Universidad de San Andrés

Departamento de Derecho

Trabajo de Graduación - Abogacía

El Dilema de la Protección de Datos Personales en las Tecnologías de Registro Distribuido

Análisis de los desafíos legales y valores optimizados

Mentor: Federico Carestia

Autor: Valentina Rocca

Legajo Nº 30194

A mis padres, por impulsarme a crecer y seguir mis sueños.

A mis amigas, por haberme acompañado en cada paso del camino.

A Federico, mi mentor, por confiar en mis ideas.

A todos, gracias.

RESUMEN

Las tecnologías de registro distribuido ("DLT", por sus siglas en inglés) se han consolidado en los últimos años como una innovación revolucionaria con fundamentos tecnológicos que asegura diversos beneficios como la autenticación de la identidad, validación de información, seguridad, descentralización, transparencia y disminución de riesgos en el uso secundario de datos.

Sin embargo, una característica inherente de las DLT es la dificultad para eliminar unilateralmente los datos almacenados en ellas ya que sus registros, una vez validados, son permanentes y prácticamente inalterables. Esta peculiar cualidad puede obstaculizar los derechos de supresión y rectificación.

Este trabajo, luego de abordar la normativa de protección de datos personales en Argentina (que está en proceso de actualización) y los fundamentos y atributos técnicos de las DLT, analiza el dilema que presenta su compatibilización. El entorpecimiento en el ejercicio de algunos derechos viene acompañado de una optimización de valores relacionados con la privacidad de la información.

La versatilidad de las DLT, y sus múltiples campos de uso actuales y futuros, imponen la necesidad de examinar los desafíos que genera la aplicación del régimen vigente de protección de datos personales, como así también la estructuración de potenciales reformas legislativas.

Palabras Clave: *Protección de Datos Personales – Tecnologías de Registro Distribuído (DLT) – Blockchain – Derecho de Supresión – Privacidad.*

ÍNDICE

1. Introducción

En la era digital actual, la protección de datos personales es un tema de creciente preocupación y debate. Con el advenimiento de tecnologías como blockchain, que ofrecen una infraestructura segura y transparente para el almacenamiento y la transferencia de datos, surgen interrogantes sobre cómo se equilibran los principios para su protección y la capacidad de ejercer los derechos de sus titulares. El presente trabajo examina el dilema de la protección de datos personales en las tecnologías de registro distribuido ("DLT", por sus siglas en inglés), centrándose en cómo las DLT dificultan el ejercicio de algunos derechos de los titulares de datos, al tiempo que optimiza otros valores relacionados con la privacidad. Es importante aclarar que el término DLT abarca un grupo heterogéneo de tecnologías con diferentes arquitecturas, conceptos, propiedades y características. Por lo tanto, este trabajo utilizará el término de manera amplia y analizará las características generales de las DLT.

Las DLT se han consolidado como una innovación revolucionaria, que permite la creación de registros distribuidos y seguros mediante el uso de criptografía y mecanismos de consenso. La inmutabilidad de los datos almacenados en un registro distribuido asegura integridad y transparencia. Es por eso que ha sido aplicada en diversos campos, como las finanzas, la logística y la atención médica. De este modo, términos como *blockchain, crypto, smart contracts* y *ethereum* pasaron de ser jerga únicamente de un nicho específico a estar en boca de todos. Hoy en día parece casi una hazaña imposible atravesar una conversación sin que en algún momento alguien no haga mención del mundo *crypto*.

Una de las características inherentes a las DLT es la dificultad para eliminar unilateralmente los datos almacenados que en ellas se registran. A diferencia de las bases de datos tradicionales, donde los datos pueden ser modificados o eliminados sin demasiado problema, los registros de una DLT son permanentes y prácticamente inalterables una vez que han sido validados y añadidos al registro. Esta característica

obstaculiza el ejercicio de algunos derechos, como el derecho de supresión o rectificación, derechos fundamentales de los titulares de datos personales.

Sin embargo, es importante reconocer que las DLT también optimizan otros valores relacionados con la privacidad. Generalmente, al ofrecer una arquitectura descentralizada, las DLT reducen la dependencia de intermediarios y minimizan el riesgo de acceso no autorizado o manipulación de datos por parte de terceros. La criptografía utilizada en las DLT propicia seguridad y confidencialidad, protegiendo así la información de carácter personal de los usuarios. Además, facilita la verificación de la autenticidad de los datos e identidad de los usuarios, contribuyendo así a generar confianza en las interacciones.

Esta paradoja plantea un dilema complejo: ¿es justificable darle la espalda a las DLT debido a su dificultad para ejercer algunos derechos de los titulares de datos, mientras optimizan otros valores relacionados con la privacidad? Para responder esta pregunta, es fundamental analizar cuidadosamente los beneficios y las limitaciones de esta tecnología en relación con la normativa de protección de datos personales. A su vez, esta discusión nos lleva a plantearnos interrogantes sobre la naturaleza cambiante de la privacidad en la era digital, las implicaciones legales y los posibles enfoques regulatorios para abordar estos desafíos.

A través de un análisis exhaustivo, este artículo busca aportar claridad y perspectivas para abordar este dilema. A tal fin, este trabajo de desarrollará de la siguiente manera: primero, se estudiará el marco normativo sobre protección de datos personales en Argentina; segundo, se evaluarán los fundamentos de las DLT, tales como su definición y sus características técnicas; tercero, se expondrán los valores de privacidad que optimizan las DLT, los posibles casos de uso de estas tecnologías y los desafíos que plantean en términos de protección de datos personales; y, por último, se presentarán algunas reflexiones finales y consideraciones para el futuro.

Estimo relevante estudiar este interroganteya que, si bien comenzó a analizarse en el derecho europeo, no se ha examinado en profundidad bajo el cuerpo normativo actual de

la Argentina que, a su vez, se encuentra en miras de ser actualizado. El proyecto de ley presentado por la Agencia de Acceso a la Información Publica para actualizar la Ley N° 25.326 plantea la incorporación del principio de neutralidad tecnológica, es decir, que el régimen de protección de datos debe ser aplicable a cualquier tratamiento de datos personales, con independencia de las técnicas, procesos o tecnologías –actuales o futuras– que se utilicen para dicho efecto. No obstante, se demostrará que la incorporación de este principio no es suficiente para resolver la problemática que se plantea en el presente trabajo. Por lo tanto, teniendo en cuenta que la adopción de las DLT es incipiente, y que el proyecto de ley sigue planteando una posible colisión entre normativa y realidad, es importante profundizar en este dilema para encontrar algunas respuestas. En efecto, esta problemática seguro sea una de las tantas que comenzarán a vislumbrarse en un futuro cercano. No es noticia que la tecnología evoluciona de manera vertiginosa y es imposible prever los cambios que producirá, pero al menos podemos apuntar a elaborar un marco normativo integral que brinde soluciones reales en vez de generar más oscuridad.

2. Protección de Datos Personales

La protección de la intimidad y la vida privada ha sido consagrada en los tratados internacionales de derechos humanos después de la Segunda Guerra Mundial, como el Pacto Internacional de Derechos Civiles y Políticos de la ONU y el Convenio Europeo de Derechos Humanos.[1] En palabras de Puccinelli, "la privacidad emerge, como concepto, con la conciencia de que el otro –sea este el prójimo o el gobierno– es un enemigo en potencia".[2] Es por ello que estos tratados garantizan la salvaguardia de los individuos frente a las intrusiones arbitrarias o ilegales del Estado en su vida privada, familia, domicilio y correspondencia, es decir, entienden al derecho a la intimidad como una libertad negativa.[3]

[1] KORFF / GEORGES, *The Origins and Meaning of Data Protection*, [2020], p 3. (Disponible en SSRN https://ssrn.com/abstract=3518386 o http://dx.doi.org/10.2139/ssrn.3518386).
[2] PUCCINELLI, *Protección de datos de carácter personal*, Buenos Aires, Astrea, [2004] p. 14.
[3] Pacto Internacional de Derechos Civiles y Políticos de 1966, Artículo 17; Convenio Europeo de Derechos Humanos de 1950, Artículo 8.

No obstante, estas garantías de derechos humanos no brindaban ni brindan una tutela adecuada contra la recolección y el uso abusivo de datos personales. No se puede derivar de estos tratados una libertad positiva del sujeto de orientar su voluntad hacia un objetivo de tomar deciciones, sin verse determinado por la voluntad de otros ni tampco se puede derivar su derecho de accionar contra otros individuos; en el mejor de los casos, se puede emprender una acción contra el Estado por no proteger adecuadamente a los individuos de las acciones de esos otros particulares, según lo establezca la legislación nacional correspondiente.[4] Por esta razón, se reconoció un derecho independiente y distinto: la "protección de datos personales".[5]

La necesidad de resguardar los derechos humanos en relación con el tratamiento automatizado de datos personales surgió en la década de 1960, junto con la aparición de Internet y nuevas tecnologías. Sin embargo, en aquel entonces, Internet era una red limitada, utilizada principalmente por científicos, militares y académicos. Además, las computadoras eran costosas y ocupaban mucho espacio y su uso estaba limitado a las grandes empresas y autoridades públicas para tareas como gestión de pagos, registro de pacientes en hospitales, censos y estadísticas, y archivos policiales.[6]

En este contexto, la primera ley de protección de datos del mundo fue adoptada en septiembre de 1970 en Hessen, Alemania.[7] A esta ley le siguieron, en Europa, en esa década, la Ley Sueca de Protección de Datos (1973), la primera Ley Federal Alemana de Protección de Datos (finales de 1977), que abarcaba el tratamiento de datos personales por parte de organismos federales y del sector privado, la Ley francesa de Informática,

[4] KORFF / GEORGES, *The Origins and Meaning of Data Protection*, [2020], p 3.
[5] PUCCINELLI, *Protección de datos de carácter personal*, [2004] p. 18.
[6] KORFF / GEORGES, *The Origins and Meaning of Data Protection*, [2020], p 4.
[7] KORFF / GEORGES, *The Origins and Meaning of Data Protection*, [2020], p 7. Ver también: GREENLEAF, «Global Tables of Data Privacy Laws and Bills» en *Privacy Laws & Business International Report (PLBIR),* 157, 6, [2019].

Ficheros y Libertades de enero de 1978, y las leyes de protección de datos de Austria, Dinamarca, Noruega y Luxemburgo (todas de 1978-1979).[8]

En esta misma época, Estados Unidos comenzó a desarrollar su marco legal en lo que refiere a las restricciones en el tratamiento automatizado de datos personales a través de leyes como la *Fair Credit Reporting Act* de 1970, la *Privacy Act* de 1974, la *Right to Financial Privacy Act* de 1978 y la *Privacy Protection Act* de 1980.[9] Sus distintos Estados fueron estableciendo sus propias legislaciones sobre la materia, por ejemplo, el *Senate Bill* n° 170 aprobado por el gobernador de California, R. Reagan.[10]

Durante la década del 80, varios países más de Europa occidental e Israel adoptaron leyes de protección de datos personales. Asimismo, tras la disolución del bloque de países de Europa Oriental, en la década del 90, estos países también comenzaron a legislar en esta materia junto con otros países de Asia-Pacífico.[11]

En América Latina, la protección de datos personales se fue incorporando gradualmente a través de reformas constitucionales, algunas de las cuales han adoptado la figura del Habeas Data. Por ejemplo, en Brasil (1988) se establece en los artículos 5° - X, XII y LXXII y artículo 105 I b); en Colombia (1991) en el artículo 15; en Paraguay (1992) en los artículos 33, 36 y 135; en Perú (1993) en los artículos 2°, 162 y 203-3; en Argentina (1994) en los artículos 19 y 43; y en Ecuador (1998) en los artículos 23.8, 23.13, 23.24 y 94.[12] Estas reformas constitucionales sentaron las bases para la promulgación progresiva de leyes específicas para proteger los datos personales.

[8] KORFF / GEORGES, *The Origins and Meaning of Data Protection*, [2020], p 8. Ver también: GREENLEAF, «Global Tables of Data Privacy Laws and Bills» en *Privacy Laws & Business International Report (PLBIR)*, [2019].
[9] PUCCINELLI, *Protección de datos de carácter personal*, [2004] p. 16.
[10] PUCCINELLI, *Protección de datos de carácter personal*, [2004] p. 17.
[11] GREENLEAF, «Global Tables of Data Privacy Laws and Bills» en *Privacy Laws & Business International Report (PLBIR)*, [2019].
[12] GREGORIO, *Protección de Datos Personales en América Latina*, Instituto de Investigación para la Justicia [2016], p. 1. Ver también: TRONCOSO REIGADA, «El desarrollo de la protección de datos personales en Iberoamérica desde una perspectiva comparada y el reequilibro en los modelos de protección de datos a nivel internacional» en *Revista Internacional de Protección de Datos Personales*, 1 [2012].

