
EDUARDO ANDRÉS CALDERÓN MARENCO
UNIVERSIDAD COOPERATIVA DE COLOMBIA, COLOMBIA
eduardo.calderon@campusucc.edu.co

IRENE JOSÉ PAOLA RAÚDEZ HERNÁNDEZ
UNIVERSIDAD AMERICANA DE MANAGUA, NICARAGUA
ipraudez@uamv.edu.ni

DESINFORMACIÓN DIGITAL Y DEMOCRACIA EN IBEROAMÉRICA: RETOS Y OPORTUNIDADES DE LA LEX CRIPTOGRÁFICA¹

DIGITAL DISINFORMATION AND DEMOCRACY IN LATIN AMERICA: CHALLENGES AND OPPORTUNITIES OF THE CRYPTOGRAPHIC LEX

Cómo citar el artículo:

Calderón E, Raúdez I, (2024). Desinformación digital y democracia en Iberoamérica: retos y oportunidades de la Lex Criptográfica. Derecho Global. Estudios sobre Derecho y Justicia, IX (26) <https://10.32870/dgedj.v9i26.728> pp. 377-401

Recibido: 29/09/23 Aceptado: 02/02/24

¹ El artículo es producto del proyecto de investigación titulado: Smart contracts y Blockchain: desafíos del ordenamiento jurídico colombiano y argentino. El proyecto es financiado entre la Universidad Cooperativa de Colombia, la Universidad Americana (UAM) y la Universidad de Concepción del Uruguay.

RESUMEN

En los últimos cinco años, desde 2019 hasta 2023, ha ganado fuerza el fenómeno de la desinformación en internet. Este preocupante auge se ha visto favorecido por el surgimiento de la pandemia de Covid-19 y las particulares características de las redes sociales digitales. A partir de un análisis documental de objeto de estudio, la desinformación digital, esta investigación propone la implementación de la Lex Criptográfica utilizando tecnología *Blockchain* como solución innovadora. La Lex Criptográfica busca asegurar la autenticidad de la información en línea y fomentar la alfabetización digital, permitiendo a las personas discernir entre información confiable y engañosa. Sin embargo, su implementación enfrenta desafíos como la protección de datos, la privacidad y la educación pública. La colaboración entre expertos técnicos, reguladores y profesionales legales, junto con una educación pública efectiva, son fundamentales para superar estos obstáculos y construir una sociedad informada y crítica en la era digital.

PALABRAS CLAVE

Desinformación digital; Lex Criptográfica; Tecnología Blockchain; Iberoamérica; Alfabetización digital.

ABSTRACT

During the period 2019-2023, digital misinformation has become a global challenge, particularly in Ibero-America, sparking new discussions about its negative effects that, in turn, impact the democratic systems of states. Based on a documentary analysis of the object of study, digital misinformation, this research proposes the implementation of the Cryptographic Lexicon using Blockchain technology as an innovative solution. The Cryptographic Lexicon aims to ensure the authenticity of online information and promote digital literacy, enabling individuals to discern between reliable and deceptive information. However, its implementation faces challenges such as data protection, privacy, and public education. Collaboration among technical experts, regulators, and legal professionals, along with effective public education, is essential to overcome these obstacles and build an informed and critical society in the digital era.

KEYWORDS

Digital misinformation; Cryptographic Lexicon; Blockchain technology; Ibero-America; Digital literacy.

Sumario: I. Introducción. II. ¿Qué es desinformación? III. Desinformación en el contexto digital. 1. Propagación exponencial de desinformación durante la pandemia del COVID-19. IV. Lex Criptográfica: una herramienta para la problemática. 1. Definiendo la Lex Criptográfica. 2. Innovación en la lucha contra la Desinformación Digital. 3. Aplicación de la tecnología Blockchain en la verificación de información. 4. Desafíos y consideraciones de la Lex Criptográfica. V. Conclusiones. Bibliografía.

I. INTRODUCCIÓN

En los últimos cinco años, desde 2019 hasta 2023, ha ganado fuerza el fenómeno de la desinformación en internet. Este preocupante auge se ha visto favorecido por el surgimiento de la pandemia de Covid-19 y las particulares características de las redes sociales digitales. Por un lado, la crisis sanitaria mundial generó incertidumbre e inquietud entre la población, terreno fértil para la propagación de noticias falsas. Por otro lado, las plataformas virtuales permiten una masiva y rápida circulación de todo tipo de contenidos, lo que facilita la viralización de la desinformación.

A lo largo de la historia, la manipulación informativa ha sido utilizada como método de influencia política y social. No obstante, las nuevas herramientas tecnológicas han simplificado en extremo esta práctica. Gracias a su alcance sin precedentes, resulta ahora mucho más sencillo inducir determinados comportamientos entre amplios sectores de la ciudadanía.

Los estudios de Aïmeur, Amri y Brassard (2023), así como de Horder (2021), arrojan luz sobre la persistencia histórica de la desinformación y su mayor prevalencia con Internet. Por un lado, los primeros analizan cómo ya existían noticias falsas antes de la impresión de libros. Según señalan, Sócrates fue condenado por propagar información errónea entre los jóvenes.

Asimismo, existe una explosión del término *fake news* en 2016, durante las elecciones estadounidenses, que se reconoce internacionalmente. Horder (2021), por otro lado, realiza la comparación con el comportamiento estadounidense, en 2004 sólo el 18% de la población mencionaba Internet como fuente primaria de información para las elecciones, mientras que para 2016 este porcentaje aumentó al 65%.

La exposición de datos relativos a Estados Unidos reviste particular relevancia, dado que este país difunde el término *fake news*. Dicho concepto fue luego adoptado por medios de comunicación iberoamericanos e incorporado incluso en legislaciones de la región.

El investigador Ángel Badillo (2019) señaló que la democratización del acceso a Internet ha dado lugar a una transformación del espacio digital, configurándose ahora como un escenario geoestratégico. Esta evolución pone de relieve la creciente dimensión que ha alcanzado el problema de la desinformación en la actual era digital. Su difusión masiva a través de las plataformas virtuales convierte su abordaje en una cuestión apremiante si se desea salvaguardar la salud de los debates públicos y los procesos democráticos.

