v.2, n.6, 2025 - Junho

REVISTA
O UNIVERSO OBSERVÁVEL

BLOCKCHAIN Y PROTECCIÓN DE DATOS PERSONALES: TENSIONES ENTRE LA INMUTABILIDAD Y EL DERECHO DE SUPRESIÓN

BLOCKCHAIN AND PERSONAL DATA PROTECTION: TENSIONS BETWEEN IMMUTABILITY AND THE RIGHT TO BE FORGOTTEN

Angie Gabriela Sánchez Erazo[1]
Mario Francisco Cuvi Santacruz[2]

Revista o Universo Observável
DOI: 10.69720/29660599.2025.000109
ISSN: 2966-0599

[1]Abogada de los Tribunales y Juzgados de la República del Ecuador por la Universidad de Guayaquil (UG), Magíster en Derecho de Comercio Internacional por la Universidad Internacional de la Rioja (UNIR), Máster en Banca y Sistemas Financieros por la Universidad Tech Tecnológica (UTECH), Especialista en Sostenibilidad y Responsabilidad Social Empresarial, Especialista en Cumplimiento y Anticorrupción por la Universidad Internacional Sek (UISEK), Doctoranda en Derecho Económico y de la Empresa por la Universidad Internacional Iberoamericana (UNINI); Investigadora y Docente de la Universidad Ecotec
E-mail: ab.angiesanchezerazo@hotmail.com
ORCID: https://orcid.org/0000-0003-4050-7298
[2]Abogado de los Tribunales y Juzgados de la República del Ecuador por la Universidad de Especialidades Espíritu Santo (UEES), Magíster en Derecho (LL.M.) por la Universidad de Melbourne (Unimelb), Doctor en Ciencias Sociales y Jurídicas por la Universidad de Córdoba (UCO); Director Ejecutivo de Posgrado e investigador de la Universidad ECOTEC
E-mail: cuvimario@gmail.com
ORCID: https://orcid.org/0000-0001-6688-4660

REVISTA O UNIVERSO OBSERVÁVEL

v.2, n.6, 2025 - Junho

BLOCKCHAIN Y PROTECCIÓN DE DATOS PERSONALES:
TENSIONES ENTRE LA INMUTABILIDAD Y EL DERECHO DE SUPRESIÓN

Angie Gabriela Sánchez Erazo e Mario Francisco Cuvi Santacruz

PERIÓDICO CIENTIFÍCO INDEXADO INTERNACIONALMENTE

ISSN
International Standard Serial Number
2966-0599
www.ouniversoobservavel.com.br

Editora e Revista
O Universo Observável
CNPJ: 57.199.688/0001-06
Naviraí – Mato Grosso do Sul
Rua: Botocudos, 365 – Centro
CEP: 79950-000

REVISTA UNIVERSO OBSERVÁVEL
O Conhecimento é o horizonte de eventos.
ISSN: 2966-0599
contato@ouniversoobservavel.com.br
www.ouniversoobservavel.com.br
Periódico Científico Indexado

RESUMEN

La tecnología blockchain se ha consolidado como uno de los pilares de la innovación tecnológica contemporánea, al ofrecer una estructura descentralizada, segura e inmutable para la gestión de datos. Sin embargo, su uso en contextos donde prevalecen derechos fundamentales, como la protección de datos personales, ha generado un debate jurídico considerable. La inmutabilidad, considerada una de las principales fortalezas de esta tecnología, colisiona con conceptos como el derecho de supresión o el derecho de supresión, un principio consagrado en diversos ordenamientos jurídicos y que permite a las personas exigir la eliminación de sus datos personales cuando estos ya no son necesarios. Este artículo analiza dicha tensión desde un enfoque interdisciplinario, considerando aspectos jurídicos, éticos y tecnológicos. Se aborda la problemática desde la normativa internacional de protección de datos (como el RGPD), las propuestas legales en Ecuador y experiencias comparadas en países como Francia, Alemania y Brasil. Además, se exploran posibles soluciones tecnológicas como los smart contracts modificables o el uso de blockchain híbridas. El análisis se apoya en una metodología descriptiva, bibliográfica y fenomenológica jurídica. Este trabajo concluye que es posible armonizar ambos intereses mediante mecanismos de pseudonimización, segmentación de información y regulación adaptativa que respete tanto la innovación como los derechos fundamentales.

Palabras clave: Blockchain, protección de datos, inmutabilidad, privacidad digital, normativa ecuatoriana, ética tecnológica.

ABSTRACT

Blockchain technology has become one of the cornerstones of modern technological innovation, offering a decentralized, secure, and immutable structure for data management. However, its implementation in contexts involving fundamental rights—particularly personal data protection—has raised significant legal debates. Immutability, one of blockchain's core strengths, conflicts with the right to be forgotten, a principle enshrined in several legal systems that allows individuals to request the deletion of their personal data. This article analyzes this tension from an interdisciplinary approach, considering legal, ethical, and technological aspects. It examines international data protection regulations (such as the GDPR), Ecuadorian legislative proposals, and comparative experiences in France, Germany, and Brazil. Technological solutions like modifiable smart contracts and hybrid blockchain architectures are also explored. The research relies on descriptive, bibliographical, and juridical-phenomenological methodologies. The findings suggest that it is possible to harmonize innovation and human rights through pseudonymization, information segmentation, and adaptive regulation.

Keywords: *Blockchain, right to be forgotten, data protection, immutability, digital privacy, Ecuadorian law, legal ethics.*

RESUMO

A tecnologia blockchain tornou-se um dos pilares da inovação tecnológica contemporânea, oferecendo uma estrutura descentralizada, segura e imutável para o gerenciamento de dados. No entanto, sua aplicação em contextos que envolvem direitos fundamentais, como a proteção de dados pessoais, tem gerado intensos debates jurídicos. A imutabilidade, vista como uma das maiores virtudes da blockchain, entra em conflito com o direito ao esquecimento, um princípio consagrado em diversas legislações que permite às pessoas solicitarem a exclusão de seus dados pessoais. Este artigo analisa essa tensão a partir de uma abordagem interdisciplinar, considerando aspectos jurídicos, éticos e tecnológicos. Examina-se a normativa internacional (como o RGPD), as propostas legislativas no Equador e experiências comparadas na França, Alemanha e Brasil. Também são exploradas soluções tecnológicas, como contratos inteligentes modificáveis e blockchains híbridas. A pesquisa adota metodologias descritiva, bibliográfica e fenomenológica jurídica. Os resultados indicam que é possível harmonizar inovação e direitos fundamentais mediante pseudonimização, segmentação de dados e regulamentações adaptativas.

Palavras-chave: Blockchain, direito ao esquecimento, proteção de dados, imutabilidade, privacidade digital, legislação equatoriana, ética jurídica.

INTRODUCCIÓN

En los últimos años, la tecnología blockchain ha irrumpido con fuerza en diversos sectores, destacándose principalmente en el ámbito financiero con el auge de las criptomonedas, pero expandiéndose rápidamente hacia campos como la gestión de registros públicos, contratos inteligentes y protección de datos. Esta tecnología se caracteriza por su estructura descentralizada, su transparencia y, sobre todo, por la inmutabilidad de la

ISSN: 2966-0599
contato@ouniversoobservavel.com.br
www.ouniversoobservavel.com.br
Periódico Científico Indexado

información registrada. Dicho principio de inmutabilidad garantiza que, una vez que los datos han sido ingresados en una cadena de bloques, estos no pueden ser alterados ni eliminados, lo cual representa una ventaja en términos de seguridad y confianza (Tapscott & Tapscott, 2016, p. 34).