Vale la pena resaltar que en paralelo ocurría el desarrollo de protocolos estándar como el TCP/IP y la adopción masiva del World Wide Web, lo que generó que Internet se transforme en una red global interconectada donde las personas comenzaron a poder acceder y compartir información de manera más eficiente.[13]

Durante las décadas siguientes, esta evolución se acrecentó. El surgimiento de servicios como el correo electrónico, los motores de búsqueda, los medios sociales, el comercio electrónico y la proliferación de dispositivos conectados, conocidos como el Internet de las cosas (IoT, por sus siglas en inglés) impulsó aún más la expansión de Internet.

Sin embargo, la creciente dependencia de Internet plantea preocupaciones sobre la seguridad y la privacidad de los datos. La falta de transparencia en el tratamiento de los datos, los ciberataques y el robo de información personal son amenazas persistentes en el entorno digital. En este contexto, la protección de los datos personales y la ciberseguridad se volvieron críticos.

2.1. Marco Normativo de Protección de Datos en Argentina

En el caso de Argentina, el derecho a la intimidad está consagrado en el Artículo 19 de la Constitución Nacional.[14] Este artículo establece que las acciones privadas de las personas, siempre y cuando no ofendan el orden público ni perjudiquen a terceros, están reservadas únicamente a Dios y no están sujetas a la autoridad de los magistrados.

En la reforma constitucional de 1994, se introdujo el concepto de amparo a través del Artículo 43 del Capítulo Segundo "Nuevos Derechos y Garantías".[15] Este artículo permite a cualquier individuo interponer una acción de amparo rápida y eficiente, cuando no exista otro recurso judicial más adecuado, contra actos u omisiones de autoridades –

[13] The European Union Blockchain Observatory & Forum, thematic report on “Metaverse” [2022], (disponible en https://www.eublockchainforum.eu/reports), p. 18-19.
[14] GAKH, “Argentina's Protection of Personal Data: Initiation and Response*”* en *A Journal of Law and Policy for the Information Society*, 2(3), [2006], p. 784.
[15] MCCLEARY, “To discovery and beyond: comprehensive look at Argentina's data protection laws” en *University of Miami Inter-American Law Review*, 47(1), 129-[ix], [2015], p. 142.

públicas o privadas– que, de manera actual o inminente, violen, restrinjan, alteren o amenacen de manera arbitraria o manifiestamente ilegal los derechos y garantías reconocidos por la Constitución, tratados internacionales o leyes.[16]

Además, se incorporó el concepto de "Habeas Data" como una forma especial de amparo.[17] Este mecanismo permite a las personas conocer los datos personales que los afectan y su propósito, almacenados en registros o bancos de datos públicos o privados destinados a proporcionar informes. En caso de falsedad o discriminación, las personas pueden exigir la eliminación, rectificación, confidencialidad o actualización de dichos datos. Es importante destacar que el secreto de las fuentes de información periodística no puede ser afectado.

En el año 2000 se promulgó la Ley Nº 25.326 de Protección de Datos Personales ("LPDP"). De los debates parlamentarios de la LPDP, surge que se tuvo en cuenta la Ley Orgánica 5/1992 española de regulación del tratamiento automatizado de datos con carácter personal y la Directiva de Protección de Datos de la Unión Europea (95/46/EC).[18] El objetivo de la LPDP es proteger de manera integral los datos personales almacenados en bases de datos públicas o privadas utilizadas para brindar informes, con el fin de garantizar el derecho al honor y la intimidad de las personas, de acuerdo con el artículo 43, párrafo tercero de la Constitución Nacional.[19] En el año 2001, el Poder Ejecutivo de la Nación reglamentó la LPDP mediante el Decreto 1558/2001.[20]

A su vez, desde 2019 Argentina es parte del Convenio para la protección de las personas con respecto al tratamiento automatizado de datos personales, conocido como "Convenio 108", que fue aprobado mediante la Ley 27.483. Este convenio, suscrito en 1981 en la ciudad de Estrasburgo, es el único instrumento multilateral de carácter vinculante en

[16] Artículo 43, Constitución Nacional.
[17] MCCLEARY, Ibid.
[18] EUSTICE / BOHN, "Navigating the Gauntlet: A Survey of Data Privacy Laws in Three Key Latin American Countries" en *The Sedona Conference Journal*, 14, [2013], p. 137-138.
[19] Ley de Protección de Datos Personales Nº 25.326 [2000]. (En adelante, "LPDP"). Artículo 1.
[20] PUCCINELLI, *Protección de datos de carácter personal*, [2004] p. 59.

materia de protección de datos personales, y requiere que los Estados parte adopten las medidas necesarias en su legislación nacional para aplicar en su territorio los principios establecidos en dicho convenio.

Argentina también firmó el Protocolo que modifica el Convenio 108, conocido como "Convenio 108+", que fue aprobado mediante la Ley 27.699. De hecho, Argentina fue el segundo país de América Latina en adherirse a este convenio, después de Uruguay. Sin embargo, el Convenio 108+ aún no está operativo a nivel mundial ya que aún está pendiente de ratificaciones.[21]

Además, mediante la Decisión de la Comisión Europea Nº 2003/490/CE, se otorgó a Argentina el reconocimiento como el primer país de América Latina en brindar una protección adecuada para la transferencia internacional de datos personales.[22] Hoy en día, Argentina mantiene esa condición.

En síntesis, el Régimen de Protección de Datos en Argentina está compuesto por la LPDP y su Decreto Reglamentario 1558/2001, así como por el Convenio 108 y el Convenio 108+. A esto se suman las resoluciones complementarias dictadas por la Agencia de Acceso a la Información Pública ("AAIP"), que establece lineamientos adicionales para asegurar la protección adecuada de los datos personales en el país.

Cabe destacar que, en septiembre de 2022, la AAIP publicó un proyecto de ley para actualizar la LPDP (el "Proyecto"). En efecto, LPDP fue promulgada hace más de 20 años. Los avances tecnológicos han transformado la manera en que interactuamos y compartimos información por lo que resulta evidente la necesidad de actualizar y fortalecer la legislación de protección de datos personales.

[21] La Convención 108+ entrará en vigor a partir del 11 de octubre de 2023 con la ratificación por parte de 38 Estados Miembro.
[22] McCLEARY, "To discovery and beyond: comprehensive look at Argentina's data protection laws" en *University of Miami Inter-American Law Review*, [2015], p. 138.

El citado proyecto de ley fue sometido a consulta pública y recibió una notable intervención de diversos actores.[23] En total, se recibieron 173 opiniones, aportes y comentarios presentados por 123 participantes provenientes de la ciudadanía en general, organizaciones de la sociedad civil, universidades e investigadores, así como el sector privado y el sector público, tanto a nivel nacional como internacional.

Durante este proceso, la AAIP tomó como línea de base los estándares y recomendaciones de relevancia internacional, incluyendo el Reglamento Europeo de Protección de Datos Personales (GDPR), el Convenio 108 y su versión modernizada, las recomendaciones de Ética de Inteligencia Artificial de la UNESCO, así como las legislaciones de otros países de la región, como Brasil y Ecuador, y los proyectos de ley en curso en Chile, Paraguay y Costa Rica. De esta manera, se buscó aprovechar la experiencia y mejores prácticas de otros países en la actualización de la normativa argentina.

Finalmente, en junio de 2023, el Poder Ejecutivo Nacional presentó el Proyecto ante la Cámara de Diputados de la Nación a través del Mensaje 87/2023.

2.1.1. Aplicación material de la Ley de Protección de Datos Personales.

El Artículo 1 de la LPDP establece que tiene por objeto "la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el Artículo 43, párrafo tercero de la Constitución Nacional".[24]

Se entiende por tratamiento de datos a operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en

[23] Resolución Nº 119/2022 y Resolución Nº 145/2022 de la AAIP.
[24] Artículo 1, LPDP.

general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.[25]

En esta misma línea, el Convenio 108+ establece que "tratamiento de datos" significa cualquier operación o conjunto de operaciones llevadas a cabo sobre los datos personales, tales como su recopilación, almacenamiento, preservación, alteración, recuperación, divulgación, suministro, eliminación o destrucción, o llevar a cabo operaciones lógicas y/o aritméticas sobre dichos datos.[26]

El Proyecto define al tratamiento como cualquier operación o conjunto de operaciones, automatizada, parcialmente automatizada o no automatizada, realizada sobre datos personales, que permita, de manera enunciativa, la recolección, conservación, organización, estructuración, almacenamiento, modificación, relacionamiento, evaluación, bloqueo o destrucción, publicación y, en general, su procesamiento, así como también su cesión a través de comunicaciones, consultas, interconexiones o transferencias.[27]

Ahora bien, la LPDP prevé una excepción a su aplicación. El Artículo 24 de la LPDP excluye de su ámbito de aplicación a las bases de datos que sean para un uso exclusivamente personal.[28] Se entiende por uso exclusivamente personal aquel uso que es doméstico y que realiza una persona humana con fines que atañen al desarrollo de su vida privada. Por lo tanto, siempre que los datos sean tratados con un fin doméstico, dicho tratamiento quedará excluido del régimen legal. Ahora bien, si estos datos personales se transmiten a un tercero, entonces el usuario se constituiría como responsable por el tratamiento, toda vez que estaría proveyendo informes.[29]

[25] Artículo 2, LPDP.
[26] Artículo 2, Convenio 108+.
[27] Artículo 2, Proyecto de Ley de Protección de Datos Personales presentado por la Agencia de Acceso a la Información Pública (en adelante, "Proyecto").
[28] Artículo 24, LPDP.
[29] PUCCINELLI, *Protección de datos de carácter personal*, [2004] p. 162.

Este mismo criterio es tomado por el Convenio 108+, que dispone no se aplicará al tratamiento de datos llevado a cabo por un individuo en el curso de actividades exclusivamente personales o domésticas.[30] De igual modo, el Proyecto excluye de su ámbito de aplicación el tratamiento de datos que efectúe una persona humana para su uso, propio o de su grupo familiar, exclusivamente privado y, por tanto, sin conexión alguna con una actividad profesional o comercial.[31]

2.1.2. Sujetos obligados

La persona física o jurídica titular de la base de datos es el responsable por el tratamiento de los datos personales y, en consecuencia, por el cumplimiento de las disposiciones de la LPDP. El Convenio 108 agrega que el responsable es aquel que, solo o en conjunto, tiene poder de decisión sobre el tratamiento de los datos personales.[32] De esta manera, se incorpora el concepto de corresponsable.

Las obligaciones más importantes que debe cumplir el responsable incluyen dar cumplimiento a las solicitudes de los titulares de datos respecto al ejercicio de sus derechos,[33] inscribirse en el Registro Nacional de Bases de Datos,[34] cumplir con el deber de confidencialidad y seguridad de la información,[35] atender las disposiciones específicas aplicables a la cesión,[36] procesamiento por parte de terceros[37] y transferencia internacional de datos[38] y respetar los principios generales del tratamiento (*i.e.*, lealtad, licitud y transparencia, minimización, proporcionalidad, limitación de la conservación y exactitud)[39].

[30] Artículo 3, Convenio 108+.
[31] Artículo 3, Proyecto.
[32] Artículo 2.d., Convenio 108.
[33] Artículos 14 y 16, LPDP.
[34] Artículo 21, LPDP.
[35] Artículos 9 y 10, LPDP.
[36] Artículo 11, LPDP.
[37] Artículo 25, LPDP y Artículo 25, Decreto 1558/2001.
[38] Artículo 12, LPDP. Ver también Resolución Nº 60-E/2016 y Resolución Nº 159/2018 de la AAIP.
[39] Artículo 4, LPDP.