Resulta crucial ilustrar la evolución reciente de este fenómeno a través del análisis de casos emblemáticos acaecidos en la región iberoamericana en los últimos años. El examen detallado de estos sucesos permitirá contextualizar los efectos de la desinformación en dicha área geográfica.

Dicho estudio pondrá de manifiesto el alcance e impacto del problema, así como la urgencia de implementar estrategias efectivas que contrarresten el mismo. Solo comprendiendo a profundidad las causas subyacentes al fenómeno será posible abordarlo de un modo eficiente, que tutele los valores democráticos de estas naciones.

Al respecto, la evaluación de los enfoques iberoamericanos revela dos posturas extremas: por un lado, algunos Estados limitan la mala información mediante regulaciones estrictas que imponen penalizaciones, por otro, otros dejan la información completamente libre, lo que puede socavar las democracias y el bien común (Hernández et al., 2022).

En este contexto, es esencial fomentar el discernimiento crítico en la población. Más que sólo otorgar libertades, se deben implementar políticas que otorguen herramientas a las personas para distinguir entre información confiable o engañosa sin restringir la misma. Este equilibrio es crucial para contrarrestar la desinformación de manera efectiva, preservando la integridad democrática.

Más allá de simplemente conceder derechos, se propone una solución equilibrada y perspicaz para abordar esta problemática creciente en Iberoamérica. Esta solución se encuentra en la implementación de la *Lex Criptográfica*, con la introducción del *Blockchain* como una herramienta tecnológica que pretende ser un puente para la alfabetización digital con el fin de contrarrestar la desinformación de los medios digitales.

Esta investigación detallada sobre las tácticas de desinformación en Iberoamérica explora las complejidades de este fenómeno y evalúa la viabilidad del *Blockchain*, mediante un enfoque basado en la criptografía, como una solución innovadora a esta problemática.

En este estudio, se examinan detenidamente las estrategias de difusión de noticias falsas, explorando la aplicabilidad específica de la variante tecnológica mencionada para garantizar la autenticidad de la información en línea. Además, se desarrollan recomendaciones prácticas que abarcan aspectos técnicos, legales y éticos. Este enfoque holístico identifica patrones recurrentes y vulnerabilidades en el sistema digital, fundamentando así las propuestas de solución. Por tanto, el objetivo general de este estudio es analizar el creciente fenómeno de la desinformación digital en Iberoamérica a partir del uso del internet para proponer soluciones a través de la tecnología *Blockchain*.

Para alcanzar este objetivo general, se desarrollan tres objetivos específicos. El primero consiste en analizar las principales causas y mecanismos de propagación de la desinformación en la región. El segundo objetivo es caracterizar el marco de la tecnología *Blockchain* y la *Lex Criptográfica* aplicables a la verificación de datos. Por último, proponer líneas de acción a través de la tecnología de *Blockchain* para la formulación de políticas públicas.

En el núcleo de esta investigación se plantea una pregunta crucial: ¿cómo puede la implementación de la *Lex Criptográfica* contrarrestar la desinformación y la

manipulación de información en Iberoamérica? Esta interrogante fundamental orienta todo el proceso investigativo, impulsando una exploración profunda y una evaluación meticulosa de las tácticas necesarias para hacer frente a este desafío digital.

Atendiendo a lo comentado anteriormente, se plantea que la implementación de la *Lex Criptográfica* en países iberoamericanos, como estrategia para mitigar la desinformación, no solo asegura la autenticidad de la información en línea, sino que también tiene el potencial de fomentar el uso de tecnologías como *Blockchain* entre los ciudadanos. Esta medida no solo impulsa la alfabetización digital, sino que también capacita a las personas para verificar la información de manera independiente, convirtiéndose en verificadores autónomos. Al proporcionar a las personas las herramientas para discernir datos y utilizar *Blockchain*, se restaura la confianza en la información digital, fortaleciendo así la democracia y cultivando una sociedad activa y crítica en la verificación de datos.

La presente investigación es de índole jurídico-descriptiva, ya que tiene como objetivo describir las características del fenómeno de la desinformación digital y la *Lex Criptográfica* para proponer posibles soluciones. Asimismo, se enmarca como una investigación teórica, dado que busca argumentar a partir de una revisión teórica los elementos que componen el objeto de estudio y su incidencia en el ámbito jurídico.

Para ello, se llevará a cabo un análisis exhaustivo del contenido que involucra recursos bibliográficos. Este análisis meticuloso permitirá identificar patrones y temas recurrentes relacionados con la desinformación. Cada hallazgo será respaldado por una rigurosa citación de todas las fuentes utilizadas, garantizando la transparencia y el debido reconocimiento del trabajo previo en el ámbito de estudio. Este enfoque inexorable no sólo respalda la implementación de la *Lex Criptográfica*, sino que también crea una base sólida y confiable para enfrentar los desafíos de la desinformación en la era digital

II. ¿QUÉ ES DESINFORMACIÓN?

La extensión del término desinformación abarca una amplia gama de otros conceptos que la definen. Estos van más allá de las noticias falsas o *fake news* e

incluyen la manipulación deliberada de la información. El poder de difusión de la información permite a quienes tienen la facilidad de difundirla alterar o cambiar por completo el origen o el contenido bruto de la información, con el objetivo de generar reacciones en la sociedad apelando a las emociones. Es importante reconocer este fenómeno, ya que se extiende a toda forma de comunicación, habiéndose utilizado durante siglos como una forma de dominio y poder por aquellos que lo emplean como un arma para influir en la opinión pública.

Entre los distintos generadores y difusores de desinformación se encuentran diversos actores políticos, como algunos partidos que la utilizan como estrategia de comunicación directamente a través de noticias falsas o sesgando la información; también colectivos de ideología radical buscan polarizar mediante contenidos identitarios excluyentes. Asimismo, determinados gobiernos recurren a estas técnicas para fines de desestabilización política e influencia. Por otra parte, existen agentes económicos cuyo modelo de negocio se sustenta en la monetización masiva de este contenido engañoso. Comprender la variedad de intereses y objetivos de estos actores, tanto estatales como no estatales, es crucial para atender las causas y mecanismos de difusión de la desinformación de forma integral, desde una perspectiva que reconozca su complejidad y alcance (López-López et al., 2023).