No obstante, esta cualidad se convierte en un desafío jurídico cuando se superpone con el derecho fundamental a la protección de datos personales y, más específicamente, con el derecho a supresión. Este derecho, consagrado en instrumentos internacionales como el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, permite a los individuos solicitar la supresión de su información personal cuando esta ya no sea necesaria o cuando se haya obtenido de forma indebida (European Parliament, 2016, art. 17).

La problemática surge, entonces, al enfrentar dos principios aparentemente incompatibles: por un lado, la inmutabilidad de blockchain, y por otro, el derecho de supresión que requiere la posibilidad de eliminar o rectificar información. Esta tensión ha generado un amplio debate en el ámbito jurídico y tecnológico sobre la viabilidad de implementar soluciones compatibles con ambos principios (Finck, 2018, p. 78).

En este contexto, resulta fundamental preguntarse cómo puede el Derecho adaptarse a las nuevas realidades tecnológicas sin vulnerar derechos fundamentales. La tecnología, por naturaleza, evoluciona más rápidamente que la legislación, lo que plantea serios retos para los operadores jurídicos, quienes deben interpretar las normas a la luz de innovaciones disruptivas que no siempre fueron previstas por el legislador (De Filippi & Wright, 2018, p. 102).

La protección de datos personales ha adquirido un estatus prioritario dentro de los sistemas jurídicos contemporáneos. En América Latina, países como Brasil han adoptado marcos normativos como la Lei Geral de Proteção de Dados (LGPD), que replican en gran medida las disposiciones del RGPD, incluyendo la posibilidad de ejercer el derecho de supresión (Doneda & Monteiro, 2020, p. 156).

Ecuador no ha sido ajeno a estas transformaciones. Con la entrada en vigor de la Ley Orgánica de Protección de Datos Personales (2021), el país reconoce el derecho de supresión como una garantía de los titulares de datos, lo que implica la necesidad de implementar mecanismos efectivos para su cumplimiento, incluso frente a tecnologías disruptivas como blockchain (Registro Oficial, 2021, art. 16).

Frente a este panorama, diversas propuestas tecnológicas han surgido con el fin de mitigar la aparente contradicción entre inmutabilidad y derecho de supresión. Por ejemplo, se han propuesto mecanismos de pseudonimización, el uso de blockchains híbridas o privadas, y la implementación de contratos inteligentes modificables que permitan ejercer cierto control sobre los datos almacenados (Zyskind, Nathan & Pentland, 2015, p. 38).

Desde el ámbito doctrinal, también se han esbozado soluciones basadas en la descentralización del consentimiento, la codificación de derechos en los protocolos de blockchain y el diseño de arquitecturas que separen los datos personales del registro inmutable, almacenándolos fuera de la cadena (Off-chain), pero vinculados mediante hash (Kosseff, 2018, p. 203).

La presente investigación se propone analizar a fondo esta tensión desde una perspectiva jurídica y tecnológica, estudiando cómo los principios de protección de datos pueden coexistir con los fundamentos técnicos de blockchain. Se considera imprescindible una revisión tanto de la normativa vigente como de las experiencias internacionales, con especial atención a los avances en Europa, América Latina y Estados Unidos.

Además, se adopta una metodología mixta, que integra el análisis descriptivo, bibliográfico y fenomenológico jurídico, a fin de ofrecer una visión integral que permita identificar los desafíos y oportunidades que plantea esta convergencia. Se pretende, en última instancia, ofrecer aportes teóricos y prácticos para el desarrollo de un marco regulatorio coherente con la innovación tecnológica y respetuoso de los derechos fundamentales.

A lo largo del artículo se explorarán estudios de caso relevantes, como los de Estonia y Francia, así como propuestas concretas para el contexto ecuatoriano, que permitan orientar tanto a legisladores como a desarrolladores en la creación de soluciones compatibles con el principio de legalidad y la efectividad de los derechos.

En suma, el artículo parte de la premisa de que no existe una contradicción insalvable entre blockchain y el derecho de supresión, sino que la clave está en el diseño jurídico-tecnológico de sistemas más flexibles, que reconozcan los límites de la tecnología y promuevan un enfoque centrado en la dignidad humana y la autodeterminación informativa (Pérez Luño, 2007, p. 119).

ISSN: 2966-0599
contato@ouniversoobservavel.com.br
www.ouniversoobservavel.com.br
Periódico Científico Indexado

PLANTEAMIENTO DEL PROBLEMA

El crecimiento acelerado de las tecnologías emergentes ha puesto a prueba los marcos jurídicos tradicionales. En particular, la irrupción de la tecnología blockchain ha planteado desafíos significativos en materia de protección de datos personales. Mientras que esta tecnología garantiza una estructura segura e inmutable para almacenar información, el derecho de supresión exige la posibilidad de suprimir datos personales cuando así lo requiera el titular. Esta aparente contradicción genera interrogantes sobre la compatibilidad entre un derecho fundamental consagrado en legislaciones modernas como el RGPD y la naturaleza técnica de la cadena de bloques, que impide por diseño la eliminación de registros ya asentados (Finck, 2018, p. 83).

En el contexto ecuatoriano, esta tensión cobra especial relevancia tras la promulgación de la Ley Orgánica de Protección de Datos Personales (2021), la cual establece expresamente el derecho de supresión como garantía legal. Sin embargo, la falta de directrices técnicas claras para su implementación en tecnologías descentralizadas abre un vacío normativo y práctico que puede derivar en la vulneración de derechos fundamentales. Además, existen riesgos de responsabilidad civil y administrativa por el tratamiento indebido de datos, en especial si se utilizan plataformas basadas en blockchain sin prever mecanismos de corrección o eliminación de la información (Registro Oficial, 2021, art. 16).

Así, el problema central radica en determinar cómo armonizar el principio de inmutabilidad de blockchain con el ejercicio efectivo del derecho de supresión, especialmente en el marco jurídico ecuatoriano, donde aún se carece de jurisprudencia y lineamientos técnicos que orienten a los operadores jurídicos, desarrolladores y empresas tecnológicas.

OBJETIVO GENERAL

Analizar las tensiones jurídicas y tecnológicas entre la inmutabilidad de blockchain y el derecho de supresión, proponiendo mecanismos normativos y técnicos que permitan su compatibilidad en el contexto ecuatoriano.

OBJETIVOS ESPECÍFICOS

1. Examinar el marco normativo ecuatoriano y comparado en materia de protección de datos personales y derecho de supresión.
2. Identificar los principales desafíos técnicos que impiden la aplicación del derecho de supresión en entornos blockchain.
3. Proponer soluciones jurídicas y tecnológicas viables que garanticen la efectividad del derecho de supresión sin comprometer los principios fundamentales de blockchain.

POSIBLE SOLUCIÓN

La solución no radica en sacrificar la esencia de la tecnología blockchain, sino en diseñar mecanismos híbridos que permitan satisfacer las exigencias del derecho de supresión. Entre las alternativas viables destacan el uso de almacenamiento off-chain para los datos sensibles, la implementación de sistemas de pseudonimización y anonimización, el desarrollo de blockchains privadas con cláusulas de gobernanza específicas, y el empleo de contratos inteligentes reversibles o editables bajo condiciones jurídicas bien definidas. Además, se propone la incorporación de principios jurídicos en los estándares técnicos de desarrollo para que la privacidad y la protección de datos sean elementos estructurales y no añadidos ex post (Zyskind et al., 2015, p. 40; Kosseff, 2018, p. 206).