Asimismo, debe informar al titular de los datos: (i) la finalidad para la que serán tratados sus datos y quiénes pueden ser sus destinatarios; (ii) la identidad y domicilio del responsable; (iii) el carácter obligatorio o facultativo de proveer sus datos; (iv) las consecuencias de no hacerlo o de proporcionar datos inexactos; (v) cómo ejercer los derechos de acceso, rectificación y supresión de los datos;[40] y (vi) la posibilidad de acudir a la AAIP para dar cumplimiento a sus derechos.[41]

Otra figura importante en el tratamiento de los datos personales es el encargado, es decir, aquel que realiza actividades de tratamiento de datos personales por cuenta y orden del responsable. La LPDP y su decreto reglamentario prevén que la realización de tratamientos por encargo debe estar regulada por un contrato que vincule al encargado del tratamiento con el responsable y que disponga que el encargado: (i) sólo actúa siguiendo instrucciones del responsable del tratamiento; (ii) no podrá utilizar los datos personales para fines distintos a los estipulados en el contrato ni cederlos a otras personales (ni aun para su conservación); (iii) cumple con las obligaciones de seguridad y confidencialidad de la LPDP; y (iv) una vez cumplida la prestación contractual, destruirá los datos, salvo excepciones.[42]

2.1.3. Aplicación territorial de la Ley de Protección de Datos Personales.

La LPDP aplica al tratamiento de datos personales de personas físicas o jurídicas con domicilio legal o delegación o sucursales en Argentina.[43]

Sin embargo, la LPDP no contiene una disposición específica que prevea su ámbito de aplicación territorial. Por lo tanto, no resulta claro si su aplicación se restringe exclusivamente a responsables del tratamiento ubicados dentro de Argentina, o si también se aplica a responsables que, a pesar de estar ubicados en el extranjero, tratan datos personales de titulares argentinos.

[40] Artículo 6, LPDP.
[41] Resolución Nº 14/2018 de la AAIP.
[42] Artículo 25, LPDP y Artículo 25, Decreto 1558/2001.
[43] Artículo 2, LPDP.

Del Artículo 44 de la LPDP surge que la jurisdicción federal rige respecto de bases de datos interconectadas en redes de alcance interjurisdiccional, nacional o internacional.[44] En esta misma línea, la AAIP señaló en una sanción contra Google SRL y Google LLC, que de este artículo surge su competencia sobre los responsables de bases de datos interconectadas que tengan alcance interjurisdiccional, nacional o internacional, en la medida en que se traten datos de titulares argentinos o que, de algún otro modo, el tratamiento de datos se conecte con, o produzca efectos en Argentina.[45]

Por su parte, el Proyecto brinda más claridad sobre este punto, ya que incluye un artículo específico sobre aplicación territorial de la ley. Al respecto, dispone que la ley aplicará en cualquiera de los siguientes casos:

1. Si el responsable o encargado del tratamiento se encuentra establecido en Argentina, incluso si el tratamiento de datos tuviese lugar fuera de dicho territorio;
2. Si el responsable o encargado, no se encuentra establecido en Argentina, pero se da alguno de los siguientes supuestos:
    a. realiza actividades de tratamiento de datos personales de cualquier tipo en Argentina de personas que se encuentran en dicho territorio;
    b. efectúa actividades de tratamiento relacionadas con la oferta de bienes o servicios a personas que se encuentren en Argentina o elabora perfiles de dichas personas;
    c. se encuentra establecido en un lugar al que se aplica la legislación argentina en virtud del derecho internacional o de disposiciones de carácter contractual.[46]

Cabe destacar que el texto del Proyecto es muy similar al de GDPR, no obstante, se diferencian en que GDPR limita su aplicación extraterritorial a aquellos casos en los que las actividades de tratamiento estén relacionadas con: (a) la oferta de bienes o servicios a

[44] Artículo 44, LPDP.
[45] Resolución Nº 69/2020 de la AAIP, "Giolito c/ Google Argentina SRL y Google LLC".
[46] Artículo 4, Proyecto.

interesados en la Unión Europea, independientemente de si a estos se les requiere su pago, o (b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión Europea.

Por su parte, el Proyecto aplica extraterritorialmente a cualquier tratamiento de datos de titulares de datos que se encuentren en Argentina, independientemente de a qué estén relacionadas las actividades. En este sentido, no resulta del todo claro la distinción de los incisos a y b, ya que el supuesto del inciso b estaría abarcado por el que se plantea en el inciso a.

2.1.4. Definición de datos personales

La LPDP limita su ámbito de protección a los datos de carácter personal. Al respecto, define datos personales como información de cualquier tipo referida a personas humanas o jurídicas, determinadas o determinables.

En este sentido, los datos adquieren carácter personal cuando se relacionan, vinculan o asocian con personas. Ahora bien, la LPDP no exige que la persona se encuentre determinada, sino con que basta que sea determinable, por lo tanto, el carácter se mantendría en aquellos supuestos en los que, si bien la realidad representada por el dato no es una persona, la información puede ser vinculada a la misma por asociación.[47]

Siguiendo este razonamiento, la LPDP no sería aplicable cuando los datos estuvieran disociados, es decir, cuando "la información obtenida no pueda asociarse a persona determinada o determinable".[48] La Resolución Nº 4/2019 de la AAIP, a través de la cual se aprobaron los criterios orientadores e indicadores de mejores prácticas en la aplicación de la LPDP, establece el criterio orientador respecto de la disociación de datos personales y dispone que "no será considerada persona determinable, en los términos del Artículo 2 de la Ley Nº 25.326, cuando el procedimiento que deba aplicarse para lograr su

[47] PEYRANO, *El acceso a la información pública y las restricciones emergentes del carácter de los datos archivados*, El Derecho, [2005] p. 12.
[48] Artículo 2, LPDP.

identificación requiera la aplicación de medidas o plazos desproporcionados o inviables".[49]

De igual modo, el Convenio 108 define "datos de carácter personal" como cualquier información relativa a una persona física identificada o identificable. A su vez, el informe explicativo del Convenio 108+ del Consejo Europeo aclara que por persona identificable se refiere a una persona que puede ser identificada directa o indirectamente. Además, la noción de "identificable" refiere no solo a la identidad del individuo en sí, sino también a lo que puede permitir "individualizar" o distinguir a una persona de otras, por lo tanto, un número de identificación, un seudónimo, datos biométricos o genéticos, datos de ubicación o una dirección IP podrían considerarse datos personales.[50]

Por el contrario, una persona no se consideraría identificable si su identificación requiriese un tiempo, esfuerzo o recursos irrazonables; solo en ese caso, los datos se considerarían anonimizados. El problema, tal como señala el informe, es que lo que constituye "tiempo, esfuerzo o recursos irrazonables" debe evaluarse caso por caso y podría mutar dependiendo de los desarrollos tecnológicos.[51]

Vemos entonces que pseudonimización no es lo mismo que anonimización. El uso de un pseudónimo o cualquier identificador/identidad digital, no equivale a la anonimización, toda vez que el titular de los datos aún puede ser identificable o individualizado. Es por ello por lo que los datos pseudonimizados sí son considerados datos personales y están alcanzados por la Convención 108.

Por su parte, el Proyecto desplaza a las personas jurídicas como potenciales titulares de datos y establece qué se entiende por "determinable". Al respecto, dispone que se entiende por determinable la persona que puede ser identificada directa o indirectamente por uno

[49] Resolución Nº 4/2019 de la AAIP, Anexo I, Criterio 3.
[50] Informe Explicativo del Convenio 108+, párr. 17-20.
[51] Ibid.

o varios elementos característicos de su identidad física, fisiológica, genética, biométrica, psíquica, económica, cultural, social o de otra índole.[52]

A su vez, el Proyecto aclara que aplicará al tratamiento de datos personales, incluso cuando los datos personales tratados no formen parte de una base de datos o se les haya aplicado medidas de pseudonimización. Solo quedarán excluidos de su ámbito de aplicación la información anónima y aquellos datos anonimizados de forma tal que el titular de los datos no sea identificable.[53]

2.1.5. Derechos de los titulares de datos personales

En lo que respecta a los derechos de los titulares de datos, la LPDP reconoce el derecho de acceso, rectificación, actualización y supresión de sus datos.

2.1.5.1. Derecho de acceso

El Artículo 14 de la LPDP regula el derecho de acceso. En particular, dispone que el titular de los datos, previa acreditación de su identidad tiene derecho a solicitar y obtener información de sus datos personales incluidos en bases de datos públicas, o privadas destinados a proveer informes.

A su vez, el Artículo 4, inc. 6 de la LPDP dispone que el responsable debe almacenarlos de manera tal que permita el ejercicio del derecho de acceso del titular de los datos.

2.1.5.2. Derecho de rectificación, actualización o supresión

Por su parte, el Artículo 16 de la LPDP regula el derecho de rectificación, actualización o supresión. Establece que toda persona tiene derecho a que sus datos sean rectificados, actualizados y, cuando corresponda, suprimidos o sometidos a confidencialidad.

Sin embargo, la supresión de los datos no procede cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, o cuando existiera una obligación legal de

[52] Artículo 2, Proyecto.
[53] Artículo 3, Proyecto.

conservarlos. Además, los datos personales deben ser conservados durante los plazos previstos en las disposiciones legales o contractuales aplicables.[54]

3. Fundamentos de las Tecnologías de Registro Distribuido

En este capítulo, se explorarán los fundamentos de las DLT, brindando una comprensión básica de la diferencia con otros tipos de bases de datos. Se estudiarán los distintos conceptos, diseños, características y propiedades de las DLT y sus fundamentos técnicos, tales como los principios de criptografía y los mecanismos de consenso, junto con otras características clave de estas tecnologías.

3.1. Importancia de los datos y su organización

Los datos frecuentemente son considerados el "petróleo del siglo XXI" ya que poseen un valor estratégico innegable y un impacto significativo en el desarrollo de industrias y tecnologías. Al igual que el petróleo fue fundamental en la revolución industrial, los datos se han convertido en un recurso invaluable en la revolución digital. Son el combustible que impulsa la toma de decisiones, la innovación y el progreso en diversos sectores.

Las empresas e industrias modernas dependen cada vez más de los datos para obtener conocimientos profundos sobre sus clientes, mercados y operaciones internas. Los datos permiten identificar patrones, tendencias y comportamientos, lo que, a su vez, ayuda a optimizar procesos, mejorar la eficiencia y desarrollar productos y servicios personalizados.

En la actualidad, la generación y recopilación de datos ha alcanzado proporciones masivas y continúa creciendo de forma exponencial. La capacidad para almacenar, procesar y analizar esta vasta cantidad de datos ha llevado a avances significativos en inteligencia artificial, aprendizaje automático, computación en la nube y otras tecnologías disruptivas.

[54] Artículo 16, inc. 5, LPDP.

Para poder almacenar, gestionar y tratar esta información, es necesario implementar bases de datos. Ali Sunyaev sostiene que existen tres tipos: bases de datos centralizadas, bases de datos descentralizadas y bases de datos distribuidas.[55]

Las **bases de datos centralizadas** residen en un solo dispositivo de almacenamiento (nodo) y, por lo tanto, son más fáciles de mantener que aquellas que están distribuidas en varios nodos. Sin embargo, estas bases de datos tienen inconvenientes en cuanto a su disponibilidad y rendimiento, es decir, la probabilidad de que el sistema sea accesible en un momento aleatorio y funcione correctamente. El rendimiento general de una base de datos centralizada puede verse afectado si se deben procesar demasiadas solicitudes durante un período específico.

Las **bases de datos descentralizadas** se caracterizan por no tener un almacenamiento central; los datos se almacenan simplemente en múltiples nodos conectados entre sí, pero generalmente separados físicamente. Estos nodos están organizados jerárquicamente, por lo tanto, las bases de datos descentralizadas incorporan múltiples bases de datos centralizadas.

Las **bases de datos distribuidas** se caracterizan por replicar los datos en múltiples nodos físicamente independientes. Cuando un nodo de una base de datos distribuida falla o no es accesible, otros nodos pueden responder a las solicitudes abiertas y proporcionar un resultado similar. Esta distribución permite aumentar la disponibilidad y evitar problemas de rendimiento. A su vez, aunque las bases de datos distribuidas están físicamente separadas en diferentes nodos, las operaciones de una base de datos distribuida siempre deberían retornar los mismos resultados, sin importar en qué nodo se realice la operación. Es por ello que se consideran lógicamente centralizadas, pero arquitectónicamente distribuidas.

[55] SUNYAEV, *Internet Computing: Principles of Distributed Systems and Emerging Internet-Based Technologies*, Springer Nature, Suiza [2005], p. 266-270.

Las **tecnologías de registro distribuido** hacen posible la realización y funcionamiento de las bases de datos distribuidas a través de mecanismos de consenso que permiten a los nodos acordar un registro casi inmutable de las transacciones a pesar de las fallas bizantinas para así lograr consistencia. Esta tecnología se hizo popular con el surgimiento de la criptomoneda Bitcoin, presentada en un white paper publicado en 2008 bajo el seudónimo de Satoshi Nakamoto.[56]

3.2. ¿Qué son las DLT?

Antes de introducir el término, es importante aclarar que, al tratarse de una clase de tecnologías, no existe una única definición para las DLT. Este término abarca a muchas formas distintas de tecnologías registro distribuido que, a su vez, varían ampliamente en términos de complejidad y detalles técnicos.