La desinformación en Iberoamérica no se limita a la mera difusión de datos incorrectos; penetra profundamente en la convivencia democrática, creando divisiones significativas en la sociedad. Asimismo, este problema tiene raíces en una historia prolongada de conflictos entre líderes políticos y los medios de comunicación en la región, mucho antes de que el término posverdad se volviera común (Amado, 2022). A lo largo de la historia, líderes políticos y otros colectivos han utilizado los medios de comunicación para manipular la opinión pública en su beneficio, resaltando la importancia de este poder de *agenda setting* (Becerra, 2014).

La mencionada problemática se manifiesta en dos esferas: los hechos y las emociones. Estas se han convertido en herramientas comunes en el ámbito político, utilizadas para desafiar hechos verificables. Se aprovecha el poder de las emociones para permitir a los políticos evadir consecuencias al distorsionar la verdad. Esta estrategia se basa en la premisa de que las emociones, al ser experiencias genuinas

e incontrolables, se perciben como auténticas y se asocian con la verdad. La capacidad de reclamar derechos políticos basados en la diferencia emocional y la percepción personal se convierte en un punto de partida fundamental para estos discursos políticos (Manfredi et al., 2022).

Considerando esta dinámica, el Balance 2022 de periodistas encarcelados, asesinados, secuestrados y desaparecidos en el mundo, publicado por Reporteros sin Fronteras, revela una realidad alarmante: casi el 65% de los periodistas asesinados en 2022 perdieron la vida en países que, en teoría, se consideran en paz. México, con 11 periodistas asesinados, representa cerca del 20% del total de profesionales de la información fallecidos este año, junto con cifras impactantes en Haití (seis asesinados) y Brasil (tres). Estos datos destacan a Iberoamérica como la región más peligrosa para los periodistas en todo el mundo, resaltando la urgente necesidad de abordar esta grave situación en la región.

A pesar de la alarma que suscitan los datos sobre la escasa o nula libertad de prensa en muchos países de la región iberoamericana, existe un antecedente histórico que documenta la utilización de canales de comunicación para influir en la opinión pública. Esta relación histórica ilustra cómo los líderes políticos dependen en gran medida de la percepción que el pueblo tiene de ellos, subrayando la importancia crucial del concepto de opinión pública en el desarrollo político. Los medios de comunicación y el ejercicio periodístico desempeñan un papel fundamental al servir como una plataforma esencial para moldear y transmitir esta percepción (González et al., 2023).

Por otra parte, es importante destacar que la respuesta regulatoria ante la desinformación es un desafío complejo, ya que involucra decisiones sobre quiénes y cómo deben llevar a cabo la regulación. Este proceso se complica aún más debido a las implicaciones para las libertades de expresión e información tanto de los usuarios como de las redes y plataformas. Se reconoce que algunos fenómenos de desinformación pueden quedar fuera de la respuesta jurídica. Existen argumentos a favor de evitar la regulación en algunos casos, y se destaca la importancia de impedir que organismos gubernamentales no independientes evalúen o restrinjan los contenidos, evitando así la orquestación del debate político (Cotino Hueso, 2022).

III. DESINFORMACIÓN EN EL CONTEXTO DIGIT

En la actual sociedad digital, el fenómeno de la desinformación sigue representando un gran desafío para la convivencia democrática. Como señalan López López et al. (2023), durante eventos políticos cruciales tales como campañas electorales, las noticias falsas tienen el potencial de interrumpir discursos legítimos y profundizar divisiones entre la ciudadanía.

Más que la libertad de expresión, estos procesos comunicativos que tienen lugar en las redes sociales ponen en juego fundamentalmente la libertad de comunicar información veraz y el derecho a recibirla de manera imparcial. Según lo planteado por Guardado (2023) en su obra “Desinformación, odio y polarización en el entorno digital”, este tipo de interacciones digitales suelen politizarse en torno a la confrontación de ideologías opuestas, construyendo falsos “enemigos”, en lugar de promover el debate constructivo de ideas. Esta dinámica de polarización puede llegar a cuestionar el ejercicio independiente del poder por parte de los organismos encargados de regular el acceso a información de los ciudadanos, y dificulta alcanzar consensos que garanticen la convivencia democrática entre grupos con posturas diferenciadas, objetivo que debe perseguir todo Estado de derecho.

Ante este panorama, se torna crucial proteger y preservar la integridad de los medios de comunicación tradicionales. Estos cumplen un rol fundamental para mantener informada a la población con contenidos verificados y, de ese modo, sostener una democracia participativa donde primen los hechos sobre las especulaciones. Una ciudadanía con mayores competencias digitales también es clave para hacer frente a los desafíos de una era signada por un exceso de información no siempre confiable.

Tal como señala, el auge de la inteligencia artificial y el aprendizaje automático ha transformado significativamente las campañas electorales al permitir un análisis detallado de los perfiles ciudadanos y sus comportamientos en línea. Sin embargo, en Iberoamérica persiste la falta de regulación efectiva respecto al uso de estos avances tecnológicos, lo que facilita que la desinformación digital se propague rápidamente a través de las redes sociales y servicios de mensajería, socavando la confianza de la ciudadanía en las fuentes de información y distorsionando con frecuencia los debates públicos (Amado, 2022).

A pesar del progreso tecnológico, las iniciativas regulatorias en Iberoamérica frecuentemente han adoptado prácticas restrictivas, imponiendo normativas que, en lugar de fortalecer la lucha contra la desinformación, han restringido con frecuencia la libertad de expresión. Conceptos como la verdad y el pluralismo de voces se han utilizado en la legislación de modo que, en realidad, restringen la libertad de expresión sin apego suficiente a los derechos fundamentales (Manfredi et al., 2022).

En los países iberoamericanos, con frecuencia se han establecido medidas restrictivas mediante leyes tales como la denominada *Ley Mordaza*, que sancionan la opinión disidente y silencian voces críticas hacia el gobierno. Estas limitaciones se han intensificado a través de normativas que habilitan al poder Ejecutivo a cerrar medios de comunicación, bloquear sitios web y controlar contenidos en línea de forma discrecional. Asimismo, figuras legales como el *lawfare* (litigios abusivos) se utilizan con el fin de penalizar la labor periodística de investigación y la crítica política. Del mismo modo, la vigilancia masiva también ha propiciado la autocensura y el temor a represalias, creando un clima poco propicio para el ejercicio pleno de la libertad de expresión en la región (Amado, 2022).