JUSTIFICACIÓN

Este estudio se justifica tanto por la novedad del problema como por su relevancia práctica y jurídica. En Ecuador, la entrada en vigor de la Ley Orgánica de Protección de Datos Personales ha generado una nueva responsabilidad para los sujetos obligados, incluyendo desarrolladores de tecnologías y entidades públicas que utilicen blockchain. No obstante, la ausencia de criterios doctrinales y técnicos sobre la compatibilidad entre blockchain y el derecho de supresión impide una aplicación efectiva de dicha ley.

Desde el punto de vista académico, existe un vacío teórico en la literatura jurídica ecuatoriana sobre esta materia, por lo que este trabajo pretende contribuir al debate nacional e internacional desde una perspectiva comparada y multidisciplinaria. En el ámbito internacional, estudios como los de Finck (2018) y De Filippi & Wright (2018) han señalado que la solución debe provenir de un diálogo entre el Derecho y la ingeniería informática, en lugar de tratar de imponer uno sobre el otro.

Adicionalmente, el desarrollo de esta investigación permite generar propuestas normativas concretas que pueden ser consideradas por legisladores, jueces y

ISSN: 2966-0599
contato@ouniversoobservavel.com.br
www.ouniversoobservavel.com.br
Periódico Científico Indexado

diseñadores de políticas públicas, fomentando una gobernanza tecnológica basada en los derechos humanos. El equilibrio entre innovación y protección de datos no solo es deseable, sino necesario para garantizar la seguridad jurídica, la confianza ciudadana y el respeto a la autodeterminación informativa en la era digital (Pérez Luño, 2007, p. 122).

ESTADO DEL ARTE

La creciente interacción entre tecnologías disruptivas y derechos fundamentales ha generado intensos debates académicos. Uno de los más relevantes y contemporáneos es el conflicto entre la inmutabilidad de la tecnología blockchain y el derecho de supresión, consagrado en instrumentos legales como el Reglamento General de Protección de Datos (RGPD) de la Unión Europea y otras normativas similares en América Latina. La tensión radica en que, mientras la blockchain se caracteriza por su registro inmutable, descentralizado y permanente, el derecho de supresión exige la eliminación de datos personales a solicitud del titular, en aras de preservar su autonomía, intimidad y reputación.

Blockchain e inmutabilidad: ¿un obstáculo al derecho a la supresión?

Primavera De Filippi y Aaron Wright (2018), en uno de los estudios pioneros sobre esta temática, advierten que la lógica descentralizada de blockchain representa un "choque frontal" con los principios del derecho a la protección de datos. La inmutabilidad del registro significa que, una vez que un dato ha sido validado y agregado a la cadena, no puede ser modificado ni eliminado sin comprometer la integridad de toda la red. Según los autores, esto plantea un dilema jurídico fundamental: o se redefine el diseño técnico de la blockchain para contemplar excepciones legales, o se reinterpretan los derechos fundamentales a la luz de las nuevas arquitecturas digitales (p. 97).

Desde una perspectiva normativa, Kuner, Cate, Millard y Svantesson (2017) examinan el artículo 17 del RGPD, que establece el derecho de supresión como una obligación activa del responsable del tratamiento de eliminar los datos personales del titular en determinados supuestos: cuando ya no son necesarios, cuando el consentimiento ha sido retirado, o cuando el tratamiento es ilícito. Sin embargo, la rigidez estructural de blockchain entra en contradicción con esta obligación, dificultando la eliminación efectiva de datos personales (p. 142). Este problema ha sido abordado por las autoridades europeas de protección de datos, quienes han advertido que la aplicación del RGPD a tecnologías blockchain debe realizarse con cautela y caso por caso.

América Latina: desafíos de implementación y regulación incipiente

En el contexto latinoamericano, Doneda y Monteiro (2020) analizan la situación de Brasil a partir de la Lei Geral de Proteção de Dados (LGPD), que incorpora el derecho a la supresión en términos similares al RGPD europeo. Aunque la ley brasileña constituye un avance normativo significativo, los autores subrayan que su aplicación en entornos basados en blockchain sigue siendo difusa, debido a la ausencia de lineamientos técnicos claros, la falta de criterios jurisprudenciales uniformes y el escaso desarrollo doctrinal sobre el tema (p. 158). Esta situación se repite en otras jurisdicciones de la región, como Argentina, Chile y México, donde el desarrollo normativo en materia de tecnologías emergentes es incipiente o fragmentario.

Los autores plantean que los legisladores latinoamericanos enfrentan el desafío de diseñar leyes que promuevan la innovación tecnológica sin poner en riesgo los derechos fundamentales. La falta de interoperabilidad entre sistemas jurídicos y plataformas tecnológicas globales agrava el problema, generando una "zona gris" en la que la protección efectiva de los derechos digitales es aún limitada.

Propuestas doctrinales y técnicas: reinterpretación y rediseño

Una de las propuestas más influyentes es la de Finck (2018), quien sostiene que los principios del RGPD no deben ser abandonados ante los desafíos técnicos de blockchain, sino reinterpretados creativamente. Para ello, sugiere aplicar mecanismos como la anonimización y la pseudonimización, que permiten ocultar o desasociar la identidad de los titulares de los datos, preservando así el espíritu del derecho de supresión sin requerir la eliminación material del bloque (p. 81). Esta reinterpretación permitiría mantener la integridad de la cadena mientras se cumple el principio de minimización de datos exigido por el RGPD.

En el ámbito técnico, Zyskind, Nathan y Pentland (2015) han desarrollado arquitecturas que separan los datos personales del libro mayor público (modelo *off-chain*). De este modo, la información sensible se almacena en servidores externos controlados por los usuarios o por terceros confiables, mientras que en la blockchain se registra únicamente un *hash* o

ISSN: 2966-0599
contato@ouniversoobservavel.com.br
www.ouniversoobservavel.com.br
Periódico Científico Indexado

firma criptográfica que verifica la integridad del dato. Si el usuario desea ejercer su derecho de supresión, puede eliminar los datos de la base externa sin alterar la blockchain, logrando una solución intermedia entre inmutabilidad y reversibilidad (Zyskind, Nathan y Pentland, 2015, p. 41). Dicho esto, el Comité Europeo de Protección de Datos (EDPB) ha establecido que el *hash* de datos personales puede ser considerado también un dato personal, en el caso de que este puede vincularse razonablemente a una persona física, por lo que los procesos de anonimización de datos se vuelve aún más relevante (EDPB, 2019, pp. 45–50).

Estas propuestas reflejan una tendencia hacia soluciones híbridas que buscan compatibilizar principios jurídicos y estructuras tecnológicas, a través de modelos de gobernanza cooperativa entre diseñadores de sistemas, legisladores, operadores de datos y ciudadanos digitales.

El caso ecuatoriano: avances normativos y vacío técnico

En Ecuador, la discusión sobre blockchain y el derecho de supresión aún se encuentra en una etapa inicial. No obstante, la Ley Orgánica de Protección de Datos Personales, vigente desde mayo de 2021, representa un avance significativo. El artículo 16 de dicha ley reconoce el derecho del titular a solicitar la supresión de sus datos personales, cuando hayan dejado de ser necesarios para los fines del tratamiento, o cuando se haya revocado el consentimiento (Registro Oficial, 2021, art. 16).

Sin embargo, la normativa no ofrece lineamientos técnicos ni doctrinales sobre cómo aplicar este derecho en arquitecturas descentralizadas e inmutables como blockchain. Tampoco se establece un régimen especial para tecnologías emergentes ni se contemplan mecanismos de disociación o almacenamiento descentralizado que permitan cumplir con las exigencias del derecho de supresión sin comprometer la lógica técnica de la cadena de bloques.

