



Tipografía de uso exclusivo como herramienta de autenticación documental en tiempos de inteligencia artificial

Flor María Torres Guzmán¹

Enlace ORCID: <https://orcid.org/0000-0002-3085-7326>

Víctor Alejandro Franco Ortiz²

Enlace ORCID: <https://orcid.org/0009-0003-4917-7704>

Fernando Luna Salas³

Enlace ORCID: <https://orcid.org/0000-0003-4574-6335>

Fecha de Recepción: 12 de agosto, 2025

Fecha de Aprobación: 19 de octubre, 2025

Fecha de Publicación: 19 de noviembre, 2025

Resumen:

La inteligencia artificial, es una herramienta que durante décadas se mantuvo con una concepción subjetiva de la ciencia ficción, y ha experimentado un aumento significativo en su utilidad práctica para el público en general desde el inicio de la década de 2020. Estas herramientas, que tienen una variedad de usos debido a su capacidad de aprendizaje, autonomía y resolución de situaciones complejas, se han puesto al servicio de los ciberdelinquentes, todo ello ante una mirada institucional sin regulación activa por parte de los Estados latinoamericanos. La falsificación de documentos es uno de los delitos más frecuentes que involucran a la IA como herramienta para llevarse a cabo, no solo por la facilidad que tienen estas herramientas para replicar documentos o imágenes en la actualidad, sino también por el acceso no regulado que tienen los delinquentes a ellas. El derecho, como ciencia que regula la sociedad, debe estar en constante evolución. Sin embargo, ante un desarrollo sin límite como el que tiene la inteligencia artificial, desde la academia se debe presentar una solución posible para prevenir la falsificación de documentos virtuales.

Palabras clave: Blockchain, Ciberdelincuencia, Diseño Legal, Falsificación, Inteligencia Artificial, Tipografía.

¹Abogada. Doctora en Derecho Público. Especialista en Derecho Constitucional y en Derecho Penal. Magíster en Gestión de Ciencia, Tecnología e Innovación. Coordinadora académica de la Facultad de Derecho - Universidad Antonio Nariño. fntg94@gmail.com

²Abogado egresado de la Universidad Antonio Nariño. Email: vfranco24@uan.edu.co

³Profesor investigador del Dpto. de Derecho Procesal y Probatorio de la Universidad de Cartagena, Magíster en Derecho de la Universidad de Cartagena y Especialista en Derecho Procesal de la Universidad Libre. Doctorando en Derecho, Ciencias Políticas y Criminológicas de la Universidad de Valencia-España. Investigador Junior por Colciencias. Director del grupo y del Semillero de investigación Ciencia y Proceso de la Universidad de Cartagena. Miembro del Instituto Colombiano de Derecho Procesal (ICDP). Correo electrónico: flunas@unicartagena.edu.co

Exclusive use typography as a document authentication tool in times of artificial intelligence

Abstract:

Artificial intelligence, a tool that for decades remained a subjective conception of science fiction, has experienced a significant increase in its practical utility for the general public since the beginning of the 2020s. These tools, which have a variety of uses due to their capacity for learning, autonomy, and resolution of complex situations, have been put at the service of cybercriminals, all under an institutional gaze without active regulation by Latin American States. Document forgery is one of the most frequent crimes that involve AI as a tool to be carried out, not only because of the ease with which these tools replicate documents or images today, but also because of the unregulated access that criminals have to them. Law, as a science that regulates society, must be in constant evolution. However, faced with limitless development such as that of artificial intelligence, academia must present a possible solution to prevent the falsification of virtual documents.

Keywords: Blockchain, Cybercrime, Legal Design, Counterfeiting, Artificial Intelligence, Typography.

Tipografia de uso exclusivo como ferramenta de autenticação documental em tempos de inteligência artificial

Resumo:

A inteligência artificial é uma ferramenta que, durante décadas, manteve uma concepção subjetiva da ficção científica e tem experimentado um aumento significativo em sua utilidade prática para o público em geral desde o início da década de 2020. Essas ferramentas, que têm uma variedade de usos devido à sua capacidade de aprendizagem, autonomia e resolução de situações complexas, foram colocadas a serviço dos cibercriminosos, tudo isso diante de um olhar institucional sem regulamentação ativa por parte dos Estados latino-americanos. A falsificação de documentos é um dos crimes mais frequentes que envolvem a IA como ferramenta para sua realização, não apenas pela facilidade que essas ferramentas têm para replicar documentos ou imagens atualmente, mas também pelo acesso não regulamentado que os criminosos têm a elas. O direito, como ciência que regula a sociedade, deve estar em constante evolução. No entanto, diante de um desenvolvimento ilimitado como o da inteligência artificial, a academia deve apresentar uma solução possível para prevenir a falsificação de documentos virtuais.