Las campañas masivas de desinformación, particularmente durante procesos electorales, han ejercido presión sobre las grandes empresas tecnológicas para que asuman responsabilidad en este ámbito. Aunque se han explorado soluciones tecnológicas, tales como la optimización de algoritmos y la detección basada en inteligencia artificial, éstas presentan limitaciones. Esto ha impulsado el desarrollo del movimiento global de verificación de datos, una corriente periodística cuya práctica se centra en constatar la veracidad de afirmaciones y contenidos difundidos (Pérez-Díaz, 2022).

La organización en red de nuevos partidos y candidatos ha dado lugar a narrativas alternativas, cuestionando el monopolio informativo tradicional y transformando el discurso público. No obstante, el periodismo convencional ha sido eclipsado por la convergencia entre información y entretenimiento, así como por estrategias políticas de influencia mediática, lo que ha devenido en una pérdida progresiva de la calidad informativa y una mayor politización de los medios, erosionando de esta forma la confianza ciudadana en la imparcialidad periodística.

En Perú y Brasil, el uso estratégico de redes sociales durante campañas electorales exacerbó la polarización política mediante la difusión de mensajes radicales. Esto creó un álgido clima online donde proliferaron la desinformación y dudas sobre instituciones, ampliando divisiones sociales (Del Águila, 2023).

En Colombia también se ha enfrentado a un aumento significativo de desinformación durante eventos políticos cruciales, como las elecciones presidenciales de 2022, y en momentos de agitación social vinculados a escándalos como las ejecuciones extrajudiciales. La posverdad y la desinformación, influenciadas por dinámicas de poder, han socavado la confianza en la verdad objetiva y minado el respaldo a la democracia deliberativa y la información pública (Gutiérrez-Coba & Rodríguez-Pérez, 2023).

Las redes redefinieron el discurso público a través de emociones intensas, influyendo en creencias y comportamientos políticos que agravaron la polarización. La educación en alfabetización mediática, entendida como dotar de habilidades críticas para evaluar contenidos y discernir información veraz de falsa, resulta necesaria para distinguir entre hechos y ficción en este complejo contexto (González & Cardona-Restrepo, 2023).

La desinformación ha evolucionado significativamente, pasando de utilizar tácticas sencillas a incorporar sofisticadas tecnologías como las *deepfakes* y la realidad aumentada, lo que dificulta identificar la información auténtica en un entorno cada vez más saturado de engaños.

Por un lado, las *deepfakes* hacen referencia a contenidos digitales manipulados mediante inteligencia artificial, los cuales pueden hacer creer falsamente que una persona realiza determinadas acciones u emite dichos específicos. Por otro lado, la realidad aumentada permite superponer datos digitales sobre la realidad física, integrando así objetos virtuales de manera interactiva con el mundo real.

Asimismo, la diversificación del panorama informativo y la irrupción de nuevos actores políticos han fragmentado el control tradicional de los medios. A su vez, las redes sociales se han consolidado como campos de batalla ideológicos y políticos, democratizando la participación ciudadana pero también desafiando la influencia que antes ejercían los medios de forma predominante, todo ello en un contexto

donde priman las batallas partidistas por sobre el debate de las ideas (Magallón, 2022).

1. Propagación exponencial de desinformación durante la pandemia del COVID-19

La propagación de la desinformación se asemeja a la forma en que se propaga una epidemia. En este caso, individuos desinformados actúan como portadores (infectados) que intentan influir en una población susceptible transmitiendo mensajes con información falsa. Por tanto, los modelos que explican la difusión de la desinformación se basan en el modelo SIR (Susceptibles-Infectados-Recuperados). Este paralelo subraya cómo la desinformación se propaga de manera similar a una enfermedad contagiosa, afectando a la sociedad y generando consecuencias significativas, especialmente en el contexto del COVID-19 (Guzmán Rincón et al., 2023).

Los datos recopilados en el estudio de García-Marín y Merino-Ortego (2022) proporcionan información clave sobre la desinformación científica relacionada con dicha epidemia global que podría resultar útil en futuras pandemias y crisis sanitarias. El estudio mostró que las verificaciones de este tipo de desinformación fueron más prominentes en los primeros meses de la pandemia, cuando la población podía sentirse más vulnerable debido al miedo, la incertidumbre y la indignación provocados por la nueva situación y las medidas restrictivas adoptadas.

En la región, un caso preocupante fue el de México, donde la desinformación acerca del COVID-19 tuvo niveles alarmantes. En este hubo difusión de curas falsas y sitios web engañosos, creando un falso sentido de seguridad y llevando a la población a evitar medidas preventivas eficaces. Además, las autoridades han contribuido a esta confusión minimizando la gravedad del virus y generando una sensación de inmunidad en ciertos grupos. Estas acciones irresponsables han socavado la confianza pública y han puesto en peligro la salud durante la pandemia, subrayando la necesidad urgente de proporcionar información precisa y confiable a la población (Article 19, 2020).

Paralelamente, otro caso de desinformación relacionado con el COVID-19 en Iberoamérica ocurre en Ecuador a inicios de 2020, cuando se anuncia el primer contagio en el país. En ese momento comienza a circular en redes sociales información sin verificar sobre la paciente involucrada. Los principales medios también carecían de datos suficientes para contextualizar adecuadamente la noticia, lo que generó incertidumbre. Este vacío propició que diversas plataformas se llenaran de noticias falsas y rumores. El caso evidenció las dinámicas de desinformación que pueden darse cuando los medios tradicionales no cumplen con verificar y dar contexto oportunamente a una noticia de alto impacto (Isch, 2023).

IV. LEX CRIPTOGRÁFICA: UNA HERRAMIENTA PARA LA PROBLEMÁTICA

A pesar de las herramientas de verificación para filtrar contenido emocional, sus medidas no son suficientes ante la desinformación online. La alfabetización mediática, entendida como el conjunto de competencias para interpretar, gestionar y usar críticamente la información y tecnologías, es clave para abordar este problema sin restringir en exceso el flujo informativo pero vigilando discursos divisivos (Corona-Rodríguez, 2021).

La introducción de la tecnología Blockchain se propone como una herramienta clave para abordar el problema de la desinformación en línea. Al encriptar la información de manera descentralizada, blockchain podría establecer conexiones más seguras entre diversas fuentes de datos, validando el origen y autenticidad de los contenidos.