Esta falta de desarrollo puede generar inseguridad jurídica tanto para los desarrolladores como para los titulares de datos, que no encuentran aún canales claros para ejercer sus derechos digitales en entornos tecnológicos innovadores. Por tanto, es urgente desarrollar tanto doctrina como regulación secundaria que aborde esta problemática desde un enfoque interdisciplinario, que articule conocimientos de Derecho, informática, ética digital y diseño institucional.

El análisis doctrinal y técnico evidencia una tensión estructural entre el diseño inmutable de la tecnología blockchain y la naturaleza revocable y garantista del derecho de supresión. Mientras algunos autores proponen rediseñar la arquitectura tecnológica para adaptarla al marco normativo vigente, otros sugieren reinterpretar los derechos digitales desde una perspectiva funcional, que priorice la efectividad sobre la forma.

La experiencia comparada muestra que ni el Derecho ni la tecnología pueden ofrecer una solución única y definitiva. En cambio, se requiere una cooperación regulatoria global, el desarrollo de mecanismos técnicos adaptativos y una reflexión jurídica profunda sobre los límites de la protección de datos en la era digital. En el caso ecuatoriano, la entrada en vigor de la Ley de Protección de Datos marca el inicio de este camino, pero es necesario avanzar hacia una legislación específica sobre tecnologías disruptivas que permita armonizar innovación y derechos fundamentales.

MARCO TEÓRICO

El presente trabajo se apoya en un marco conceptual interdisciplinario que permite abordar el conflicto entre la inmutabilidad de la tecnología blockchain y el derecho de supresión desde una perspectiva integral. Este marco se estructura en cuatro pilares teóricos fundamentales: la teoría del derecho a la protección de datos personales, los principios tecnológicos de inmutabilidad y descentralización de la blockchain, el enfoque de derechos humanos frente a las tecnologías emergentes y la teoría de la gobernanza algorítmica. La articulación de estas corrientes permite identificar no solo las tensiones estructurales entre derecho y tecnología, sino también posibles vías de compatibilización regulatoria.

1. Teoría del Derecho a la Protección de Datos Personales

El derecho a la protección de datos personales se ha consolidado como un derecho autónomo e independiente dentro del catálogo de derechos fundamentales, especialmente a partir del desarrollo legislativo y jurisprudencial en Europa y América Latina. Su base filosófica se encuentra en la doctrina de la autodeterminación informativa, que concibe al individuo como titular del control sobre el uso y tratamiento de su información personal. Este enfoque supera la visión clásica de la privacidad como mero derecho a la intimidad, otorgando protagonismo

ISSN: 2966-0599
contato@ouniversoobservavel.com.br
www.ouniversoobservavel.com.br
Periódico Científico Indexado

al sujeto como gestor activo de su identidad digital.

El Reglamento General de Protección de Datos (RGPD) de la Unión Europea constituye el instrumento normativo más avanzado en esta materia. En su artículo 17 se establece expresamente el derecho de supresión, entendiendo como tal la facultad del titular de datos de solicitar la supresión de su información personal cuando esta ya no sea necesaria, se haya tratado ilícitamente o se haya retirado el consentimiento. Según Kuner et al. (2017), este derecho refleja una evolución normativa hacia una protección proactiva, donde el consentimiento no solo legitima el tratamiento inicial de los datos, sino que también otorga al titular el poder de limitarlo o revocarlo en cualquier momento (p. 140).

Esta dimensión del consentimiento refuerza la noción de que los datos personales no pueden ser tratados como meros objetos transferibles, sino como extensiones de la personalidad jurídica del individuo, cuya protección se vincula directamente con los principios de dignidad humana, libertad e igualdad.

2. Inmutabilidad y Descentralización en Blockchain

La blockchain o cadena de bloques es una tecnología que permite registrar transacciones de forma descentralizada, criptográficamente segura y prácticamente inalterable. En este sistema, los datos son agrupados en bloques enlazados entre sí mediante funciones hash, lo que asegura su integridad y resistencia a la manipulación. Como explican Tapscott y Tapscott (2016), "cada bloque está conectado al anterior, de modo que una alteración en un punto compromete toda la cadena", generando una estructura que garantiza transparencia, verificabilidad y confianza sin necesidad de intermediarios (p. 45).

La inmutabilidad es una de sus características más celebradas desde el ámbito técnico, ya que evita el fraude, garantiza la trazabilidad y refuerza la confianza en sistemas descentralizados. Sin embargo, desde una perspectiva jurídica, esta cualidad plantea serias dificultades, especialmente cuando entra en conflicto con derechos que exigen reversibilidad, como el derecho de supresión. Una vez que un dato personal ha sido almacenado en una blockchain pública, su eliminación se vuelve prácticamente inviable, a menos que el sistema haya sido diseñado desde el inicio para permitir algún tipo de modificación parcial, disociación o supresión fuera de la cadena (*off-chain*).

La descentralización implica la ausencia de una autoridad central que pueda intervenir o ejecutar una orden de supresión, lo que complica aún más la exigibilidad efectiva de los derechos. Este modelo técnico exige, por tanto, un replanteamiento de las categorías jurídicas tradicionales que daban por sentada la existencia de un "responsable del tratamiento".

3. Derechos Humanos y Tecnología

El enfoque de derechos humanos aplicados a la tecnología proporciona un marco normativo y ético esencial para analizar las consecuencias sociales de la innovación tecnológica. Según Antonio Enrique Pérez Luño (2007), todo avance técnico debe someterse a una evaluación desde los principios rectores del constitucionalismo moderno: la dignidad humana, la libertad individual, la igualdad sustantiva y la justicia (p. 119). Desde esta óptica, no es aceptable que el diseño tecnológico imponga limitaciones estructurales al ejercicio de derechos fundamentales, como ocurre en ciertos usos de blockchain que impiden ejercer el derecho de supresión.

La tecnología no es neutra, y su arquitectura refleja decisiones de diseño que pueden favorecer o restringir el ejercicio de derechos. Por ello, el enfoque de derechos humanos plantea que los sistemas tecnológicos deben incorporar valores jurídicos desde su concepción (*privacy by design*), asegurando que principios como la proporcionalidad, la necesidad y la responsabilidad estén presentes en cada etapa del ciclo de vida del dato. La protección de los datos personales, en consecuencia, debe entenderse no solo como un objetivo posterior a la innovación, sino como una exigencia previa al desarrollo e implementación de tecnologías.

4. Teoría de la Gobernanza Algorítmica

La cuarta dimensión teórica que sustenta este trabajo es la gobernanza algorítmica, entendida como un nuevo paradigma normativo que responde al desafío de regular tecnologías disruptivas como la inteligencia artificial, el big data y la blockchain. Según Yeung (2018), la gobernanza algorítmica exige el diseño de marcos normativos dinámicos, adaptativos y evolutivos, que combinen principios legales clásicos con mecanismos técnicos de autocontrol y vigilancia inteligente (p. 507).

En este sentido, se plantea la necesidad de que los derechos fundamentales sean codificados dentro del diseño del sistema

ISSN: 2966-0599
contato@ouniversoobservavel.com.br
www.ouniversoobservavel.com.br
Periódico Científico Indexado

tecnológico, de modo que el cumplimiento normativo no dependa exclusivamente de regulaciones externas (*ex post*), sino que esté integrado en el código fuente (*ex ante*). Esta propuesta implica un cambio de paradigma: el Derecho no solo debe interpretar la tecnología, sino también influir en su diseño estructural.

