derecho al olvido en internet", *La Ley Unión Europea*, n. 17, 2014.

Martínez Vázquez, F. "El reciente marco de la protección de datos personales (RGPD y nueva LOPDP): las obligaciones del responsable y del encargado, el Delegado de Protección de Datos y el régimen sancionador". *Revista Universidad, Ética y Derechos – Rueda*, n. 3-4, 2019, pp.41-57.

Moreno Bobadilla, A. "Los derechos digitales en Europa tras la entrada en vigor del Reglamento de Protección de Datos Personales: Un antes y un después para el derecho al olvido digital", *Estudios Constitucionales*, vol. 18, n.2, 2020 (disponible en: http://dx.doi.org/10.4067/S0718-52002020000200121; última consulta 13/05/2024).

Pazos Castro, R. "El mal llamado <<derecho al olvido>> en la era de Internet, Boletín del Ministerio de Justicia, vol. 69, n. 2183, 2015 (disponible en https://dialnet.unirioja.es/descarga/articulo/5342701.pdf; última consulta 15/05/2024).

Piñar Mañas, J. L. "Caso google ¿una mejor privacidad?", *El País*, 15 de mayo de 2014 (disponible en https://elpais.com/elpais/2014/05/14/opinion/1400086304_243572.html; última consulta 12/05/2024)

Politou, E., Casino, F., Alepis, E. & Patsakis, C. "Blockchain Mutability: Challenges and Proposed Solutions". *IEEE Transactions On Emerging Topics In Computing*, vol. 9, n.4, 2021, pp. 1972-1986 (disponible en https://doi.org/10.1109/tetc.2019.2949510; última consulta 17/05/2024).

Polonetsky, J., Tene, O., & Finch, K. "Shades of Gray: Seeing the Full Spectrum of Practical Data De-Identification", *Santa Clara Law Review*, vol. 56, n.3, 2016 (disponible en https://ssrn.com/abstract=2757709; última consulta 24/05/2024).

Posner, R. A. *Economic analysis of law*. Aspen Publishing, 2014.

Puig Pascual, A. "Identidad Digital Sobre «Blockchain» a Nivel Nacional". *ICADE. Revista De La Facultad De Derecho*, n. 101, 2018 (disponible en https://doi.org/10.14422/icade.i101.y2017.006; última consulta 16/04/2024).

Rallo Lombarte, A. V. "El nuevo derecho de protección de datos". *Revista Española de Derecho Constitucional*, n. 116, pp. 45-74 (disponible en https://doi.org/10.18042/cepc/redc.116.02; última consulta 7/03/2024).

Recuero, M. "La identificabilidad de los datos de carácter personal: una incertidumbre latente en tiempos del Reglamento general de protección de datos", *Derecho digital y nuevas tecnologías*, Thomson Reuters – Aranzadi, 2022, pp. 1225-1248.

Rivest, R. L.; Shamir, A.; Tauman, Y. “How to leak a secret.” In: Advances in Cryptology: ASIACRYPT, Berlin, 2001, pp. 552–565 (disponible en https://iacr.org/archive/asiacrypt2001/22480554.pdf; última consulta 7/06/2024).

Roberto, J. “Dispelling Myths: How a Pruned Ethereum Node Can Fully Verify the Blockchain”, 2018 (disponible en https://medium.com/coinmonks/how-a-pruned-ethereum-node-can-fully-verify-the-blockchain-bbe9f29663ed; última consulta 25/05/2024).

Romero Ugarte, J. L., “Tecnología de registros distribuidos (DLT): una introducción”, *Boletín Económico/Banco de España, 4/2018*, 2018.

Sayeed, S. & Marco-Gisbert, H. (2019). “Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack”, *Applied Sciences*, vol. *9*, n. 1788, 2019 (disponible en https://doi.org/10.3390/app9091788; última consulta 18/05/2024).

Shah, P., Forester, D., Raspe, C., & Mueller, H. “Blockchain technology: Data Privacy issues and potential mitigation strategies”, *Practical Law*, 2019 (disponible en https://www.davispolk.com/sites/default/files/blockchain_technology_data_privacy_issues_and_potential_mitigation_strategies_w-021-8235.pdf; última consulta 31/05/2024).

STOA, “Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law?”, 2019.

Swan, M., *Blockchain. Blueprint for a new economy*, O’Reilly, 2015.

Tatar, U., Gokce, Y., & Nussbaum, B. (2020). “Law versus technology: Blockchain, GDPR, and tough tradeoffs”, *Computer Law And Security Report/Computer Law & Security Report*, vol. *38*, 2020 (disponible en https://doi.org/10.1016/j.clsr.2020.105454; última consulta 17/05/2024).

The European union Blockchain Observatpory and Forum, “Blockchain and the GDPR”, 2018.

The European Blockchain Services Infrastructure (EBS), "Sandbox Project", 2024 (disponible en https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/Sandbox+Project; última consulta 23/05/2024)

Troncoso Reigado, A. "Del Principio de seguridad de los datos al derecho a la seguridad digital", *Economía industrial*, n 410,2018, p. 127-151.

Van Humbeeck, A., "The Blockchain-GDPR paradox",*CodeMine*, 2017 (disponible en https://blog.codemine.be/posts/20171121-blockchain-gdpr-paradox/; última consulta 23/05/2024).

Winston, M. & Salmon, J. "A guide to blockchain and data protection", *Hogan Lovells*, 2018 (disponible en https://engagepremium.hoganlovells.com/_uploads/blockchain-insights/5649DataProtection-BlockchainPaperARTWORKSTAGE3Low-res-gumfy.pdf; última consulta 30/05/2024)

Yeung, K., Regulation by Blockchain: The Emerging Battle for Supremacy between the Code of Law and Code as Law, *The Modern Law Review*, vol. 82, n. 2, pp. 207-209.