Antes de analizar en profundidad esta propuesta, es necesario explicar brevemente el origen, evolución y la propuesta de la “Lex Criptográfica” como el conjunto de normas legales necesarias para el desarrollo e implementación de soluciones basadas en blockchain ante la desinformación digital.

Una vez definido este contexto normativo, es posible ahondar en el potencial de la tecnología subyacente. Al descentralizar el almacenamiento de datos encriptados, blockchain podría fomentar la alfabetización mediática de los ciudadanos. Al validar fehacientemente el origen y evolución de la información, esta herramienta

técnica permitiría desarrollar competencias críticas a la hora de evaluar contenidos en línea.

1. Definiendo la Lex Criptográfica

La Lex Criptografica se puede entender como la extensión natural de la Lex Mercatoria. Al igual que ésta, la Lex Criptografica se basa en la autorregulación de los agentes que participan en la red blockchain más allá del monopolio legislativo estatal. Surge de forma similar a como lo hizo la Lex Mercatoria en la Edad Media y tras la Segunda Guerra Mundial, cuando los comerciantes crearon sus propias normas para escapar de los ordenamientos jurídicos formales de la época y favorecer el comercio internacional (López Rodríguez, 2021).

Para comprender mejor la Lex Criptográfica, es fundamental entender que la criptología, derivada del griego (Krytós lógos) que significa palabra oculta, se centra en el estudio de métodos para ocultar, almacenar, comunicar y revelar información. Su objetivo principal es asegurar la comunicación entre remitente y receptor, destacando el uso de técnicas criptológicas para garantizar la seguridad de la información transmitida. La criptología se basa en tres componentes esenciales: confidencialidad, integridad y disponibilidad (Cardoso, 2022).

Al igual que ocurre con la Lex Mercatoria, la Lex Criptográfica también ha sido objeto de críticas. Algunas de estas críticas son las mismas que se esgrimen contra la Lex Mercatoria, dado su origen no estatal y falta de legitimidad democrática. También se alega que carece de mecanismos coercitivos para hacer cumplir sus normas. Otras críticas son más propias y se refieren a que los algoritmos no pueden prever todas las circunstancias que pueden surgir en una relación contractual ni sustituir al Derecho en su función de organizar la sociedad y salvaguardar valores como el orden público o los derechos fundamentales (López Rodríguez, 2021).

La exploración de la criptografía y su funcionamiento es algo que se ha aventurado en mayor medida en las ciencias económicas y su desenvolvimiento en la sociedad. Un ejemplo ilustrativo es el uso de criptomonedas, las cuales se generan y transfieren de manera descentralizada mediante técnicas de criptografía para garantizar la integridad. Además, se respaldan en tecnologías de registro o libros de contabilidad gestionados y actualizados de forma independiente por numerosas computadoras.

Este proceso tiene como objetivo verificar la autenticidad y evitar duplicaciones en el uso de las criptomonedas (Barroilhet Díez, 2019).

La Lex Criptográfica revela su conexión con la programación informática como una herramienta para dar forma a acuerdos privados con implicaciones legales, como los contratos. En este contexto, la Lex Criptográfica se desarrolla a través de prácticas y costumbres arraigadas en la comunidad de usuarios del entorno digital, estableciendo las bases para la creación de normas comunes. La efectividad de estas normas depende de la formación de la *opinio iuris*.

Es esencial vincular estas prácticas y costumbres con el ámbito de la criptología, ya que desempeña un papel crucial en la seguridad de la información. La criptología asegura la inalterabilidad de los datos, garantiza su perdurabilidad, reduce costos y fomenta la confianza. En este sentido, la Lex Criptográfica incorpora la seguridad como uno de sus aspectos fundamentales, convirtiéndola en un recurso valioso en el contexto de la certificación (Diago Diago, 2021). Cabe destacar que la seguridad se ve significativamente reforzada por la tecnología blockchain, reconocida como “una de las tecnologías más relevantes para la protección de la información de las transacciones” (Valencia-Arias et al., 2023, p. 217).

Considerando lo mencionado anteriormente, al emprender el proceso de definición de la *Lex Criptográfica*, es esencial comprender que esta se manifiesta siempre a través de un código computacional expresado en un lenguaje de programación. Este código se utiliza para crear un contrato inteligente, el cual debe insertarse de manera encriptada en la tecnología Blockchain. Resulta imposible desvincular elementos esenciales como el código, la información, la criptografía y la cadena de bloques en la delimitación de esta Lex.

En otras palabras, la *Lex Criptográfica* toma forma a través de una sinergia de componentes tecnológicos, donde el código actúa como el lenguaje que define los términos de la información. Esta información se asegura y registra de manera segura mediante la encriptación de la tecnología *Blockchain*, creando así un sistema regulatorio que depende intrínsecamente de estos elementos interconectados. La inseparabilidad de estos componentes es lo que da forma y fundamento a la *Lex Criptográfica*.

En este contexto, la Lex Criptográfica emerge como un enfoque legal innovador en relación con la tecnología *Blockchain* y las criptomonedas. A diferencia de los sistemas legales convencionales, esta se fundamenta en protocolos y códigos de software, fomentando estructuras jurídicas descentralizadas que van más allá de las fronteras nacionales. Esta nueva perspectiva legal rechaza la dependencia de interpretaciones subjetivas, centrándose en datos y votaciones mayoritarias para establecer decisiones judiciales (Becker, 2022).

En Iberoamérica, este enfoque adquiere especial relevancia en la lucha contra la desinformación. La implementación de la tecnología *Blockchain* a través de la *Lex Criptográfica* podría proporcionar conexiones de información más seguras mediante codificación descentralizada. Sin embargo, para aprovechar al máximo este potencial, es fundamental instruir a la población sobre el uso de esta herramienta y sus diversas aplicaciones, más allá de simplemente combatir la desinformación. Este conocimiento no solo fortalecerá la capacidad de discernir información confiable de la manipulada, sino que también allanará el camino hacia una sociedad digital más segura y participativa en la región iberoamericana.