En el caso específico de blockchain, esta teoría sugiere implementar mecanismos de disociación criptográfica, almacenamiento selectivo off-chain y control granular del acceso a los datos, como estrategias para compatibilizar la arquitectura técnica con los derechos del usuario. Así, el Derecho no impone límites al desarrollo tecnológico, sino que guía su evolución hacia modelos compatibles con el estado de derecho y la protección de la persona.

ESTUDIOS DE CASO Y EXPERIENCIAS INTERNACIONALES

Las experiencias internacionales en torno al conflicto entre la inmutabilidad de blockchain y el ejercicio del derecho de supresión evidencian una pluralidad de respuestas normativas, institucionales y tecnológicas. Lejos de ser homogéneas, estas soluciones reflejan las tensiones existentes entre los valores de seguridad, transparencia y descentralización, propios del entorno blockchain, y los principios jurídicos fundamentales vinculados a la protección de datos personales. Se examinan casos representativos que ilustran las distintas aproximaciones adoptadas por países y organismos a nivel comparado.

1. Unión Europea: Caso Google Spain y el precedente del derecho de supresión

Uno de los antecedentes más influyentes en la consolidación del derecho de supresión es el caso Google Spain SL v. Agencia Española de Protección de Datos (C-131/12), resuelto por el Tribunal de Justicia de la Unión Europea (TJUE) en 2014. En esta sentencia, el TJUE reconoció por primera vez el derecho de los ciudadanos a solicitar que sus datos personales no sean indexados por motores de búsqueda, cuando dicha información ya no sea pertinente o resulte perjudicial. Si bien este caso no involucra tecnologías blockchain, sentó un precedente clave al definir el derecho a la supresión como un derecho fundamental dentro del marco del tratamiento digital de datos.

Este fallo introdujo la idea de que la tecnología debe adaptarse a los derechos, y no a la inversa. Se reafirmó la responsabilidad de los intermediarios tecnológicos (como Google) en la gestión de datos personales, incluso si estos no han sido los originarios del contenido. Este enfoque ha servido de base para el desarrollo de principios aplicables también al ecosistema blockchain, como la **intervención humana significativa** y la necesidad de mantener vías efectivas para ejercer derechos digitales.

2. Estonia: innovación institucional con respeto a los derechos

Estonia es frecuentemente citada como uno de los países más avanzados en gobernanza digital. Desde 2012, ha implementado un sistema basado en KSI Blockchain, utilizado para proteger la integridad de registros públicos como historiales médicos, judiciales y fiscales. A diferencia de las blockchains públicas tradicionales, este modelo se basa en la verificación de integridad mediante hash y el almacenamiento externo (off-chain), lo que permite eliminar o modificar los datos personales sin alterar la cadena de bloques (E-Estonia Briefing Centre, 2020, p. 12). Recordando que el hash de datos personales no debe poder vincularse razonablemente a una persona física para mantener una adecuada protección de datos bajo el criterio de la EDPB.

Este diseño demuestra que es posible mantener los beneficios de inmutabilidad y trazabilidad de blockchain sin sacrificar los derechos de supresión. El enfoque estonio respeta el principio de proporcionalidad tecnológica al segmentar la información y evitar que datos personales sean almacenados directamente en la cadena. Esta práctica ha sido aplaudida por diversos organismos internacionales y constituye un modelo replicable en otros contextos.

3. Francia: propuestas de blockchain reversible y gobernanza del consentimiento

En 2018, la Comisión Nacional de Informática y Libertades (CNIL) de Francia publicó el informe *Blockchain et protection des données personnelles*, donde propone un enfoque técnico-jurídico para compatibilizar blockchain con el RGPD. Entre las principales recomendaciones se destaca el uso de identificadores indirectos, como los hash de datos personales, y la aplicación de técnicas de disociación o cifrado asimétrico que permitan eliminar la relación entre el dato y su titular (CNIL, 2018, p. 6).

Además, la CNIL plantea el desarrollo de "blockchains reversibles" en sectores sensibles como la salud, donde el consentimiento del usuario es programado como una variable contractual dentro de contratos inteligentes,

ISSN: 2966-0599
contato@ouniversoobservavel.com.br
www.ouniversoobservavel.com.br
Periódico Científico Indexado

permitiendo la revocación o modificación de accesos en tiempo real. Esta propuesta fortalece el principio de consentimiento informado y refuerza la idea de que los sistemas tecnológicos deben incorporar mecanismos de gobernanza algorítmica desde su diseño.

4. Brasil: gobernanza flexible y blockchain privada

En América Latina, Brasil ha sido uno de los países más activos en la incorporación del derecho de supresión dentro de su ordenamiento jurídico a través de la Lei Geral de Proteção de Dados (LGPD). Esta normativa recoge explícitamente el derecho de supresión y permite su ejercicio incluso frente a tecnologías emergentes. Según Doneda y Monteiro (2020), Brasil ha impulsado el uso de blockchains privadas o con permisos (*permissioned blockchains*) como medio para implementar mecanismos de gobernanza interna, capaces de atender solicitudes de supresión sin afectar la integridad técnica del sistema (p. 160).

En estos entornos controlados, es posible diseñar protocolos de acceso y modificación que cumplan con las obligaciones legales en materia de protección de datos, siempre que exista una entidad responsable que centralice las decisiones sobre la eliminación o disociación de los datos. Este modelo plantea una interesante combinación entre descentralización tecnológica y centralización regulatoria, que puede ser útil para sectores como el financiero, el médico o el educativo.

5. Estados Unidos: aproximación sectorial desde la CCPA

En el sistema jurídico estadounidense, no existe un derecho de supresión reconocido a nivel federal. Sin embargo, leyes estatales como la California Consumer Privacy Act (CCPA) han introducido mecanismos similares, otorgando a los consumidores el derecho a solicitar la eliminación de su información personal recolectada por las empresas. Según Kosseff (2018), la implementación de la CCPA ha impulsado el desarrollo de infraestructuras híbridas donde los datos personales se almacenan de forma externa a la blockchain (off-chain), permitiendo su eliminación sin comprometer la cadena (p. 205).

Empresas tecnológicas en California han comenzado a aplicar interfaces regulatorias, es decir, capas intermedias de software que conectan blockchain con bases de datos convencionales, permitiendo cumplir con solicitudes de supresión. Aunque estas soluciones no resuelven todos los problemas, demuestran que es posible adaptar modelos técnicos a los requisitos legales existentes sin sacrificar la operatividad de los sistemas descentralizados.

Las experiencias internacionales analizadas permiten identificar una tendencia convergente: los sistemas blockchain no deben ni pueden estar por encima del orden jurídico. En lugar de ello, deben adaptarse estructuralmente a los principios de derechos humanos y a las garantías propias del Estado de derecho. Esta compatibilización depende en gran medida del diseño técnico del sistema, así como de la capacidad normativa para establecer marcos jurídicos flexibles, técnicamente informados y orientados a la protección del usuario.

Los casos revisados muestran que el conflicto entre la inmutabilidad de blockchain y el derecho de supresión no es insoluble, sino que exige un diálogo interdisciplinario constante entre programadores, juristas, reguladores y usuarios. Solo a través de esta interacción será posible desarrollar infraestructuras tecnológicas que no solo sean eficientes y seguras, sino también legítimas desde el punto de vista jurídico y ético. Es relevante sobre el tema mencionar que, según lo establece el *California Consumer Privacy Act* (Cal. Civ. Code § 1798.105, 2018), se permiten excepciones al derecho de supresión en aquellos casos en los que la eliminación no sea posible por motivos técnicos razonables.