Las DLT prometen aumentar la eficiencia y la transparencia de las colaboraciones entre individuos y/u organizaciones basadas en cualidades inherentes como la resistencia a la manipulación y a la censura, así como la democratización de los datos. Es por ello que en los últimos años se han desarrollado cada vez más DLT aplicables a distintas industrias y procesos, por ejemplo, la gestión de la cadena de suministro, las finanzas o la atención médica. Cada DLT se basa en un diseño de DLT particular (como Ethereum o IOTA) que se define como una especificación formal de un concepto de DLT (como blockchain) con características únicas.[57]

En términos generales, las DLT son bases de datos digitales compartidas y sincronizadas, que se mantienen mediante nodos físicamente distribuidos, es decir, son bases de datos distribuidas. Las DLT están diseñadas para lograr resiliencia a través de la replicación, esto implica que frecuentemente estén involucradas múltiples partes en el mantenimiento de estas bases de datos. En estos sistemas, los datos se recopilan, almacenan y procesan

[56] NAKAMOTO, *Bitcoin: A Peer-to-Peer Electronic Cash System* [2009].
[57] KANNENGIEßER / LINS / DEHLING / SUNYAEV, "Trade-offs between Distributed Ledger Technology Characteristics", en *ACM Computing Surveys*, 53(2), 42, [2020], p. 2.

de manera descentralizada, utilizando mecanismos de consenso. Además, en principio las tecnologías de registro distribuido solo permiten agregar datos, es decir, los datos solo pueden ser eliminados en circunstancias extraordinarias.[58]

En las DLT, los datos se transfieren y se añaden en forma de transacciones y se almacenan en una secuencia ordenada cronológicamente. Cuando un nodo recibe una nueva transacción, ésta se valida mediante una prueba de propiedad de la representación digital del activo basada en firmas digitales y criptografía de clave pública.[59] Cada transacción contiene metadatos (como el destinatario de la transacción o la marca de tiempo) y una representación digital de ciertos activos (como criptomonedas) o el código de programa de un *smart contract*.

3.2.1. Conceptos, diseños, características y propiedades

Al tratarse de un grupo de tecnologías, cada tipo de DLT abarca diversos conceptos, diseños, características y propiedades. *Veamos*.

Los **conceptos** de DLT describen la estructura básica y el funcionamiento de los diseños de DLT en un nivel abstracto. Por ejemplo, blockchain es un concepto de DLT que describe el uso de bloques que forman una lista enlazada. Cada bloque contiene múltiples transacciones que han sido añadidas al bloque por los nodos. Otros conceptos de DLT no se basan en generar una única cadena de bloques e incluso no utilizan bloques en absoluto. Por ejemplo, el concepto de DLT BlockDAG enlaza bloques generados en un grafo acíclico dirigido (DAG), mientras que en los DAG basados en transacciones (TDAG) las transacciones se enlazan directamente entre sí.[60]

[58] EPRS, *Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law?,* [2019], p. 3.
[59] NOFER / GOMBER / HINZ / SCHIERECK, *Blockchain. Business & Information Systems Engineering*, 59(3), [2017], p. 183-187.
[60] KANNENGIEßER / LINS / DEHLING / SUNYAEV, "Trade-offs between Distributed Ledger Technology Characteristics", en *ACM Computing Surveys*, [2020], p. 4.

Los **diseños** de DLT especifican una descripción abstracta de los conceptos de DLT al agregar valores y procesos concretos para las características inherentes de DLT, como el tamaño máximo de bloque o un mecanismo de consenso para lograr una cierta tolerancia a fallos. Hay diferencias importantes entre los diseños de DLT. Estas diferencias hacen que algunos diseños de DLT sean adecuados para algunas aplicaciones y no adecuados para otras. Por ejemplo, el diseño de DLT Bitcoin crea un nuevo bloque cada 10 minutos y tiene un tamaño de bloque máximo fijo de 1 MB. En contraste, el diseño de DLT Ethereum publica nuevos bloques en promedio cada 17 segundos y el tamaño del bloque es decidido individualmente por los nodos para aumentar la flexibilidad del libro de contabilidad distribuido. Un libro de contabilidad distribuido es una instancia de la especificación formal de un diseño de DLT.[61]

Las **características** de DLT representan características de los diseños de DLT, que pueden ser de naturaleza técnica (por ejemplo, intervalo de creación de bloques) o administrativa (por ejemplo, verificación del controlador del nodo). Las características técnicas limitan los cambios futuros de las características administrativas (por ejemplo, falta de escalabilidad en cuanto al tamaño de la red de un registro distribuido).[62]

Las **propiedades** de DLT son grupos de características compartidas por cada diseño de DLT. Kannengießer identificó 6 propiedades de las DLT: flexibilidad, opacidad, rendimiento, gobernanza, practicidad y seguridad (ver Tabla 1). Por ejemplo, la capacidad y la escalabilidad –ambas características– están asociados con el rendimiento. Aunque todos los diseños de DLT cubren todas las propiedades de DLT, no necesariamente cubren todas las características de DLT. Por ejemplo, los TDAG no utilizan bloques y no presentan características de DLT relacionadas con bloques (como el tamaño del bloque o el intervalo de creación de bloques).

Propiedad DLT	Descripción

[61] KANNENGIEßER / LINS / DEHLING / SUNYAEV, ibid.
[62] KANNENGIEßER / LINS / DEHLING / SUNYAEV, ibid.

Flexibilidad	Grado de libertad en cuanto a la aplicación y personalización del registro distribuido.
Opacidad	Grado de imposibilidad de seguimiento del uso y funcionamiento del registro distribuido.
Rendimiento	Grado de eficiencia en cuanto al uso de recursos informáticos y tiempo para realizar una tarea determinada en un registro distribuido.
Gobernanza	Capacidad de guiar y verificar el correcto funcionamiento de un registro distribuido.
Practicidad	Medida en que los usuarios de un registro distribuido pueden alcanzar sus objetivos con respecto a las limitaciones sociales y sociotécnicas.
Seguridad	Probabilidad de que el funcionamiento del registro distribuido y los datos almacenados no se vean comprometidos.

Tabla 1: Propiedades DLT identificadas por Kannengießer.[63]

3.2.2. Fundamentos técnicos

La mayoría de las DLT utilizan funciones criptográficas para garantizar integridad de los datos y autenticación de identidad. En particular, suelen utilizar funciones *hash* para crear un registro permanente e inalterable de los datos y criptografía de clave asimétrica para autenticar a las partes asociadas a cada transacción.[64]

3.2.2.1. Funciones Hash

El *hashing* es un método para obtener un resultado de tamaño fijo prácticamente único (valor *hash*) para una entrada de casi cualquier tamaño (por ejemplo, un archivo, un texto o una imagen).[65] Para obtener un valor hash, basta con aplicar una función hash a cualquier entrada de información; el cambio más insignificante a dicha información produce un valor hash totalmente distinto. Además, esta función tiene dos características muy importantes: (i) es una función unidireccional, es decir, no es posible aplicar la

[63] KANNENGIEßER / LINS / DEHLING / SUNYAEV, "Trade-offs between Distributed Ledger Technology Characteristics", en *ACM Computing Surveys*, [2020], p. 13.
[64] BACON, *et. al.*, "Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralised Ledgers" en *Richmond Journal of Law and Technology* 1, 62, [2018], p. 4.
[65] YAGA / MELL / ROBY / SCARFONE, "Blockchain Technology Overview" National Institute of Standards and Technology Internal Report 8202 [2018], p. 12

fórmula al valor hash para recuperar el dato inicial; y (ii) es prácticamente imposible que dos datos distintos den como resultado el mismo valor hash.[66]

El algoritmo hash más utilizado en las DLT es el *Secure Hash Algorithm* (SHA) que tiene un tamaño de salida de 256 bits (SHA-256). Este algoritmo tiene una salida de 32 caracteres (8 bits), lo que significa que hay $22^{56} \approx 10^{77}$, o 115.792.089.237.316.195.423.570.985.008.687.907.853.269.984.665.640.564.039.457.584.007.913.129.639.936 posibles valores hash. El algoritmo para SHA-256, así como otros, se encuentra especificado en el Federal Information Processing Standard (FIPS) 180-4.[67]

Valor inicial	Valor Hash (SHA-256)
Hola	e633f4fc79badea1dc5db970cf397c8248bac47cc3acf9915ba60b5d76b0e88f
hola	b221d9dbb083a7f33428d7c2a3c3198ae925614d70210e28716ccaa7cd4ddb79

Tabla 2: Ejemplo de aplicación de SHA-256 en la palabra "hola" cambiando una mayúscula.

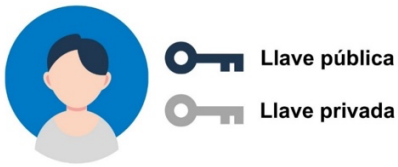
3.2.2.2. Criptografía de clave pública

La criptografía de clave asimétrica (o criptografía de clave pública/privada) utiliza un par de claves: una clave pública y una clave privada que están matemáticamente relacionadas entre sí.[68] Aunque existe una relación entre las dos claves, no es posible conocer la clave privada a partir del conocimiento de la clave pública.

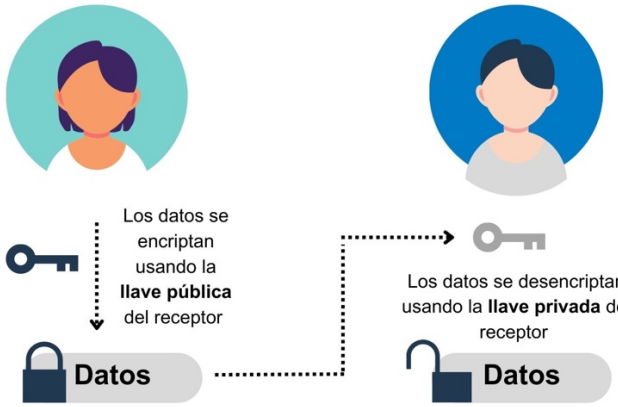
Una infraestructura de clave pública (PKI, por sus siglas en inglés) comprende hardware, software, políticas, procedimientos y roles que se utilizan para la transferencia segura de datos electrónicos a través de una red insegura, como Internet. La criptografía de clave

[66] BACON, *et. al.*, "Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralised Ledgers" en *Richmond Journal of Law and Technology* 1, 62, [2018], p. 6-7.
[67] YAGA / MELL / ROBY /SCARFONE, ibid.
[68] EL IOINI / PAHL, "A Review of Distributed Ledger Technologies" en *OTM 2018 Conferences - Cloud and Trusted Computing* [2018], p. 2.

pública se puede utilizar para cifrar datos, verificar identidades en la red y firmar digitalmente –que a su vez permite verificar la autenticidad del documento firmado.[69]



Los datos se cifran utilizando la clave pública del receptor. Los datos cifrados solo se pueden descifrar utilizando la clave privada que corresponde a la clave pública utilizada para el cifrado.[70] Encontrar una clave privada coincidente con una clave pública correspondiente mediante fuerza bruta no es computacionalmente factible (excluyendo los computadores cuánticos).[71]



En DLT, la clave privada se utiliza para firmar digitalmente una transacción y garantizar que el origen de la transacción sea legítimo. Dado un bloque de datos que necesita ser

[69] SUNYAEV, *Internet Computing: Principles of Distributed Systems and Emerging Internet-Based Technologies*, Springer Nature, Suiza [2005], p. 280.
[70] BACON, *et. al.*, "Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralised Ledgers" en *Richmond Journal of Law and Technology* 1, 62, [2018], párr. 21.
[71] BACON, *et. al.*, "Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralised Ledgers" en *Richmond Journal of Law and Technology* 1, 62, [2018], párr. 26.

firmado digitalmente y la clave privada relevante, la siguiente función produce una firma digital única para ese bloque de datos.[72]

Para verificar si un usuario ha firmado un bloque firmado digitalmente, se deben conocer el bloque de datos, la firma y la clave pública. La siguiente función devuelve una respuesta binaria si un usuario cuya clave pública es conocida ha firmado el bloque de datos.