2. Innovación en la lucha contra la Desinformación Digital

En la lucha contra la desinformación digital, se ha propuesto usar *Blockchain* para verificar identidades de manera segura sin revelar datos personales. Aunque es un avance importante, hay desafíos, como mantener la seguridad de los datos mientras se distribuyen tareas computacionales. Para contrarrestar la desinformación, es esencial ilustrar a las personas sobre cómo funcionan estas tecnologías y brindar acceso fácil y comprensible a estas innovaciones (Malina et al., 2021).

¿Pero qué es exactamente la tecnología *Blockchain* y cómo puede utilizarse de la manera que aborda este artículo? Para entenderlo, la tecnología *blockchain* es un sistema de registro digital que permite un seguimiento seguro e inalterable de la información, ya sea de forma pública o privada. Su valor radica en su capacidad para crear registros transparentes y resistentes a la manipulación. En la lucha contra la desinformación digital, las cadenas de bloques públicas pueden verificar la autenticidad de datos, como noticias y verificaciones de hechos, evitando la alteración de la información (Sulkowski, 2018).

Además, al establecer reglas claras y difíciles de violar mediante código digital, se crea un entorno en línea más seguro y transparente, empoderando a los usuarios para discernir información confiable de la manipulada. Esta combinación de tecnología *Blockchain* y regulación mediante código digital se presenta como una estrategia innovadora e integral para abordar la desinformación digital de manera efectiva (Ungureanu, 2020).

Raikwar et al. (2019) proporcionan información valiosa sobre las diferentes clasificaciones de las *Blockchains* y los sistemas de autorización descentralizados. En el contexto de combatir la desinformación, es esencial elegir la tecnología adecuada para asegurar la autenticidad de la información y permitir un acceso sin restricciones al conocimiento genuino. Hay opciones que van desde *Blockchains* públicas totalmente abiertas hasta privadas altamente seguras. La elección óptima podría ser una tecnología pública con permisos, que equilibra transparencia y seguridad. En este modelo, expertos verificadores validan la autenticidad de la información, proporcionando una forma sólida de verificar datos confiables y luchar eficazmente contra la desinformación digital.

3. Aplicación de la tecnología Blockchain en la verificación de información

La tecnología *Blockchain* permite conectar diferentes organizaciones sin importar las fronteras, creando un registro seguro e inmutable de información. Esto significa que todas las partes pueden acceder a documentos relacionados con información engañosa de forma segura y transparente en línea. Además, *Blockchain*, junto con otras tecnologías, protege contra la difusión de información falsa en sistemas públicos y privados. Esta tecnología actúa como una especie de ley digital, regulando acciones y transacciones de manera confiable, lo que podría cambiar la forma en que la ley y la tecnología se integran en el futuro (Dimitropoulos, 2020), pero lo cierto es que ya se hace uso de estas prácticas que han configurado a la *Lex Criptográfica*.

En Brasil, la *Lex Criptográfica* se ha vuelto crucial en la lucha contra la desinformación digital. Se estableció la Infraestructura de Clave Pública Brasileña (ICP-Brasil) para autenticar documentos electrónicos, utilizando criptografía

para proteger firmas digitales y permitir transacciones seguras en línea. Además, la criptología, incluida la criptografía, está sujeta a regulación legal. La *Lex Criptográfica* o regulación inteligente implica el uso de códigos autoejecutables protegidos por criptografía en lugar de depender de las predicciones de legisladores. Esta innovadora propuesta garantiza la seguridad y la ejecución automática de las leyes, utilizando tecnología criptográfica para proteger las normativas legales de manera eficaz y segura (Cardoso, 2022).

Esta propuesta de regulación se presenta como una innovación que sirve de puente hacia una información más segura, aprovechando la tecnología *Blockchain*. En este proceso, la educación emerge como un pilar fundamental. Instruir a la población sobre esta tecnología y sus implicaciones es crucial, ya que representa no solo una forma de autolegislación, sino también una educación jurídica autónoma. Este conocimiento capacita a las personas para comprender la tecnología y participar activamente en su desarrollo y regulación. (Dimitropoulos, 2020).

La implementación de esta regulación ofrece una oportunidad invaluable para dotar a las personas con conocimientos y habilidades necesarios para contribuir a la construcción de un futuro digital más seguro y transparente. Al promover la comprensión y la adopción de esta tecnología, la región iberoamericana podría inaugurar una nueva era de autolegislación y educación jurídica. Este enfoque transformaría fundamentalmente la forma en que las sociedades interactúan con la información, redefiniendo las estructuras legales y sociales en el mundo digital.

4. Desafíos y consideraciones de la Lex Criptográfica

La *Lex Criptográfica* enfrenta mayores desafíos cuando trasciende el ámbito contractual para involucrarse en el uso y compartir de información de manera más general. La verificación y lucha contra la desinformación requieren mecanismos regulados que puedan dar respuesta a problemáticas como la protección de datos y derechos de autor, las cuales se rigen por un marco normativo más complejo que el contractual. Dado que esta información podría involucrar intereses más allá de las partes en una transacción e incluso afectar terceros, es necesario que esté sujeta al escrutinio de jueces y tribunales. Del mismo modo, se debe reconocer la representación de otros actores involucrados y la interfaz con los sistemas legales tradicionales.

La naturaleza transfronteriza y el manejo de datos sensibles conlleva la necesidad de establecer estándares y mecanismos de supervisión regulatoria que garanticen derechos, debido a que excede el marco de la mera autorregulación. Por lo tanto, su implementación en este ámbito demanda trabajar de forma coordinada con las legislaturas para desarrollar la seguridad jurídica requerida ante la complejidad normativa y de intereses en juego (Rodríguez, 2021).

La implementación de esta tecnología requiere una comprensión profunda de sus complejidades. Además, la colaboración cercana entre expertos técnicos y reguladores se vuelve crucial para asegurar su aplicación segura y efectiva en la lucha contra la desinformación. Superar los desafíos asociados con la integración de esta tecnología en un entorno digital tan dinámico y complejo es fundamental. Estos desafíos incluyen cuestiones de privacidad, interoperabilidad y educación pública sobre el uso adecuado de esta tecnología para verificar la autenticidad de la información. En última instancia, aunque la elección de la clasificación adecuada de *Blockchain* es un paso crucial, abordar la desinformación requiere un enfoque colaborativo y multifacético para superar estos obstáculos y construir una infraestructura digital más confiable y segura (Agnikhotram et al., 2019).