NORMATIVA ECUATORIANA SOBRE PROTECCIÓN DE DATOS Y BLOCKCHAIN

El marco jurídico ecuatoriano ha mostrado avances significativos en materia de derechos digitales, especialmente a través de la incorporación del derecho a la protección de datos personales dentro del bloque constitucional y del desarrollo de normativa ordinaria como la Ley Orgánica de Protección de Datos Personales (LOPDP). No obstante, el país aún enfrenta desafíos estructurales para garantizar el cumplimiento efectivo de estos derechos frente al uso de tecnologías emergentes como blockchain, cuya naturaleza inmutable y descentralizada pone a prueba las categorías jurídicas tradicionales.

1. Constitución de la República del Ecuador y derechos digitales

El punto de partida del análisis normativo debe situarse en el artículo 66, numeral 19 de la Constitución de 2008, que reconoce expresamente el derecho a la protección de datos personales, incluyendo las facultades de acceso, rectificación, cancelación y

ISSN: 2966-0599
contato@ouniversoobservavel.com.br
www.ouniversoobservavel.com.br
Periódico Científico Indexado

oposición (ARCO). Este derecho se configura como una garantía autónoma, de igual jerarquía que otros derechos fundamentales, y protege la autodeterminación informativa del individuo en el entorno digital.

La Carta Magna también incorpora principios como la seguridad jurídica (art. 82), la prevalencia del interés superior de la persona (art. 11.8), y la progresividad de los derechos (art. 11.8), todos los cuales deben servir como parámetros interpretativos para resolver conflictos entre innovaciones tecnológicas y derechos fundamentales.

Aunque la Constitución no menciona expresamente la tecnología blockchain, su apertura axiológica y normativa permite que derechos como el olvido digital se apliquen incluso frente a infraestructuras tecnológicas descentralizadas, siempre que exista una amenaza o afectación a la dignidad, privacidad o integridad de la persona.

2. Ley Orgánica de Protección de Datos Personales (LOPDP)

La LOPDP, publicada en el Registro Oficial Suplemento N.º 459 del 26 de mayo de 2021, representa el principal cuerpo normativo ordinario en la materia. Esta ley se alinea con los estándares internacionales establecidos por el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, y reconoce expresamente el derecho de supresión en su artículo 16. En dicho artículo, se establece que el titular podrá solicitar la supresión de sus datos personales cuando:

- Se haya cumplido la finalidad del tratamiento.
- El consentimiento haya sido revocado.
- Los datos hayan sido tratados de manera ilícita.
- Exista una obligación legal de supresión.

La ley incorpora principios rectores como la licitud, finalidad, minimización, exactitud, confidencialidad, responsabilidad proactiva y portabilidad (LOPDP, art. 7), los cuales deben aplicarse en cualquier actividad de tratamiento de datos, sin importar el soporte técnico utilizado.

No obstante, uno de los principales vacíos de la LOPDP es la ausencia de disposiciones específicas que regulen el tratamiento de datos personales en el contexto de tecnologías disruptivas, como la blockchain. No se mencionan conceptos como almacenamiento descentralizado, hash criptográfico, contratos inteligentes, ni técnicas de anonimización o pseudonimización adaptadas al entorno blockchain. Esto genera incertidumbre jurídica respecto a la posibilidad de exigir, por ejemplo, la supresión de datos almacenados en redes inmutables.

3. Blockchain en el contexto ecuatoriano: falta de normativa específica

En lo que respecta a la regulación de blockchain como tecnología, Ecuador carece de una legislación específica que defina sus usos, límites, o implicaciones jurídicas. Las referencias más cercanas provienen de documentos técnicos emitidos por entidades como el Banco Central del Ecuador y la Superintendencia de Compañías, Valores y Seguros, que han manifestado preocupaciones sobre el uso de activos digitales y criptomonedas, pero no han desarrollado criterios jurídicos aplicables al tratamiento de datos personales en redes blockchain.

Por otro lado, la Propuesta de Ley de Economía Digital, actualmente en debate en la Asamblea Nacional, incluye disposiciones sobre infraestructura tecnológica y gobernanza digital, pero no aborda el conflicto entre inmutabilidad tecnológica y los derechos digitales, lo que perpetúa el vacío normativo existente.

Esta omisión es especialmente grave si se considera que blockchain ya está siendo utilizada por startups, proyectos académicos e incluso instituciones públicas para gestionar datos contractuales, financieros y administrativos. La falta de normas específicas deja sin protección efectiva a los titulares de datos en estos entornos.

4. Jurisprudencia constitucional: apertura a los derechos digitales

Aunque la Corte Constitucional del Ecuador aún no ha emitido un pronunciamiento específico sobre la relación entre blockchain y derechos digitales, sí ha avanzado en reconocer la exigibilidad directa de los derechos fundamentales en entornos tecnológicos. En la Sentencia No. 1149-19-JP/21, el tribunal enfatizó la necesidad de interpretar los derechos constitucionales de forma evolutiva y adaptativa, de modo que se garantice su aplicabilidad frente a los desafíos del entorno digital.

Este tipo de jurisprudencia abre la posibilidad de un futuro control de constitucionalidad sobre sistemas tecnológicos que, por su diseño, impidan o dificulten el ejercicio de derechos como la supresión, la rectificación o el consentimiento informado. El principio de eficacia directa de los derechos constitucionales permite exigir su cumplimiento

ISSN: 2966-0599
contato@ouniversoobservavel.com.br
www.ouniversoobservavel.com.br
Periódico Científico Indexado

sin necesidad de normas intermedias, lo que podría servir como base para demandas judiciales contra implementaciones inadecuadas de tecnologías blockchain.

5. Necesidades regulatorias y recomendaciones

Ante este panorama, resulta urgente que el legislador ecuatoriano adopte una ley especializada en tecnologías disruptivas, o en su defecto, reforme la LOPDP para incorporar disposiciones específicas sobre el tratamiento de datos en entornos blockchain. Entre las medidas recomendadas se encuentran:

- Exigir que los sistemas blockchain implementados en el país adopten un diseño compatible con la protección de datos, incluyendo mecanismos como almacenamiento off-chain, hash no reversibles, y anonimización criptográfica.
- Establecer una figura legal de responsable técnico de la red, incluso en sistemas descentralizados, para garantizar la rendición de cuentas, que no puede ser la misma que el responsable de tratamiento o el oficial de cumplimiento contemplado en la legislación, puesto que la figura no tiene un rol definido con claridad en entornos descentralizados como blockchain.
- Promover el uso de blockchains privadas o con permisos, donde existan mecanismos institucionales de gobernanza que permitan atender solicitudes de rectificación o eliminación.
- Incentivar el desarrollo de guías técnicas y criterios de interpretación, en coordinación con la Agencia de Protección de Datos Personales y organismos técnicos.

Ecuador ha dado un paso fundamental al consagrar el derecho de supresión en su legislación y en su Constitución. Sin embargo, el desarrollo tecnológico, especialmente en lo relativo a blockchain, ha superado el ritmo de la legislación, generando un vacío regulatorio que pone en riesgo la eficacia de estos derechos. La armonización entre innovación tecnológica y protección de derechos fundamentales exige una acción legislativa decidida, así como el desarrollo de criterios jurisprudenciales claros que permitan resolver conflictos entre inmutabilidad y supresión de datos. Solo así se podrá garantizar que la transformación digital en el país no ocurra a costa de los principios del Estado constitucional de derechos y justicia.