3.2.2.3. Redes P2P

Como se mencionó anteriormente, las DLT se distribuyen en diferentes nodos de la red, es decir se mantienen mediante dispositivos de almacenamiento y computación físicamente distribuidos. La configuración de estos nodos puede ser sin permiso o con permiso. Los nodos sin permiso permiten a cualquiera crear un nodo y escribir transacciones en el registro mayor participando en el mecanismo de consenso. Los nodos con permiso no pueden ser creados por nadie y/o limitan el acceso de escritura al registro mayor.[73]

A su vez, es posible distinguir entre DLT públicas y privadas. Las DLT públicas permiten que cualquiera pueda leerlas. Las DLT privadas sólo permiten a determinados miembros acceder a su contenido. La distribución y propiedad de los nodos influye en la descentralización del sistema. En general, las DLT públicas sin permisos conducen naturalmente a una mayor descentralización de la red. Dado que cualquiera puede crear un nodo, esto conduce a un mayor número de nodos y a una mayor variabilidad de los intereses de los usuarios participantes. Normalmente, los datos se replican en todos los

[72] BACON, *et. al.*, "Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralised Ledgers" en *Richmond Journal of Law and Technology* 1, 62, [2018], párr. 22.
[73] HUNHEVICZ / HALL, "Do you need a blockchain in construction? Use case categories and decision framework for DLT design options" en *Advanced Engineering Informatics*, 45, 101094 [2020], p. 5.

nodos participantes. Sin embargo, existen opciones de diseño de DLT que no replican los datos en todos los nodos, sino sólo en los nodos a los que se permite acceder a los datos.[74]

	Privada	Pública
Con permiso	DLT con permisos de lectura y escritura.	DLT con acceso de lectura sin permisos y permisos para el acceso de escritura.
Sin permiso	DLT con acceso de lectura autorizado y acceso de escritura sin autorización.	DLT con acceso de lectura y escritura sin permisos.

Tabla 3: Clasificación DLT según configuración de los nodos.

En los diseños de DLT públicos (por ejemplo, Bitcoin), se requiere un mecanismo de incentivos, ya que los nodos validadores deben estar motivados para compartir sus recursos computacionales. El mecanismo de incentivos especifica un esquema de recompensas para los nodos que participan en la generación y/o validación de bloques y transacciones, la búsqueda de consenso y el mantenimiento de la DLT. La participación de los nodos en un libro de contabilidad distribuido para recibir una recompensa monetaria se denomina minería. En consecuencia, los nodos validadores a menudo se denominan mineros. Por ejemplo, los nodos validadores en la red de Bitcoin reciben una cierta cantidad de monedas si son los primeros en crear un nuevo bloque válido. Dichos mecanismos de incentivos se aplican principalmente en las DLT que utilizan nodos con controladores de nodos desconocidos, lo que permite un alto grado de descentralización.[75]

3.2.2.4. Mecanismos de consenso

Todos los nodos de un registro distribuido mantienen una copia local del registro, por lo que todos los nodos deben estar sincronizados y acordar un estado común del registro

[74] HUNHEVICZ / HALL, "Do you need a blockchain in construction? Use case categories and decision framework for DLT design options" en *Advanced Engineering Informatics*, 45, 101094 [2020], p. 5.
[75] KANNENGIEßER / LINS / DEHLING / SUNYAEV, "Trade-offs between Distributed Ledger Technology Characteristics", en *ACM Computing Surveys*, [2020], p. 6.

distribuido para alcanzar la consistencia. Para este propósito, se utiliza un mecanismo de consenso para gestionar la negociación entre los nodos, los cuales (eventualmente) acuerdan un estado común del registro distribuido.[76]

Los mecanismos de consenso se basan en modelos de confianza, que consideran amenazas e incertidumbres en el proceso de búsqueda de consenso, como las fallas bizantinas. Los modelos de confianza forman un conjunto de suposiciones que deben cumplirse para garantizar el consenso entre los nodos (por ejemplo, al menos el 51% de los nodos deben estar de acuerdo en un estado determinado). En Bitcoin, se presentó el primer mecanismo de consenso tolerante a fallas bizantinas que se puede aplicar a gran escala: el consenso Nakamoto basado en *Proof of Work* (PoW). Sin embargo, el consenso Nakamoto tiene varias desventajas, como un rendimiento deficiente, un consumo exhaustivo de energía y vulnerabilidad a ataques a la integridad. Para superar estas desventajas, se han desarrollado numerosos mecanismos de consenso alternativos que ya se han aplicado en diseños de DLT, como *Proof of Stake* (PoS), *Round Robin Consensus Model, Proof of Authority Consensus Model, Proof of Elapsed Time Model*.[77]

En registros distribuidos grandes (por ejemplo, Bitcoin o Ethereum), donde los nodos pueden unirse y abandonar arbitrariamente la red, no es posible alcanzar un consenso entre todos los nodos antes de que los nuevos datos se registren. Por lo tanto, los datos recién agregados no están finalizados y solo se proporciona una finalidad probabilística; existe una cierta probabilidad de que los datos se puedan modificar o eliminar. La probabilidad de finalidad de una transacción aumenta a medida que se agregan más bloques (o transacciones) al libro mayor distribuido después de la transacción. En contraste con la finalidad probabilística, existe la finalidad total, donde todos los nodos

[76] YAGA / MELL / ROBY / SCARFONE, "Blockchain Technology Overview" National Institute of Standards and Technology Internal Report 8202 [2018], p. 18.
[77] YAGA / MELL / ROBY / SCARFONE, "Blockchain Technology Overview" National Institute of Standards and Technology Internal Report 8202 [2018], p. 21-24. Ver también: SUNYAEV, *Internet Computing: Principles of Distributed Systems and Emerging Internet-Based Technologies*, Springer Nature, Suiza [2005], p. 281-283.

están de acuerdo en el nuevo estado antes de que los datos se agreguen. Una vez que se agregan, los datos no se pueden modificar ni eliminar.[78]

4. DLT frente al Régimen de Protección de Datos Personales

4.1. Beneficios

En la siguiente sección ahondaremos en los beneficios que brindan las DLT en relación con la protección de datos personales. Muchas de las características inherentes de las DLT optimizan valores y principios relacionados con la privacidad y las convierten en herramientas poderosas para abordar los desafíos de protección de datos en el mundo digital.

En efecto, la autenticación de la identidad, validación de la exactitud e inalterabilidad de la información, seguridad, descentralización, disminución de los riesgos de usos secundarios y transparencia son todos aspectos importantes para proteger la privacidad de los datos personales y son todas características propias de las DLT. A continuación, se desarrollarán algunos aspectos en los que la adopción de dichas tecnologías en el tratamiento de datos personales resulta beneficiosa.

4.1.1. Seguridad de la información

En los tiempos que corren, la ciberseguridad pasó a ser un tema crítico. A medida que nos volvemos cada vez más dependientes de la tecnología, se vuelve fundamental proteger la información. En efecto, la LPDP requiere que todos aquellos involucrados en el tratamiento de datos personales adopten medidas técnicas y organizativas para garantizar la integridad y la seguridad de los datos.

[78] SUNYAEV, *Internet Computing: Principles of Distributed Systems and Emerging Internet-Based Technologies*, Springer Nature, Suiza [2005], p. 268.

Se estima que a comienzos de 2021 el cibercrimen aumentó un 600%, se calcularon 2.200 ciberataques por día durante 2022 y se espera que ocurran 800.000 a lo largo de 2023.[79] A su vez, según un informe del World Economic Forum, el 91% de los líderes cibernéticos y empresariales entrevistados cree que es probable que en los próximos dos años se produzca un evento cibernético catastrófico y el 43% cree que en ese mismo período es probable que un ciberataque afecte materialmente su organización.[80] Es por eso que las organizaciones están empezando a invertir cada vez más recursos en ciberseguridad.

Las DLT en general son seguras por diseño. Por un lado, al utilizar criptografía asimétrica, la información que se agrega a la DLT está encriptada, por lo tanto, refuerza la privacidad en el tratamiento. A su vez, al tratarse de bases de datos distribuidas y descentralizadas, si se infringen las actualizaciones de la DLT en un nodo, el sistema lo rechaza. Por último, los mecanismos de consenso implican que para que un ataque sea exitoso, el atacante debería tomar control de más del 50% de los sistemas de la red.[81] En una DLT con miles de nodos, esto es sumamente improbable.

Muchos de los riesgos asociados con el uso de servicios de almacenamiento en la nube pueden ser evitados utilizando DLT. Sus fundamentos técnicos y características inherentes aumentan la seguridad de la información. Al respecto, algunos sostienen que blockchain no tiene vulnerabilidades. Si bien bitcoin, la aplicación de blockchain más conocida, ha tenido una mala percepción pública en cuanto a seguridad, en realidad, los hackeos se produjeron en otros sistemas donde se almacenaban claves privadas de bitcoin;

[79] Información publicada por Packetlabs, una compañía de ciberseguridad que compila más de 230 estadísticas sobre seguridad informática (disponible en https://www.packetlabs.net/posts/239-cybersecurity-statistics-2023/)
[80] World Economic Forum, *Global Cybersecurity Outlook* (Enero 2023).
[81] KSHETRI, "Blockchain's roles in strengthening cybersecurity and protecting privacy" en *Telecommunications Policy*, 41(10), [2017]. Ver también: BACON, *et. al.*, "Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralised Ledgers" en *Richmond Journal of Law and Technology* 1, 62, [2018], párr. 45-49.

en efecto, nunca se comprometió ninguna transacción de bitcoin enviada de un usuario a otro.[82]

4.1.2. Responsabilidad proactiva

Otra característica de las DLT es que permiten cumplir con el principio de *accountability* o responsabilidad proactiva receptado por varios marcos regulatorios de protección de datos.

Si bien en Argentina este principio no ha sido adoptado explícitamente, la AAIP incorporó en el Proyecto el principio de responsabilidad proactiva y demostrada y exige que los sujetos involucrados en el tratamiento de datos personales adopten las medidas técnicas, organizativas o de cualquier otra índole que sean útiles, oportunas y efectivas a fin de garantizar un tratamiento adecuado de los datos personales, el cumplimiento de las obligaciones dispuestas por la ley y que permitan demostrar su efectiva implementación.

Las DLT son por definición un registro secuencial de datos, compartido, sincronizado e inmutable. Por esta misma razón, funcionan como "fuente de certeza sobre la ocurrencia de uno o varios hechos sin la intervención de ningún otro elemento de confianza más que su propio funcionamiento".[83] Todo tratamiento de datos queda registrado en la DLT y puede ser auditado, facilitando así la puesta en práctica del principio de responsabilidad proactiva y demostrada.[84]

4.1.3. Validación de la identidad

Un uso interesante de las DLT está relacionado con la validación de la identidad. La Resolución de la AAIP Nº 4/2019 sobre criterios orientadores e indicadores de mejores prácticas de la LPDP dispone que el responsable de la base de datos debe acreditar que

[82] KSHETRI, "Blockchain's roles in strengthening cybersecurity and protecting privacy" en *Telecommunications Policy*, [2017].
[83] https://www.argentina.gob.ar/sites/default/files/2022/08/o_lemon.pdf
[84] KSHETRI, "Blockchain's roles in strengthening cybersecurity and protecting privacy" en *Telecommunications Policy*, [2017].

quien haya prestado el consentimiento sea efectivamente el titular de los datos requeridos y no otra persona, esto es, que cuente con mecanismos de validación de identidad eficaces.

La realidad es que, en el ecosistema digital, garantizar que una persona es quién dice ser es más difícil de lo que parece. En el mundo físico, hemos desarrollado diversas formas de resolver este problema, que suelen implicar algún tipo de "prueba" de las reivindicaciones de identidad, por ejemplo, pasaportes, licencias de conducir y diplomas. En el mundo digital, este tipo de credenciales son necesarias y, si bien se han desarrollado una amplia variedad de mecanismos, el funcionamiento actual de la identidad digital plantea inconvenientes persistentes y cada vez más graves.[85]

Por un lado, la fragmentación de la identidad digital plantea un gran problema. En la actualidad, los usuarios tienen distintas identidades asociadas a distintos nombres de usuario y alias sin que exista una asociación entre ellas. Esto dificulta la interoperabilidad y genera que cada plataforma tenga que implementar sus propios mecanismos de validación de identidad. Por otro lado, los datos personales asociados a la identidad no están debidamente protegidos. Muchas veces, los mecanismos de validación de identidad requieren información adicional de los usuarios y no es debidamente protegida. Esto genera que, por un lado, se incumpla con el principio de minimización del tratamiento, ya que se tratan datos que no son estrictamente necesarios para el fin y, a su vez, agrava el daño de un incidente de seguridad, ya que compromete más información personal.[86]

Para resolver estos problemas, se comenzó a desarrollar el concepto de identidad digital autogestionada. La identidad digital autogestionada permite a las personas interactuar con el mundo digital con la misma libertad y capacidad de confianza que en el mundo físico.[87] Las soluciones de identidad digital autogestionada necesitan registros de información descentralizados e inmutables para poder almacenar las pruebas de la propiedad de los

[85] The European Union Blockchain Observatory & Forum, thematic report on "Blockchain and digital identity" [2019], (disponible en https://www.eublockchainforum.eu/reports).
[86] Ibid.
[87] ALLENDE LÓPEZ, *Identidad Digital Auto gestionada: el futuro de la identidad digital: autogestión, billeteras digitales y blockchain*, ed. Da Silva / Pardo [2020], p. 27.

identificadores únicos y la validez de las credenciales digitales.[88] Por ello, las DLT son una gran herramienta para el desarrollo de estos mecanismos, ya que sirven para crear identificadores digitales (llaves públicas) y proporcionan una infraestructura descentralizada para el control de acceso y consentimiento del uso de datos.[89]

4.2. Aplicaciones y casos de uso relevantes

Además de los beneficios asociados a su uso, la versatilidad de las DLT permite su aplicación en una gran variedad de sectores y se están estudiando aún más usos para esta tecnología innovadora. En efecto, las DLT tendrán un rol fundamental en la próxima generación de Internet, o Web 3.0, ya que permitirá la descentralización y transparencia en el mundo digital.