La educación tanto del público en general como de los profesionales del derecho se presenta como un desafío fundamental. La falta de comprensión puede dar lugar a malentendidos y conflictos legales. Por esta razón, es crucial implementar programas educativos que garanticen que los ciudadanos y los expertos legales estén plenamente informados sobre el funcionamiento de la lex criptográfica y las implicaciones legales de las transacciones basadas en *Blockchain*.

En última instancia, la implementación efectiva de esta tecnología en el ámbito de la información requiere una colaboración estrecha y continua entre expertos técnicos, reguladores y profesionales legales. Solo a través de una comprensión profunda, la formulación de regulaciones apropiadas y la educación pública se podrán superar los desafíos y construir una infraestructura digital confiable y segura para el intercambio de información en un país.

La colaboración entre el gobierno y el sector privado se convierte en un elemento crucial, especialmente dado el histórico problema de desinformación fomentada

tanto por actores políticos como privados. Ignorar estos problemas o mostrar falta de interés en abordarlos podría agravar las dificultades actuales. Para superar estos desafíos, es esencial establecer un diálogo efectivo entre las autoridades gubernamentales y las empresas privadas.

Este diálogo debe conducir a la creación de regulaciones adecuadas y a la implementación de programas educativos que no solo aborden las complejidades técnicas de la *lex* criptográfica y la tecnología *Blockchain*, sino que también consideren los aspectos éticos y sociales.

V. CONCLUSIONES

En este estudio, se evaluó la viabilidad de implementar la *Lex* Criptográfica como una solución innovadora para combatir la desinformación digital en Iberoamérica, un fenómeno que ha erosionado la integridad de los procesos democráticos y la confianza ciudadana.

Para ello, se emplearon dos metodologías clave: un análisis cualitativo exhaustivo de fuentes primarias, que reveló el impacto perjudicial de la desinformación en procesos electorales y confianza ciudadana en países de Iberoamérica, y una evaluación técnica de la tecnología *Blockchain* para implementar la *Lex* Criptográfica, demostrando su capacidad para asegurar la autenticidad de datos de manera descentralizada y segura.

Los hallazgos destacaron la necesidad de abordar desafíos éticos y regulatorios, especialmente en relación con la protección de datos personales y la prevención del uso indebido de la tecnología para el control social o manipulación electoral. Aunque la tecnología *Blockchain* puede garantizar la autenticidad de la información, se subrayó la importancia de establecer regulaciones claras para evitar su uso indebido.

Se identificó como un desafío significativo la aceptación de la *Lex* Criptográfica por parte de los Estados, ya que, a pesar de su capacidad para combatir la desinformación, también plantea preocupaciones sobre la recopilación no autorizada de datos de usuarios.

Además, se presenta como necesidad de establecer salvaguardas legales para proteger la privacidad de los ciudadanos y minimizar el riesgo de vigilancia masiva. La integración armoniosa entre las *Blockchain* públicas y la confianza gubernamental se destacó como crucial para el éxito de iniciativas como la Lex Criptográfica, subrayando la importancia de encontrar formas de complementar estas tecnologías con las estructuras gubernamentales existentes. Este estudio resalta la importancia de abordar estos desafíos de manera colaborativa y responsable para construir una infraestructura digital confiable y segura en la región.

BIBLIOGRAFÍA

- Agnikhotram, S., & Kouroutakis, A. (2019). Doctrinal challenges for the legality of smart contracts: Lex cryptography or new, smart way to contract. *Journal of High Technology Law*, 19 (2), 300-328. <https://heinonline.org/HOL/P?h=hein.journals/jhtl19&i=300>
- Aïmeur, E., Amri, S., & Brassard, G. (2023). Fake news, disinformation and misinformation in social media: a review. *Social Network Analysis and Mining*, 13 (1). <https://doi-org.basesbiblioteca.uexternado.edu.co/10.1007/s13278-023-01028-5>
- Article 19. (9 de julio de 2020). *Coronavirus, opacidad, violencia, impunidad y desinformación*. https://articulo19.org/wp-content/uploads/2020/07/Book-A19_InformeCovid_2020-V03.pdf
- Badillo, Á. (2019). *La sociedad de la desinformación: propaganda, «fake news» y la nueva geopolítica de la información*. Real Instituto Elcano. <https://media.realinstitutoelcano.org/wp-content/uploads/2021/10/dt8-2019-badillo-sociedad-de-desinformacion-propaganda-fake-news-y-nueva-geopolitica-de-informacion.pdf>
- Barroilhet Díez, A. (2019). Criptomonedas, economía y derecho. *Revista Chilena de derecho y tecnología*, 8(1), 29-67. <http://dx.doi.org/10.5354/0719-2584.2019.51584>
- Becerra, M. (2014). Medios de comunicación: América Latina a contramano. *Nueva Sociedad*, (249). <https://nuso.org/articulo/medios-de-comunicacion-america-latina-a-contramano/>
- Becker, K. (2022). Blockchain Matters—Lex Cryptographia and the Displacement of Legal Symbolics and Imaginaries. *Law Critique*, 33, 113-130. <https://doi.org/10.1007/s10978-021-09317-8>
- Cardoso (2022). Cryptography and Law: The Case of Brazil. *Digital Law Journal*, 3, 8-19. <https://doi.org/10.38044/2686-9136-2022-3-3-8-19>
- Cardoso, O. (2022). Cryptography and law: The case of Brazil. *Digital Law Journal*, (3), 8-19. <https://doi.org/10.38044/2686-9136-2022-3-3-8-19>