METODOLOGÍA

El presente estudio aplica un enfoque metodológico cualitativo y multidisciplinario, que integra elementos del análisis jurídico, técnico y ético, con el fin de comprender y proponer soluciones a la tensión entre blockchain y el derecho de supresión en el contexto ecuatoriano e internacional. Es así como se detallan los métodos utilizados:

Método Descriptivo

El método descriptivo ha sido empleado para explicar las características esenciales de la tecnología blockchain, el funcionamiento del derecho de supresión y su tratamiento en diversas jurisdicciones. Este enfoque permite caracterizar los elementos técnicos que dificultan la eliminación de datos personales en cadenas de bloques y describir cómo el derecho responde actualmente a estos desafíos (Hernández, Fernández & Baptista, 2014, p. 92).

Método Bibliográfico

Se ha recurrido al método bibliográfico mediante una revisión documental sistemática de textos normativos, sentencias constitucionales, informes de autoridades de protección de datos (como la CNIL), y artículos científicos publicados en bases como Scopus, Google Scholar y RedALyC. Este análisis proporciona el sustento teórico y normativo para interpretar el conflicto entre los principios tecnológicos y los derechos fundamentales (Arias Galicia, 2012, p. 81).

Método Fenomenológico Jurídico

Este método se ha aplicado para comprender el fenómeno jurídico en su contexto, considerando cómo el derecho de supresión adquiere una dimensión distinta cuando interactúa con tecnologías emergentes. A través del análisis fenomenológico se exploran las implicaciones éticas y jurídicas del tratamiento inmutable de datos personales, desde la perspectiva de la dignidad humana, la autodeterminación informativa y el principio de legalidad (Vigo, 2001, p. 67).

El uso combinado de estos métodos permite articular una propuesta integral que no solo describa el problema, sino que también oriente a los operadores jurídicos y legisladores sobre posibles reformas normativas y buenas prácticas tecnológicas.

DISCUSIÓN Y RESULTADOS

Definición del Conflicto

El conflicto central abordado en esta investigación radica en la incompatibilidad técnica entre la inmutabilidad propia de la

ISSN: 2966-0599
contato@ouniversoobservavel.com.br
www.ouniversoobservavel.com.br
Periódico Científico Indexado

tecnología blockchain y el derecho de supresión, que exige la supresión o modificación de datos personales bajo ciertas condiciones legales. A pesar de los esfuerzos normativos, como el RGPD o la LOPDP ecuatoriana, la mayoría de sistemas blockchain no han sido diseñados para contemplar la eliminación de registros, lo que genera una brecha entre la legalidad y la arquitectura tecnológica.

Tabla de Implementación y Resultados

País	Estrategia Adoptada	Tecnología	Nivel de Éxito
Estonia	Hash + Off-chain	KSI Blockchain	Alto
Francia	Identificadores indirectos + pseudonimización	Blockchain privada	Moderado
Brasil	Smart contracts reversibles	Blockchain híbrida	En desarrollo
EE. UU. (California)	Interfaz regulatoria entre CCPA y DLTs	Ethereum + APIs	Bajo
Alemania	Segmentación de nodos	Permissioned DLTs	Moderado

Nota: Se analizaron cinco iniciativas internacionales que han propuesto soluciones al problema:
Fuente: Elaboración propia con base en CNIL (2018), E-Estonia (2020), Doneda y Monteiro (2020).

Estos resultados sugieren que **los sistemas que permiten una separación lógica entre los datos personales y la cadena inmutable son los más viables** para garantizar el derecho de supresión sin socavar la funcionalidad de blockchain.

CUESTIONES ÉTICAS

El uso de tecnologías como blockchain plantea importantes dilemas éticos en relación con la autonomía, la privacidad y la dignidad de las personas. Si bien la descentralización y la inmutabilidad se valoran por su potencial para prevenir la manipulación y el fraude, estas características también pueden convertirse en fuentes de vulnerabilidad para los titulares de datos cuando no se consideran sus derechos fundamentales desde el diseño de la arquitectura tecnológica.

Desde la perspectiva de la ética jurídica, uno de los principios esenciales es el respeto a la autonomía individual, entendida como la capacidad del sujeto para tomar decisiones informadas sobre el tratamiento de sus datos personales. En este sentido, Pérez Luño (2007) sostiene que la tecnología debe estar al servicio de la persona humana, y no al revés. Cuando los sistemas informáticos se estructuran de manera opaca o inmodificable, se corre el riesgo de convertir a la persona en un objeto de control tecnológico, en lugar de sujeto de derechos (p. 121).

La ausencia de mecanismos efectivos para la rectificación, actualización o supresión de información puede derivar en formas de "exposición perpetua" que contradicen los principios de proporcionalidad, temporalidad del castigo y derecho a la rehabilitación social, especialmente en el tratamiento de datos sensibles como los antecedentes penales, diagnósticos médicos o registros crediticios. Esta situación entra en conflicto no solo con normas jurídicas, sino también con principios éticos como la justicia restaurativa y el respeto a la evolución de la personalidad.

En este contexto, el diseño tecnológico debe incorporar desde el inicio valores como la reversibilidad, la transparencia algorítmica y el control efectivo del usuario, permitiendo que el ejercicio de derechos no dependa exclusivamente de la voluntad de los desarrolladores o de la arquitectura técnica, sino que esté garantizado como una condición ética mínima para el uso legítimo de datos personales en entornos digitales.

ANÁLISIS DE LOS RESULTADOS

A partir de la revisión normativa, doctrinal y técnica realizada a lo largo de esta investigación, se pueden sintetizar los siguientes hallazgos relevantes:

- Compatibilidad condicional entre blockchain y el derecho de supresión: Aunque en un inicio se consideró que la inmutabilidad de blockchain hacía imposible el ejercicio del derecho de supresión, los avances técnicos han demostrado que esta incompatibilidad no es absoluta. Existen soluciones de diseño como el almacenamiento *off-chain*, la pseudonimización, el cifrado homomórfico y la separación entre hash e identidad, que permiten conciliar ambos valores, siempre que el hash no pueda ser vinculado a una persona física.
- Diseños híbridos como solución viable: La propuesta más viable en la actualidad consiste en

ISSN: 2966-0599
contato@ouniversoobservavel.com.br
www.ouniversoobservavel.com.br
Periódico Científico Indexado

almacenar los datos personales fuera de la blockchain (off-chain) y vincularlos a la cadena mediante identificadores criptográficos. Este enfoque permite eliminar o modificar los datos en servidores controlados por el usuario o el responsable del tratamiento, sin alterar la cadena de bloques, manteniendo así tanto la integridad técnica como el cumplimiento normativo. Se insiste que para esto se requerirían reformas a la LOPDP pues el responsable de tratamiento en la ley actual no tiene un claro rol cuando se trata de estructuras descentralizadas.

- Experiencias internacionales exitosas: Países como Estonia y Francia han logrado implementar sistemas basados en blockchain compatibles con el derecho de supresión, gracias a su enfoque regulatorio flexible, tecnológicamente informado y centrado en los derechos humanos. Estas jurisdicciones no han prohibido la innovación, sino que han regulado su uso mediante guías técnicas, estructuras de gobernanza y marcos de cumplimiento adaptativos.
- Ecuador: normativa reconocida, implementación ausente: Aunque Ecuador ha reconocido formalmente el derecho de supresión tanto en su Constitución como en la Ley Orgánica de Protección de Datos Personales, la falta de desarrollo reglamentario y técnico impide que este derecho sea efectivamente aplicable en entornos basados en blockchain. No existen lineamientos sobre almacenamiento descentralizado, ni criterios para distinguir entre blockchains públicas, privadas o con permisos, lo que debilita la operatividad de la norma.
- Necesidad de un enfoque interdisciplinario: Los resultados indican que la solución al conflicto entre tecnología e inmutabilidad no es exclusivamente jurídica ni técnica. Se requiere un enfoque interdisciplinario, que combine el análisis normativo con conocimientos de ingeniería informática, ciberseguridad, ética digital y gobernanza de datos. En este punto, vale la pena explorar los *hard fork* o procesos de reescritura consensuada a mayor profundidad en un trabajo futuro, particularmente por los efectos que estos procesos técnicos podrían tener sobre la inmutabilidad de las blockchain.
- Urgencia de reforma regulatoria en Ecuador: La situación nacional revela un vacío operativo que podría derivar en vulneraciones a los derechos fundamentales si no se implementan, de manera urgente, mecanismos normativos, institucionales y técnicos que orienten el uso de tecnologías disruptivas conforme a los principios del Estado constitucional de derechos y justicia.