Palavras-chave: Blockchain, Cibercrime, Design Legal, Falsificação, Inteligência Artificial, Tipografia.



1. INTRODUCCION

Mercadotecnia social en u La inteligencia artificial durante la presente década ha tomado un papel protagónico en el desarrollo tecnológico global, abandonando su papel anterior como una teoría de la ciencia ficción. Por consiguiente, el Derecho, como ciencia que evoluciona con los cambios sociales del mundo, también debe encontrar las formas de regular una herramienta con tantas implicaciones y potencialidades.

Las relaciones entre inteligencia artificial y juridicidad plantean grandes y variados cuestionamientos, los cuales se pueden resumir en dos macrogrupos. En primer lugar, el problema del uso de las herramientas de inteligencia artificial en la práctica jurídica: “la inteligencia artificial en la práctica del derecho”; y, en segundo lugar, el tema de la garantía de unos principios jurídicos básicos —y particularmente de los derechos fundamentales y humanos— en el marco del desarrollo y de la utilización de los sistemas de inteligencia artificial: “el derecho en la práctica de la inteligencia artificial”. Dicho de otra manera, hoy en día las relaciones entre derecho e inteligencia artificial se desarrollan en una doble vía o tensión, dado que, por una parte, existe la necesidad para la juridicidad de adaptarse a los cambios de la realidad científica, social y global, pero a la vez existe la necesidad de que el derecho y su práctica no desconozcan los valores, principios y garantías alcanzadas. (Luna, Perona y Carrillo, 2023, p. 236)

Desde que las herramientas de inteligencia artificial empezaron a demostrar una funcionalidad real en el ámbito comercial desde principios de la década de 2020, estas, aunque útiles en múltiples ámbitos de la vida cotidiana y profesional, también han tomado fuerza dentro de los esquemas delincuenciales que afectan al mundo, generando contenido o documentos falsificados que dificultan la autenticación.

El desproporcionado aumento en las capacidades de la inteligencia artificial para crear y difundir elementos gráficos que distan de la realidad ha permitido que los grupos delincuenciales utilicen estos como medios para cometer innumerables delitos.

La incapacidad técnica de los gobiernos para asegurar y controlar el uso de estas herramientas de inteligencia artificial, y para evitar que sean utilizadas

para aumentar el accionar delincencial del crimen organizado, es una problemática que deberá ser abordada desde la academia.

Los documentos han sido de los elementos más manipulados por las herramientas de inteligencia artificial, incluso para los expertos peritos es una tarea compleja definir la autenticidad de estos. Es por lo cual que la tipografía de uso exclusivo ha sido propuesta como una posible aproximación para la autenticación documental dentro del proceso judicial.

En este sentido, dentro del proceso judicial, la prueba documental ha desempeñado un papel fundamental. No solo por su fuerza probatoria al exponer hechos y eventos relevantes, sino también por su contribución a la eficiencia procesal al respaldar los argumentos de las partes mediante las diversas interpretaciones que pueden darse a los documentos presentados. (Flórez, 2014)

Aunque se han desarrollado protocolos aceptados a nivel global, diseñados para garantizar la autenticidad y las diferentes cadenas de custodia de las pruebas digitales, estos ya no presentan la robustez necesaria para garantizar la confiabilidad que se requiere para afirmar la autenticidad de un documento legalmente válido.

Por lo tanto, ante la incapacidad estructural de lo establecido internacionalmente para manejar esta materia, se ha formulado la pregunta de cuál podría ser la solución a corto plazo para controlar la proliferación de documentos falsificados mediante la tecnología, los cuales son comparables a los verídicos.

Es entonces cuando entra en acción el diseño legal, que, mediante una solución adaptada al usuario, implementa las fuentes tipográficas de uso exclusivo como forma de asegurar la autenticidad de los documentos emitidos por las entidades emisoras. Esto se entiende en el contexto de que, con las medidas de ciberseguridad, la emisión de estos documentos será exclusiva de las entidades dueñas de la fuente tipográfica.

Por consiguiente, mediante el presente análisis académico-jurídico, se ha formulado la siguiente pregunta de investigación: ¿La utilización de fuentes tipográficas de uso exclusivo de una entidad será una solución a corto plazo para la problemática que

genera la inteligencia artificial frente a la falsificación de documentos?, considerando que la IA es una tecnología emergente con una alta variabilidad, lo que requiere una solución igualmente variable para afrontar una realidad a largo plazo.