Algunos de los usos actuales y potenciales de las DLT son los siguientes:

- **Finanzas y criptomonedas**:[90] El sector financiero ha sido uno de los primeros en adoptar DLT. Las criptomonedas, como Bitcoin, se basan en esta tecnología y han revolucionado la forma en que se realizan las transacciones financieras. Las DLT aplicadas a esta finalidad permiten la transferencia segura y transparente de activos digitales, eliminando la necesidad de intermediarios y reduciendo los costos asociados.

- **Registros de propiedad**:[91] Las DLT tienen la capacidad de eliminar la necesidad de registros públicos de propiedad. En efecto, el registro de la titularidad de la propiedad en DLT contribuye a la reducción de gastos y simplifica la determinación de las cadenas de traspaso de la propiedad en el tiempo.

[88] ALLENDE LÓPEZ, *Identidad Digital Auto gestionada: el futuro de la identidad digital: autogestión, billeteras digitales y blockchain*, ed. Da Silva / Pardo [2020] P. 38
[89] The European Union Blockchain Observatory & Forum, thematic report on "Blockchain and digital identity" [2019], (disponible en https://www.eublockchainforum.eu/reports), p. 6
[90] The European Union Blockchain Observatory & Forum, thematic report on "Decentralised Finance (DeFi)" [2022], (disponible en https://www.eublockchainforum.eu/reports.
[91] QUINN / CONNOLLY, "Distributed ledger technology and property registers: displacement or status quo", *Law, Innovation and Technology*, 13:2, 377-397 [2021].

- **Logística y cadena de suministro**: Las DLT ofrecen soluciones para mejorar la trazabilidad y la transparencia en la cadena de suministro.[92] Mediante el registro de cada paso de un producto en la DLT, se puede rastrear su origen, su ubicación y su historial de manejo. Esto permite verificar la autenticidad de los productos, prevenir el fraude y garantizar el cumplimiento de los estándares de calidad. Además, la aplicación de *smart contracts* puede automatizar y agilizar los procesos de pagos y acuerdos entre diferentes actores de la cadena de suministro.[93]

- **Salud y registros médicos**:[94] Las DLT tienen el potencial de transformar la gestión de registros médicos y la interoperabilidad de sistemas de salud. Al utilizar DLT, los registros médicos electrónicos pueden almacenarse de manera segura y descentralizada, permitiendo un acceso controlado y seguro por parte de profesionales de la salud autorizados. Esto mejora la privacidad del paciente, evita la duplicación de registros y facilita la coordinación en el cuidado de la salud. Además, las DLT puede ser utilizado para la trazabilidad de medicamentos, asegurando la autenticidad y el seguimiento de los productos farmacéuticos.

- **Sistemas de votación**: Las DLT son una gran herramienta para realizar procesos de votación electrónica.[95] Al registrar los votos en estas tecnologías, se podría evitar la manipulación y el fraude electoral. Así, la transparencia y la inmutabilidad de la información en DLT podrían garantizar la integridad del proceso.

[92] The European Union Blockchain Observatory & Forum, thematic report on "Blockchain for Supply Chain Transparency" [2022], (disponible en https://www.eublockchainforum.eu/reports).
[93] Ver: https://bfa.ar/blockchain/casos-de-uso/trazabilidad-de-alimentos
[94] The European Union Blockchain Observatory & Forum, thematic report on "Blockchain Applications in the Healthcare Sector" [2022], (disponible en https://www.eublockchainforum.eu/reports).
[95] The European Union Blockchain Observatory & Forum, thematic report on "Governance of and with blockchains" [2020], (disponible en https://www.eublockchainforum.eu/reports), p. 24-25.

- **Identidad digital**: Como se mencionó en la sección anterior, las DLT permiten verificar la identidad de las personas, por eso, son una gran herramienta para desarrollar credenciales de identidad digital. En efecto, en Estonia ya se está utilizando esta tecnología para para generar el sistema de Digi-ID, un sistema de identificación digital.[96]

Estos son solo algunos ejemplos de todos los posibles casos de uso de las DLT. No es sorpresivo que esta tecnología sea incipiente; la capacidad de almacenar, verificar y transferir datos de manera segura y transparente ofrece un potencial significativo para mejorar la eficiencia, la confianza y la privacidad en todo tipo de industrias.

Sin embargo, tal como se desarrollará en las próximas secciones, también plantea desafíos relacionados con la protección de los datos personales.

4.3. Aplicación del Régimen de Protección de Datos a las DLT

A continuación, analizaremos las DLT a la luz del Régimen de Protección de Datos para entender mejor en que medida aplican sus conceptos y principios. A su vez, veremos qué puntos entran en tensión o plantean mayores obstáculos.

4.3.1. Actividades de tratamiento de datos personales en las DLT

Como ya se explicó, la definición de tratamiento de datos personales que brinda la LPDP, tanto como la del Convenio 108+ y el Proyecto, es realmente amplia. Bajo esta definición, el mero almacenamiento de datos personales sería una actividad de tratamiento.

En este sentido, no quedan dudas de que el registro de información en DLT, ya sea para almacenarlos o realizar otro tipo de procesamiento (por ejemplo, utilizarlos para fines analíticos), constituye una actividad de tratamiento de datos personales, sin perjuicio de lo que se haga con esa información posteriormente.

[96] ALLENDE LÓPEZ, *Identidad Digital Auto gestionada: el futuro de la identidad digital: autogestión, billeteras digitales y blockchain*, ed. Da Silva / Pardo [2020], p. 44.

Sin embargo, vale la pena analizar si la excepción de aplicación de la LPDP por uso exclusivamente personal podría ser aplicable en algunas actividades de tratamiento en DLT. Este punto fue analizado bajo GDPR, que contempla la misma excepción que la LPDP, el Convenio 108+ y el Proyecto.

Al respecto, la autoridad de control de protección de datos francesa, la *Commission Nationale de l'Informatique et des Libertés* ("CNIL"), sostuvo que cuando personas físicas ingresan datos personales en una blockchain en el marco de actividades que no sean comerciales ni profesionales (por ejemplo, una persona que compra o vende bitcoin desde su cuenta personal), no pueden ser consideradas responsables del tratamiento a la luz de GDPR por aplicación de la excepción de uso exclusivamente personal.[97]

No obstante, este razonamiento se contradice con el criterio interpretativo de la Corte Europea de Justicia de esta excepción, que en reiteradas ocasiones remarcó que debe interpretarse restrictivamente y referida únicamente a actividades tratamiento de datos que efectúe una persona humana para su uso, propio o de su grupo familiar. Como sostuvo en el caso *Bodil Lindqvist*, esto claramente excluye los casos en los que el tratamiento importa la puesta a disposición de los datos a un número indefinido de personas.[98] Este criterio también fue adoptado por el Grupo de Trabajo del Artículo 29, GDPR.

Así, la Corte Europea de Justicia y el Grupo de Trabajo del Artículo 29 GDPR proponen un estándar doble: no solo analizan la naturaleza de la actividad, sino que también evalúan el nivel de diseminación de los datos personales.

Siguiendo este razonamiento, a diferencia de lo planteado por la CNIL, la excepción de uso exclusivamente personal no parece contemplar al tratamiento de datos personales en DLT. Por un lado, las DLT privadas y/o con permiso suelen utilizarse con fines comerciales, por lo tanto, quedarían excluidas de la excepción por la misma naturaleza de

[97] EPRS, *Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law?,* [2019], p. 11.
[98] Ibid.

la actividad. Por otro lado, si bien las DLT públicas y/o sin permiso podrían utilizarse para fines exclusivamente privados, no estarían alcanzadas por la excepción dado que los datos estarían puestos a disposición de un numero indefinido de personas.[99]

4.3.2. Sujetos obligados en las DLT

Definir los roles y las responsabilidades de los sujetos involucrados en el tratamiento de datos personales en las DLT no es sencillo. En las DLT privadas y/o con permisos suele haber un administrador que actúa como responsable y unos pocos participantes y nodos que a su vez son conocidos por el administrador. Por el contrario, en las DLT públicas y/o sin permisos donde cualquiera puede unirse, leer y escribir, es más difícil determinar quiénes son responsables y quienes encargados. De los desarrolladores, nodos, usuarios y mineros ¿quién decide los fines y los medios del tratamiento?

La respuesta a esta pregunta dependerá de lo que entendamos por "decidir los fines y los medios del tratamiento" y de la interpretación más o menos amplia que hagamos de la corresponsabilidad en el tratamiento de los datos. Al interpretar "medios de tratamiento", el Grupo de Trabajo del Artículo 29 sostuvo que debe entenderse como las cuestiones sustanciales que son esenciales al tratamiento; el cómo se tratan los datos. Esto incluye qué datos se tratan, por cuanto tiempo, con quién se comparten y cómo se procesan. Por lo tanto, el responsable sería el que determina esos aspectos y podría delegar las medidas técnicas y organizativas a los encargados del tratamiento.[100]

En lo que refiere a los medios del tratamiento, la discusión se vuelve más polarizada. Por ejemplo, en el caso *Wirtschaftsakademie Schleswig-Holstein*[101] de la Corte Europea de Justicia, el Abogado General Bot sostuvo que cualquiera que elija una infraestructura técnica particular para realizar actividades de tratamiento puede ser un corresponsable,

[99] EPRS, *Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law?,* [2019], p. 13.
[100] EPRS, *Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law?,* [2019], p. 43. Ver: Opinión 1/2010 del Grupo de Trabajo del Artículo 29 sobre los conceptos de responsable y encargado (WP 169) 00264/10/EN.
[101] Caso C-210/16 Wirtschaftsakademie Schleswig-Holstein [2018] EU:C:2017:796.

aun cuando solo tenga control limitado sobre los fines y ningún control significativo sobre los medios.[102]

A su vez, en el caso *Jehovan todistajat,*[103] la Corte Europea de Justicia confirmó que la corresponsabilidad debe interpretarse de manera amplia. En efecto, sostuvo que una persona humana o jurídica que influencie el tratamiento de datos personales para finalidades propias y que, como resultado de ello participe en la determinación en los fines y medios del tratamiento, puede ser considerado responsable.[104]

Sin embargo, esta posición fue criticada por el Abogado General Bobek en el caso *Fashion ID*,[105] quien advirtió sobre las consecuencias de una interpretación demasiado amplia de corresponsabilidad. Para él, los precedentes citados conducen a que el único criterio relevante para determinar la corresponsabilidad sea haber facilitado el tratamiento.[106]

Así como no existe consenso sobre la interpretación de corresponsabilidad, tampoco existe consenso sobre la determinación de los responsables en DLT. Las DLT están diseñadas de manera tal que una multiplicidad de actores influencia los medios de tratamiento. Por lo tanto, varios de estos actores califican potencialmente como responsables.

En las DLT privadas y/o con permisos, suele haber una entidad o individuo especifica encargada de determinar los medios y, en muchos casos, los fines del tratamiento. En esos casos, esa entidad o individuo sería el responsable. Ahora bien, esto no excluye la posibilidad de que haya corresponsables. Si seguimos el criterio de *Wirtschaftsakademie Schleswig-Holstein*, todos aquellos que utilicen la infraestructura para fines propios serán

[102] EPRS, *Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law?,* [2019], p 40.
[103] Caso C-25/17 Jehovan todistajat[2018] EU:C:20:2018:551.
[104] EPRS, *Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law?,* [2019], p. 42.
[105] Caso C-25/17 Fashion ID [2018] EU:C:2018:1039.
[106] EPRS, *Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law?,* [2019], p. 42.

corresponsables. Por ejemplo, veamos el caso de una DLT conformada por varios actores que participan en una cadena de producción. El creador de la DLT sería el responsable, sin embargo, todos aquellos que haya decidido participar en beneficio propio y, en consecuencia, hayan habilitado el tratamiento de nuevos datos personales, también podrían ser corresponsables.[107]

En las DLT publicas y/o sin permisos es más difícil determinar los responsables. La identidad del responsable dependerá de la perspectiva que se adopte. Por ejemplo, visto desde un nivel macro, la finalidad del tratamiento es "prestar el servicio asociado", mientras que los "medios" se refieren al software utilizado por los nodos y los mineros. Desde una perspectiva micro, la finalidad del tratamiento es "registrar una transacción específica en una DLT", mientras que los medios se refieren "a la elección de la DLT".[108] En el análisis del Panel para el Futuro de la Ciencia y la Tecnología ("STOA") del Parlamento Europeo sobre Blockchain y GDPR, el STOA analizó el rol de los siguientes actores: desarrolladores, mineros, nodos y usuarios.