CONCLUSIONES

1. El estudio ha evidenciado que la tensión entre blockchain y el derecho de supresión no es únicamente un conflicto técnico, sino un problema de fondo entre dos paradigmas: el de la descentralización tecnológica y el del control individual sobre la información. Mientras la primera apuesta por la inmutabilidad, la segunda exige flexibilidad jurídica para proteger los derechos fundamentales.
2. A nivel internacional, diversas jurisdicciones han comenzado a implementar modelos que permiten cierta armonización entre ambos principios. Soluciones como la pseudonimización, la segmentación off-chain, y la programación de derechos mediante smart contracts demuestran que la tecnología puede adaptarse al derecho, siempre que se diseñe con enfoque ético y legal desde su origen.
3. En Ecuador, si bien la Ley Orgánica de Protección de Datos Personales reconoce formalmente el derecho de supresión, existe una laguna regulatoria respecto a su aplicación efectiva en entornos descentralizados blockchain. La ausencia de lineamientos técnicos, jurisprudencia vinculante y estándares regulatorios impide a los desarrolladores, empresas y funcionarios públicos actuar con seguridad jurídica.
4. La investigación confirma que no es necesario renunciar a los beneficios de la tecnología blockchain para garantizar la protección de datos personales. Por el contrario, el desafío radica en diseñar entornos de innovación tecnológica regulada, donde

ISSN: 2966-0599
contato@ouniversoobservavel.com.br
www.ouniversoobservavel.com.br
Periódico Científico Indexado

los valores jurídicos y constitucionales formen parte de la arquitectura misma del sistema.

5. El artículo concluye que es urgente un enfoque de gobernanza algorítmica que integre principios jurídicos en el diseño y despliegue de tecnologías disruptivas. Solo así se podrá proteger de forma efectiva la dignidad humana, el consentimiento informado y la autodeterminación informativa en la era digital. Esto se debe trabajar en conjunto con los equipos técnicos y fundadores de soluciones tecnológicas para evitar que una adecuada gobernanza y regulación se convierta en una traba para el desarrollo.

RECOMENDACIONES

1. Desarrollo de lineamientos técnicos oficiales: El Estado ecuatoriano, a través de la Superintendencia de Protección de Datos Personales, deberá emitir normas técnicas que orienten el tratamiento de datos personales en entornos blockchain, incluyendo criterios sobre anonimización, segmentación de datos y consentimiento.

2. Incorporación de principios jurídicos en el diseño tecnológico: Las universidades, empresas tecnológicas y desarrolladores deben trabajar con juristas para asegurar que los sistemas blockchain se construyan respetando el marco constitucional y legal, integrando el derecho de supresión como una función programable.

3. Reformas a la legislación secundaria: Se recomienda reformar la LOPDP para incorporar disposiciones específicas sobre tecnologías emergentes, como blockchain, inteligencia artificial y big data, asegurando la protección efectiva de los derechos digitales. En virtud de la complejidad de estos procesos, y con el objetivo de no detener o trabar el desarrollo tecnológico, se debe considerar la aplicación de la figura de sandbox regulatorio para tecnología blockchain.

4. Capacitación de operadores jurídicos y técnicos: Se debe fortalecer la formación interdisciplinaria de jueces, legisladores, programadores y abogados en temas de gobernanza tecnológica, ética digital y derechos humanos, a fin de garantizar una interpretación armónica entre tecnología y derecho.

5. Establecer precedentes jurisprudenciales nacionales: La Corte Constitucional del Ecuador debe pronunciarse sobre la aplicabilidad del derecho de supresión en entornos tecnológicos, con el fin de orientar a los órganos judiciales inferiores y asegurar el respeto del bloque de constitucionalidad.

6. Promover blockchains híbridas y reversibles: Fomentar la investigación y desarrollo de modelos blockchain adaptativos que permitan la ejecución de derechos fundamentales como el derecho de supresión sin sacrificar la eficiencia, trazabilidad y descentralización.

REFERENCIAS

Arias Galicia, F. (2012). *El proyecto de investigación científica en el contexto universitario*. México: Trillas.

CNIL. (2018). *Blockchain et protection des données personnelles*. Commission Nationale de l'Informatique et des Libertés. https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_blockchain.pdf

De Filippi, P., & Wright, A. (2018). *Blockchain and the law: The rule of code*. Harvard University Press.

Doneda, D., & Monteiro, F. (2020). A proteção de dados pessoais no Brasil: Convergência com a GDPR e desafios na implementação da LGPD. *Revista de Direito da Proteção de Dados e Privacidade*, 1(1), 151–164.

European Parliament. (2016). *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 (Reglamento General de Protección de Datos - RGPD)*. Diario Oficial de la Unión Europea, L 119/1.

E-Estonia Briefing Centre. (2020). *The Digital Republic: How Estonia Leads in Digital Governance*. https://e-estonia.com

Finck, M. (2018). Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law? *European Data Protection Law Review*, 4(1), 74–95.

ISSN: 2966-0599
contato@ouniversoobservavel.com.br
www.ouniversoobservavel.com.br
Periódico Científico Indexado

https://doi.org/10.21552/EDPL/2018/1/6

Google Spain SL v. Agencia Española de Protección de Datos (TJUE, C-131/12). Sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014.

Hernández, R., Fernández, C., & Baptista, P. (2014). *Metodología de la investigación* (6.ª ed.). McGraw-Hill Education.

Kosseff, J. (2018). *The privacy advocate's guide to blockchain: Technical and legal considerations*. *Iowa Law Review*, 103(1), 193–220.

Kuner, C., Cate, F. H., Millard, C., & Svantesson, D. J. B. (2017). The challenge of 'big data' for data protection. *International Data Privacy Law*, 7(1), 47–51. https://doi.org/10.1093/idpl/ipx005

Pérez Luño, A. E. (2007). *Derechos humanos y revolución tecnológica*. Madrid: Editorial Tecnos.

Registro Oficial del Ecuador. (2021). *Ley Orgánica de Protección de Datos Personales*. Suplemento No. 459, 26 de mayo de 2021.

Sentencia No. 1149-19-JP/21. Corte Constitucional del Ecuador.

Tapscott, D., & Tapscott, A. (2016). *Blockchain revolution: How the technology behind bitcoin is changing money, business, and the world*. Penguin.

Vigo, R. J. (2001). *Fundamentos de la fenomenología jurídica*. Buenos Aires: Abeledo-Perrot.

Yeung, K. (2018). Algorithmic regulation: A critical interrogation. *Regulation & Governance*, 12(4), 505–523. https://doi.org/10.1111/rego.12160

Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing privacy: Using blockchain to protect personal data. *Proceedings of the IEEE Security and Privacy Workshops*, 180–184. https://doi.org/10.1109/SPW.2015.27