- Corona-Rodríguez, José Manuel. (2021). La importancia de la Alfabetización Mediática Informativa en el contexto pandémico: propuesta de actualización y nuevas preguntas. *Diálogos sobre educación. Temas actuales en investigación educativa*, 12(22), 00020. Epub 06 de diciembre de 2021. <https://doi.org/10.32870/dse.v0i22.979>
- Cotino Hueso, L. (2022). Quién, cómo y qué regular (o no regular) frente a la desinformación. *Teoría y realidad constitucional*, (49), 199-238. <https://dialnet.unirioja.es/servlet/articulo?codigo=8450040>
- Del Águila, A. (2023). *Las raíces de la polarización en las Américas: Los casos de Estados Unidos, Brasil y Perú*. IDEA Internacional. <https://doi.org/10.31752/idea.2023.66>.
- Diago Diago, M. P. (2021). Ciberactivismo, «Lex» informática, «blockchain» y oráculos: desafíos en la era digital. En, J. J. Castelló Pastor, *Desafíos jurídicos ante la integración digital: aspectos europeos e internacionales* (pp. 443-465). <https://www.millenniumdipr.com/archivos/1624954554.pdf>
- Dimitropoulos, G. (2020). *The law of blockchain*. *Washington Law Review*, 95(3), 1117-1192. <https://heinonline.org/HOL/P?h=hein.journals/washlr95&i=1115>
- Ebrahim, T. Y. (2020). *National cybersecurity innovation*. *West Virginia Law Review*, 123(2), 483-546. <https://heinonline.org/HOL/P?h=hein.journals/wvb123&i=503>
- García-Marín, D. & Merino-Ortego, M. (2022). Desinformación anticientífica sobre la COVID-19 difundida en Twitter en Hispanoamérica. *Cuadernos. info*, (52), 24-46. <https://doi.org/10.7764/cdi.52.42795>
- González, J. I. & Cardona-Restrepo, P. (2023). La posverdad y las redes sociales como desafíos al periodismo en la era digital. *Ánfora*, 30(55), 332-359. <https://doi.org/10.30854/anf.v30.n55.2023.977>
- Guallar, J., Codina, L., Freixa, P., & Pérez-Montoro, M. (2020). Desinformación, bulos, curación y verificación. Revisión de estudios en Iberoamérica 2017-2020. *Telos: Revista de Estudios Interdisciplinarios en Ciencias*

- Sociales*, 22(3), Venezuela. (Pp.595-613). <https://doi.org/10.36390/telos223.09>
- Gutiérrez-Coba, L., & Rodríguez-Pérez, C. (2023). Post-truth strategies and disinformation in the 2022 Colombian presidential elections [Estrategias de posverdad y desinformación en las elecciones presidenciales colombianas 2022]. *Revista de Comunicación*, 22(2), 225–242. <https://doi.org/10.26441/RC22.2-2023-3270>
- Guzmán Rincón, A., Barragán Moreno, S., Rodríguez-Canovas, B. et al. (2023). Social networks, disinformation and diplomacy: A dynamic model for a current problem. *Humanities and Social Sciences Communications*, 10(1), Article 505. <https://doi.org/10.1057/s41599-023-01998-z>
- Hernández Alfonso, E. A., & Paz Enrique, L. E. (2022). *Desarrollo, medios públicos y políticas latinoamericanas de comunicación*. *Question/Cuestión*, 3(72), E722. <https://doi.org/10.24215/16696581e722>
- Horder, J. (2021). Online free speech and the suppression of false political claims. *Journal of International and Comparative Law*, 8(1), 15-52. <https://heinonline.org/HOL/P?h=hein.journals/jintcl8&i=17>
- L. Malina et al. (2021). Post-Quantum Era Privacy Protection for Intelligent Infrastructures. *IEEE Access*, 9, 36038-36077. <https://doi.org/10.1109/ACCESS.2021.3062201>
- López López, P. C., Mila Maldonado, A., & Ribeiro, V. (2023). La desinformación en las democracias de América Latina y de la península ibérica: De las redes sociales a la inteligencia artificial (2015-2022). *Uru: Revista De Comunicación y Cultura*, (8), 69–89. <https://doi.org/10.32719/26312514.2023.8.5>
- López Rodríguez, A. (2021). Ley aplicable a los smart contracts y Lex Cryptographia. *Cuadernos de Derecho Transnacional*, 13(1), 441-459. DOI: <https://doi.org/10.20318/cdt.2021.5966>
- M. Raikwar., D. Gligoroski., & K. Kralevska. (2019). SoK of used cryptography in blockchain. *IEEE Access*, 7, 148550-148575, <https://doi.org/10.1109/ACCESS.2019.2946983>

- Manfredi, J., Gómez-Iniesta, P., & Amado, A. (2022). Desinformación de Estado: emociones al servicio de la causa. *Communication & Society*, 35(2), 205-221. <https://revistas.unav.edu/index.php/communication-and-society/article/download/42467/36054/>
- Pérez-Díaz, P.L. (2022). La cultura de la verificación periodística frente a la desinformación digital y sus efectos polarizadores. En, Arroyas Langa, E.; Pérez-Díaz, P.L.; Pérez-Escolar, Marta (eds.), *El debate público en la red: polarización, consenso y discursos del odio*. Salamanca: Comunicación Social Ediciones y Publicaciones. <https://doi.org/10.52495/c4.emcs.10.p96>
- Reporteros sin Fronteras. (2022). *Balance 2022 de periodistas encarcelados, asesinados, secuestrados y desaparecidos en el mundo*. <https://www.rsf-es.org/wp-content/uploads/2022/12/Balance-2022.pdf>
- Rodríguez, A. (2021). Applicable law to smart contracts and lex cryptographia. *Cuadernos de Derecho Transnacional*, 13(1), 441-459. <https://doi.org/10.20318/cdt.2021.5966>
- Sulkowski, A.J. (2019). Blockchain, Business supply chains, Sustainability and Law: the future of Governance, legal framework and lawyers? *Delaware Journal of Corporate Law*, 43, 305-345. <https://www.djcl.org/wp-content/uploads/2019/08/43.2.A3.pdf>
- Ungureanu, C. (2020). The ubiquity of law in cyberspace. *Analele Stiintifice Ale Universitatii Alexandru Ioan Cuza Din Iasi Stiinte Juridice*, (66), 5-10. <https://heinonline.org/HOL/P?h=hein.journals/anuaiclaw66&i=694>
- Valencia-Arias, A., Echeverri Gutiérrez, C. A., Acosta Agudelo, L. C., Echeverri Gutiérrez, M. S., & Rodríguez Valencia, C. A. (2023). Tendencias investigativas en facturación electrónica a nivel internacional entre 1979 y 2022. *Revista Virtual Universidad Católica del Norte*, (68), 217-254. <https://www.doi.org/10.35575/rvucln.n68a10>
- Isch, G. (2023). Crisis de imagen y sanitaria: la tormenta perfecta en el ecuador del covid-19. *Uru: Revista De Comunicación Y Cultura*, (7), 103-117. <https://doi.org/10.32719/26312514.2023.7.6>