4.3.2.1. Desarrolladores

Según la opinión de la STOA, los desarrolladores de software son los más alejados a la figura del responsable. Si bien tienen un rol relevante en el diseño y actualización de la DLT, generalmente no son los que deciden sobre la adopción de tales actualizaciones, teniendo poca influencia sobre los medios del tratamiento. Por lo tanto, en líneas generales, los desarrolladores de software no suelen actuar como responsables del tratamiento en contextos DLT.

4.3.2.2. Mineros

En las DLT que funcionan a través de mecanismos de consenso de PoW, los mineros son responsables por la incorporación de nueva información en el registro. Los mineros

[107] EPRS, *Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law?,* [2019], p. 45.
[108] EPRS, *Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law?,* [2019], p. 45.

ejecutan el protocolo, añaden información al registro y pueden descargar una copia de la DLT en sus propias máquinas. Sin embargo, es debatible si estas facultades son determinantes respecto de los medios y los fines del tratamiento. Si bien tienen control significativo sobre los medios al elegir qué versión del protocolo ejecutar, no determinan la finalidad de la transacción en particular. En este sentido, la CNIL determinó que es poco probable que los mineros puedan ser considerados responsables.

4.3.2.3. Nodos

Como se explicó más arriba, los nodos son los dispositivos que almacenan una copia total o parcial de la DLT y participan en la validación de los bloques. Cuando un minero encuentra un hash válido para un bloque, lo transmite a otros nodos, que a su vez ejecutan un cálculo para verificar si el hash es válido y, en caso afirmativo, añaden el nuevo bloque a su propia copia local del registro.

Al iniciar o guardar una transacción en su propio registro, el nodo estaría actuando como responsable, ya que estaría persiguiendo una finalidad propia, *i. e.,* participar en la DLT. Por lo tanto, los nodos pueden entenderse como corresponsables, ya que tienen la influencia suficiente como para elegir, iniciar o cambiar las reglas de una DLT.

4.3.2.4. Usuarios

Los usuarios, que pueden ser tanto personas físicas como jurídicas, son aquellos que firman y envían transacciones a la DLT. Los usuarios podrían ser considerados responsables del tratamiento de datos cuando el diseño de la DLT conduce al hecho de que sólo el usuario que realiza la transacción puede determinar los fines y los medios del tratamiento de datos, es decir, registrar una transacción específica en la DLT.

A su vez, la citada opinión de la STOA señala en que los usuarios pueden ser tanto responsables respecto de los datos que registran en la DLT, como encargados, por ejemplo, cuando almacenan una copia completa del registro en su propio dispositivo.[109]

4.3.3. Aplicación extraterritorial de la ley en las DLT

Las DLT tienen una naturaleza transfronteriza. Por lo tanto, es necesario analizar la aplicación extraterritorial de la LPDP en un contexto de descentralización extrema.

Siguiendo el criterio explicado en la sección 2.1.3., bajo la normativa actual, podría argumentarse que el tratamiento de datos personales bajo las tecnologías DLT solo estaría alcanzado en tanto se traten datos personales de personas físicas o jurídicas con domicilio legal o delegación o sucursales en Argentina. El Proyecto refuerza esta posición, ya que específicamente prevé que la ley será aplicable aun cuando el responsable o encargado, no se encuentra establecido en Argentina en la medida que realice actividades de tratamiento de datos personales de cualquier tipo en Argentina de personas que se encuentran en dicho territorio.

Además, a diferencia de GDPR, no sería necesario analizar si el uso de dichas tecnologías cae dentro de alguno de los dos supuestos planteados por GDPR, si no que, bajo el Proyecto, basta con determinar si se están tratando datos personales de titulares de datos argentinos para que este sea aplicable.

Una problemática que plantean las DLT en relación con este punto es que suelen estar alcanzadas por múltiples normas de protección de datos personales.

Si una empresa actúa como responsable por el tratamiento de una base de datos utilizada en múltiples jurisdicciones, deberá verificar la existencia de normas de protección de datos personales y cumplir con ellas. En cambio, en una DLT pública y sin permisos, donde no está tan claro quién determina los medios y fines del tratamiento de datos ¿quién

[109] EPRS, *Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law?,* [2019], p. 47.

es responsable de verificar el cumplimiento con la normativa aplicable?. En esta misma línea, ¿quién es responsable de verificar el cumplimiento de los requisitos aplicables a la transferencia internacional de datos personales? Las respuestas a estas preguntas dependerán del criterio que se adopte para identificar a los responsables tal como se expuso en la sección anterior.

4.3.4. Datos personales

El punto más importante para analizar quizás sea determinar qué datos personales son tratados en las DLT. Como explicamos en el capítulo anterior, los datos que se añaden al registro suelen ser los *hash* de otros datos e información transaccional ¿En qué medida pueden ser considerados datos personales?

Por un lado, las llaves públicas pueden ser consideradas datos personales toda vez que permiten identificar a un titular de datos. Como se explicó en la sección 2.2.2.2., cada usuario en la DLT posee una llave pública que comparte con terceros para realizar transacciones. A su vez, cada usuario posee una llave privada que sería una suerte de código o contraseña que está relacionada matemáticamente con la llave publica y que permite desencriptar información que fue encriptada con la llave pública.

Las llaves publicas ocultan la identidad del usuario, salvo que se relacionen con información adicional. En la práctica, esta asociación puede ocurrir por la revelación voluntaria de la llave publica por parte del usuario para recibir fondos, la revelación ilícita tras un incidente de seguridad o porque se requiere la revelación de información adicional para cumplir con obligaciones legales tales como KYC o prevención de lavado de dinero.[110] En este sentido, las llaves públicas serían datos pseudonimizados y estarían alcanzadas por el Régimen de Protección de Datos.

A su vez, a través de la llave publica se puede acceder a información transaccional adicional. Esta información abarca cualquier otro dato que no sean llaves públicas y que

[110] EPRS, *Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law?,* [2019], p. 27.

se utilicen en las DLT. Por ejemplo, la información transaccional podría ser el nombre, dirección o email incluidos en determinada transacción.[111]

Para determinar si la información transaccional califica como datos personales, se debe evaluar cada caso en particular. En efecto, resulta evidente que, si la información transaccional refiere a datos sobre mercadería en el contexto de una DLT utilizada en procesos de producción, no serían datos personales. Ahora bien, si un grupo de entidades financieras utilizan DLT para compartir información referida a requerimientos KYC, parecería que esa información sí revestiría carácter personal.[112] En síntesis, para determinar si la información transaccional califica como datos personales hay que evaluar si es información relacionada a una personal determinada o determinable.

Se debe tener en cuenta que tanto las llaves públicas como la información transaccional puede almacenarse en las DLT en texto simple, hasheada o encriptada.[113] Para establecer si en los dos últimos casos la información reviste carácter personal, es necesario determinar si los mecanismos de hash y criptografía devuelven datos pseudonimizados o anonimizados.

Como ya se explicó, la función hash es unidireccional, es decir, no puede aplicarse a un valor hash para revelar el valor original. Sin embargo, si se conoce la gama de valores de entrada de la función hash pueden ser reproducidos para obtener el valor de un registro concreto. En consecuencia, el Grupo de Trabajo del Artículo 29, GDPR, ha advertido que las funciones hash son una medida de seguridad útil ya que reducen la probabilidad de asociación de un conjunto de datos con la identidad original del titular, pero no un método de anonimización.[114]

[111] Ibid.
[112] EPRS, *Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law?,* [2019], p. 28.
[113] EPRS, *Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law?,* [2019], p. 29.
[114] EPRS, *Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law?,* [2019], p. 30,

Otro enfoque es el de la *Personal Data Protection Commission* (PDPC) de Singapur, que considera que son datos personales todos aquellos que sean accesibles a través de la DLT. Esto no solo incluye los datos que se recolecten como parte de una transacción (nombre, dirección y todo metadato relacionado), sino también los datos personales que se conserven fuera del registro pero que sean accesibles a través de enlaces visibles en la cadena y/o sean accesibles para todos los participantes de la cadena sin control de accesos.[115]

4.4. Los desafíos que plantean las DLT

Como se mencionó a lo largo de este trabajo, las DLT están diseñadas para garantizar la integridad de los datos y la confianza en la red al dificultar la eliminación o modificación unilateral de los datos. Sin embargo, esto plantea una colisión con el Régimen de Protección de Datos Personales toda vez que dificultan el ejercicio de los derechos de los titulares; va en contra del principio de limitación de la conservación de los datos personales; y no es claro contra quién se deben ejercer los derechos.

4.4.1. Supresión y rectificación de datos personales en DLT

Suprimir o modificar datos registrados en una DLT es difícil. Esto es así porque estas redes suelen estar diseñadas para dificultar la modificación unilateral de los datos para garantizar la integridad de los datos y, así, generar confianza en la red. Por ejemplo, en las DLT donde el mecanismo de consenso utilizado es el PoW, para suprimir un dato la mayoría de los nodos conectados tendrían que verificar de nuevo la legitimidad de cada transacción efectuada hacia atrás, deshacer toda la DLT bloque a bloque y reconstruirla, y luego distribuir cada paso de transacción bloque a bloque a todos los nodos existentes.[116]

[115] PDPC (Personal Data Protection Commission Singapore), "Consideraciones para el diseño de blockchain", p. 9. Disponible en https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Blockchain-Guide_final.ashx?la=en.
[116] EPRS, *Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law?,* [2019], p. 75

Por lo tanto, el ejercicio de estos derechos se ve dificultado por factores técnicos, pero también por el diseño de la gobernanza. Incluso si hubiera una manera de garantizar la supresión o modificación de una perspectiva técnica, podría ser difícil desde el punto de vista organizativo conseguir que todos los nodos apliquen los cambios en su propia copia del registro (especialmente en las DLT públicas y sin permisos).

Ahora bien, para poder analizar si es posible suprimir datos en una DLT primero hay que entender que significa "supresión". Por su parte, la LPDP no profundiza en el significado de supresión. Es lógico pensar que supresión equivale a la destrucción total de los datos, de hecho, este fue el criterio adoptado por la Corte Europea de Justicia en el caso *Nowak*.

Sin embargo, puede haber alternativas a la destrucción que podrían garantizar el cumplimiento del derecho de supresión establecido en la LPDP. Por ejemplo, al analizar la supresión bajo GDPR, la Autoridad de Protección de Datos de Austria reconoció que la anonimización podría considerarse como un medio para lograr la supresión de los datos. Por otro lado, la Oficina del Defensor de la Información del Reino Unido sostiene hace tiempo que "poner los datos fuera de uso" es suficiente en términos de supresión.

Como vemos, no hay un criterio único sobre lo que implica la supresión de los datos. A los fines de este trabajo, entendemos que la supresión puede ser alcanzada a través de la destrucción o la anonimización (ya que en este caso los datos quedarían fuera del ámbito de aplicación de la LPDP).

Teniendo en cuenta estas problemáticas, algunos proponen como solución la destrucción de la clave privada, lo que generaría que los datos encriptados con una clave pública sean inaccesibles. En efecto, esta fue la alternativa propuesta por la CNIL al sugerir que la supresión podía ser alcanzada cuando la clave privada de la función hash se elimina junto con la información de otros sistemas en los que se almacenó para su procesamiento. Sin embargo, la aplicación de esta medida no eliminaría los hashes de la DLT. Como mencionamos anteriormente, habría que evaluar si esto constituye la pseudonimización o la anonimización de los datos para después evaluar si es suficiente para dar cumplimiento

al derecho de supresión. Además, esto implicaría el bloqueo de toda la información asociada a esa clave pública ¿qué pasa si el titular solo quiere eliminar un dato?

Por otro lado, otros proponen que los datos de carácter personal sean almacenados *off-chain*, es decir, en una base de datos externa a la DLT y que solo se almacene el hash asociado a esos datos en la DLT.[117] Esta alternativa no podría aplicarse a las llaves públicas. Sin perjuicio de ello, no resulta claro si el hash que queda registrado en la DLT pero que deja de estar asociado a los datos externos podría ser considerado un dato personal. Como mencionamos arriba, la función hash es unidireccional, es decir, no puede obtenerse el valor inicial por medio del valor hash. Ahora bien, sería posible asociar ese hash a un dato personal utilizando información adicional.

Más allá de este interrogante, los datos *off-chain* deben estar controlados por al menos un tercero confiable, lo que reduce el grado de descentralización de las aplicaciones en DLT (esta solución no podría aplicarse a DLT públicas y sin permisos). Además, se genera otra problemática, ya que es necesario garantizar la confidencialidad y disponibilidad de esta nueva base de datos externa.[118] Al final, se genera un *trade-off*, donde el desarrollador de la DLT debe elegir sacrificar algunas propiedades beneficiosas de estas tecnologías para poder garantizar el cumplimiento con la LPDP.

Además, cabe destacar que la LPDP exige que los datos sean destruidos cuando dejan de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados, aun cuando el titular no hubiera solicitado la supresión.[119] Por lo tanto, más allá de las dificultades que puedan plantear las solicitudes de rectificación o supresión de datos de una DLT, la propia naturaleza permanente de estas tecnologías colisiona con el principio de limitación de conservación.

[117] EPRS, *Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law?,* [2019], p. 32.
[118] KANNENGIEßER / LINS / DEHLING / SUNYAEV, "Trade-offs between Distributed Ledger Technology Characteristics", en *ACM Computing Surveys*, [2020], p. 26.
[119] Artículo 4, LPDP.

4.4.2. ¿Quién es responsable de garantizar el ejercicio de estos derechos?

Por último, siguiendo lo expuesto en la sección 4.3.2., no es tarea fácil determinar quién o quiénes son los responsables por el tratamiento en un contexto DLT. Por lo tanto, no es claro a quién debería solicitarle el ejercicio de sus derechos un titular de datos. Aun cuando fuera claro cuáles son los individuos o entidades que actúan como responsables (por ejemplo, los nodos), quizás no sea fácil acceder a su identidad.

Es por ello por lo que la CNIL señaló que cuando un grupo decide utilizar colectivamente una DLT, deben determinar quién será el responsable *ab initio*.[120] Además, sugirió la posibilidad de crear una nueva persona jurídica o de designar una persona jurídica existente como responsable del tratamiento. Esto permite a los titulares identificar la entidad con la que deben ponerse en contacto para hacer valer sus derechos y proporciona un único punto de contacto para las autoridades de protección de datos.

Sin embargo, debe tenerse en cuenta que una iniciativa de este tipo no impediría, sin embargo, la identificación de otros corresponsables del tratamiento por decisiones judiciales posteriores, y la imposición de obligaciones relacionadas con la LPDP a estos actores.

5. Conclusiones y Reflexiones Finales

A lo largo del presente trabajo se contrastaron los beneficios y los desafíos legales que implican las DLT en lo que refiere al tratamiento de datos personales. A tal fin, primero se analizó el Régimen de Protección de Datos Personales, luego se estudiaron los fundamentos, características y definición de las DLT y por último se expusieron los valores de privacidad que optimizan las DLT, los posibles casos de uso de estas tecnologías y los retos que plantean en términos de protección de datos personales.

[120] EPRS, *Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law?,* [2019], p. 45.

En conclusión, nos encontramos ante un escenario crucial en el que se deben tomar decisiones estratégicas y equilibradas en relación con el tratamiento de datos personales en las DLT. Si bien plantean obstáculos y desafíos para garantizar los derechos de los titulares de datos, no podemos pasar por alto los beneficios significativos que las DLT ofrecen en términos de autenticación de identidad, seguridad, descentralización y transparencia.

Los reguladores y desarrolladores de todo el mundo estan comenzando a abordar esta problemática y buscar posibles soluciones. En el caso de Argentina, el BCRA dispuso en su última comunicación sobre ciberseguridad que las entidades financieras deberán tener en consideración los aspectos de protección de datos personales en el uso de tecnologías de registros distribuidos al evaluar los riesgos relacionados con la tecnología y seguridad de la información, sin embargo, no especifica cómo deben hacerlo.[121]

Asimismo, varios organismos del sector público de la nación están colaborando con representantes del sector privado, académico y de la sociedad civil en el proyecto de Blockchain Federal Argentina (BFA), una plataforma multiservicios abierta y participativa pensada para integrar servicios y aplicaciones sobre blockchain. Algunos de los casos de uso enumerados en el sitio web oficial son: licitaciones públicas, trazabilidad de alimentos, títulos académicos y pólizas de caución.[122]

Cabe resaltar que la página de BFA promulga que la BFA no entra en conflicto con el derecho de supresión de datos ya que "el almacenamiento de información es *off-chain*, esto quiere decir que la plataforma no funciona como una nube para almacenar archivos, sino que cada servicio desplegado es responsable de los mismos. En el registro de BFA sólo se almacenan los digestos criptográficos (los hashes) de esos archivos, lo que basta para garantizar que los mismos no han sido modificados". Pero siguiendo todo lo expuesto, vimos que esto no siempre es suficiente.

[121] Comunicación "A" 7724 del BCRA.
[122] Puede acceder al sitio web oficial de Blockchain Federal Argentina en https://bfa.ar/.

Por eso, teniendo en cuenta que el Régimen de Protección de Datos se encuentra actualmente en miras de ser actualizado, es esencial que se dé espacio a esta discusión para desarrollar una ley que brinde claridad y certeza a una situación que aún esta lejor de serlo. Si bien es cierto que el Proyecto de la AAIP introduce el principio de neutralidad tecnológica, cabe preguntarse en qué medida se puede aplicar una regulación neutral a la tecnología, sin tener en cuenta que puede haber sistemas que por su naturaleza requieren de una interpretación particularizada de los principios, tales como las DLT.

En última instancia, nos enfrentamos a un camino que se bifurca: ¿ignoraremos que las DLT llegaron para quedarse y adoptaremos soluciones a medias, dejando vacíos normativos y interrogantes sin resolver? ¿o aprovecharemos esta oportunidad para desarrollar un marco normativo sólido que brinde soluciones prácticas a los desafíos que plantea el ecosistema digital en constante evolución?

La respuesta a estas preguntas y la dirección que tomemos serán fundamentales para determinar el futuro de la protección de datos en un mundo donde las DLT tienen cada vez más preponderancia. Es esencial que las autoridades de protección de datos y los legisladores trabajen en conjunto para encontrar un equilibrio entre la innovación y la regulación, de modo que se fomente el desarrollo de las DLT sin dejar de lado la protección de los derechos de los titulares de datos.

Referencias bibliográficas

- ALLENDE LÓPEZ, *Identidad Digital Auto gestionada: el futuro de la identidad digital: autogestión, billeteras digitales y blockchain*, ed. Da Silva / Pardo [2020].
- BACON, *et. al.*, "Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralised Ledgers" en *Richmond Journal of Law and Technology* 1, 62, [2018].
- EL IOINI / PAHL, *A Review of Distributed Ledger Technologies* en Springer Nature, Suiza, AG [2018].
- EPRS, "Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law?". Informe elaborado a solicitud del Panel para el Futuro de la Ciencia y la Tecnología (STOA) y gestionado por la Unidad de Previsión Científica, dentro de la Dirección General de Servicios de Investigación Parlamentaria (EPRS) del Secretariado del Parlamento Europeo [2019].
- EUSTICE / BOHN, "Navigating the Gauntlet: A Survey of Data Privacy Laws in Three Key Latin American Countries" en *The Sedona Conference Journal*, 14, [2013].
- GAKH, "Argentina's Protection of Personal Data: Initiation and Response*"* en *A Journal of Law and Policy for the Information Society*, 2(3), [2006].
- GREENLEAF, «Global Tables of Data Privacy Laws and Bills» en *Privacy Laws & Business International Report (PLBIR),* 157, 6, [2019].
- GREGORIO, *Protección de Datos Personales en América Latina*, Instituto de Investigación para la Justicia [2016].
- HUNHEVICZ / HALL, "Do you need a blockchain in construction? Use case categories and decision framework for DLT design options" en *Advanced Engineering Informatics*, 45, 101094 [2020].
- KANNENGIEßER / LINS / DEHLING / SUNYAEV, "Trade-offs between Distributed Ledger Technology Characteristics", en *ACM Computing Surveys*, 53(2), 42, [2020].
- KORFF / GEORGES, *The Origins and Meaning of Data Protection*, [2020], p 3. (Disponible en SSRN https://ssrn.com/abstract=3518386 o http://dx.doi.org/10.2139/ssrn.3518386).
- KSHETRI, "Blockchain's roles in strengthening cybersecurity and protecting privacy" en *Telecommunications Policy*, 41(10), [2017].

- MCCLEARY, "To discovery and beyond: comprehensive look at Argentina's data protection laws" en *University of Miami Inter-American Law Review*, 47(1), 129-[ix], [2015].
- NAKAMOTO, *Bitcoin: A Peer-to-Peer Electronic Cash System* [2009].
- NOFER / GOMBER / HINZ / SCHIERECK, *Blockchain. Business & Information Systems Engineering*, 59(3), [2017].
- PDPC (Personal Data Protection Commission Singapore), "Consideraciones para el diseño de blockchain". Disponible en https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Blockchain-Guide_final.ashx?la=en.
- PEYRANO, *El acceso a la información pública y las restricciones emergentes del carácter de los datos archivados*, El Derecho, [2005].
- PUCCINELLI, *Protección de datos de carácter personal*, Buenos Aires, Astrea, [2004].
- QUINN / CONNOLLY, "Distributed ledger technology and property registers: displacement or status quo", *Law, Innovation and Technology*, 13:2, 377-397 [2021].
- SUNYAEV, *Internet Computing: Principles of Distributed Systems and Emerging Internet-Based Technologies*, Springer Nature, Suiza [2005].
- The European Union Blockchain Observatory & Forum, thematic report on "Decentralised Finance (DeFi)" [2022], (disponible en https://www.eublockchainforum.eu/reports).
- The European Union Blockchain Observatory & Forum, thematic report on "Blockchain for Supply Chain Transparency" [2022], (disponible en https://www.eublockchainforum.eu/reports).
- The European Union Blockchain Observatory & Forum, thematic report on "Blockchain Applications in the Healthcare Sector" [2022], (disponible en https://www.eublockchainforum.eu/reports).
- The European Union Blockchain Observatory & Forum, thematic report on "Governance of and with blockchains" [2020], (disponible en https://www.eublockchainforum.eu/reports).
- The European Union Blockchain Observatory & Forum, thematic report on "Blockchain and digital identity" [2019], (disponible en https://www.eublockchainforum.eu/reports).

- The European Union Blockchain Observatory & Forum, thematic report on "Metaverse" [2022], (disponible en https://www.eublockchainforum.eu/reports).
- TRONCOSO REIGADA, «El desarrollo de la protección de datos personales en iberoamérica desde una perspectiva comparada y el reequilibro en los modelos de protección de datos a nivel internacional» en *Revista Internacional de Protección de Datos Personales*, 1 [2012].
- YAGA / MELL / ROBY /SCARFONE, "Blockchain Technology Overview" National Institute of Standards and Technology Internal Report 8202 [2018].

- Convenio Europeo de Derechos Humanos de 1950.
- Caso C-101/01 Bodil Lindqvist [2003] EU:C:2003:596.
- Caso C-210/16 Wirtschafsakademie Schleswig-Holstein [2018] EU:C:2017:796.
- Caso C-25/17 Jehovan Todistajat [2018] EU:C:2018:551.
- Caso C-40/17 Fashion ID GmbH [2018] EU:C:2018:1039, Opinión de AG Bobek.
- Caso C-434/16 Nowak [2017] EU:C:2017:994.
- Comunicación "A" 7724 del BCRA.
- Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos Personales (Convenio 108).
- Grupo de Trabajo del Artículo 29, Opinión 1/2010 sobre los conceptos de responsable y encargado (WP 169) 00264/10/EN.
- Pacto Internacional de Derechos Civiles y Políticos de 1966.
- Protocolo de Modernización del Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos Personales (Convenio 108+).
- Resolución Nº 119/2022 de la AAIP.
- Resolución Nº 14/2018 de la AAIP.
- Resolución Nº 145/2022 de la AAIP.
- Resolución Nº 159/2018 de la AAIP.
- Resolución Nº 4/2019 de la AAIP.
- Resolución Nº 60-E/2016 de la AAIP.
- Resolución Nº 69/2020 de la AAIP.