Teniendo en cuenta lo planteado, con la finalidad de brindar solución a esta pregunta de investigación, se ha formulado el objetivo general de identificar si la utilización de fuentes tipográficas de uso exclusivo es una solución a corto plazo para la problemática de falsificación causada por el uso indebido de la inteligencia artificial. Esto implica: I. Revisar la situación frente a la inteligencia artificial a nivel global como regional y los efectos negativos del uso de la IA en cuanto a la falsificación de documentos; II. Determinar el desarrollo jurídico y normativo frente a la tipografía forense en Colombia con el fin de obtener los elementos base que se usan en los peritajes; para con esto, III. Evaluar si el uso de elementos de ciberseguridad y blockchain será apropiado para garantizar la autenticidad de los documentos.

2. METODOLOGIA

Los procesos de reflexión están orientados a la interpretación—hermenéutica—la comprensión del diseño metodológico y la explicación de una realidad, en el área del saber investigada (López, Alarcón y Luna, 2025, p. 87). Es por ello que para abordar la problemática de la falsificación documental, se propone un enfoque basado en el diseño legal. Esta metodología de investigación se centra en desarrollar soluciones que sean tanto prácticas como sostenibles en el tiempo, alineadas con las necesidades y expectativas de los usuarios. El objetivo es crear mecanismos que permitan evolucionar al derecho para adaptarse de manera óptima a las demandas sociales y la tecnología emergente.

La primera etapa de la investigación implica una profunda comprensión del problema en cuestión. Se identifican los desafíos asociados con la falsificación documental en la era de la inteligencia artificial y se analizan críticamente las deficiencias en los métodos de autenticación existentes. Además, se reconoce la creciente desconfianza en la capacidad de los gobiernos para regular eficazmente la tecnología emergente de la IA.

A través de una revisión exhaustiva de la información disponible sobre la falsificación documental, la tecnología Blockchain, la tipografía exclusiva y el diseño legal, además del análisis de casos relevantes de falsificación documental y sus implicaciones jurídicas y sociales, se busca obtener una comprensión más profunda del alcance del problema y explorar posibles soluciones.

Con la información obtenida, se idean y prototipan una serie de soluciones potenciales, desarrollando mecanismos innovadores, como la posible implementación de la tipografía de uso exclusivo con mecanismos de ciberseguridad y Blockchain, los cuales podrían ofrecer una respuesta efectiva a la falsificación documental en la era digital.

Estas soluciones serán sometidas a un proceso interactivo de co-creación y evaluación, donde se colabora estrechamente con usuarios y stakeholders para mejorar los prototipos. La retroalimentación recibida permitirá ajustar y mejorar continuamente las soluciones en aras de garantizar su efectividad y aceptabilidad.

Una vez desarrolladas, se implementará el piloto de la solución en entornos controlados o simulados para evaluar su viabilidad y efectividad en la práctica. Esto permite un monitoreo cercano en cuanto a la implementación del piloto y se identifican nuevos desafíos u oportunidades de mejora.

Finalmente, se evalúa el impacto de la solución y se desarrollará una estrategia para escalarlas a un nivel más amplio, garantizando su sostenibilidad a mediano plazo. Se deberán difundir los hallazgos encontrados, con el objetivo de promover la adopción de soluciones basadas en este enfoque en la lucha constante que ofrece la falsificación documental con base en la IA generativa.

3. RESULTADOS

La inteligencia artificial y su utilización en la falsificación de documentos

La justicia digital avanza a pasos agigantados, como consecuencia de la necesidad social y de las importantes actualizaciones que exige la administración de justicia para estar en consonancia con los modernos avances tecnológicos (Correa, Luna y Pacheco, 2022, p. 302). En ese orden, la inteligencia artificial se presenta como un campo de la informática que tiene un enfoque en desarrollar sistemas y programas capaces de realizar



tareas que en términos simples requieren de la inteligencia humana, tales como el aprendizaje, la adaptabilidad, la toma de decisiones y la resolución de problemas. Los sistemas de este grupo utilizan algoritmos y modelos matemáticos para procesar gran cantidad de datos, identificar patrones y realizar inferencias para automatizar procesos, aumentar la eficiencia y precisión en la toma de decisiones, además de ofrecer soluciones en temas complejos en variadas áreas.

La regulación de la inteligencia artificial y el debate ético que suscita, así como el inicio de un uso masificado de una herramienta con tantas posibilidades, se ha realizado durante la última década, únicamente con la consideración de ser una herramienta sectorizada que se definía desde el punto de vista subjetivo de la utilización práctica.

Las herramientas que basan su funcionamiento en la inteligencia artificial no habían tenido un punto de análisis protagonista dentro de la academia más allá de una aproximación a un futuro uso poco certero. Sin embargo, con la llegada de la década de 2020, ha surgido la oportunidad de que las diferentes variables sean consideradas dentro del espectro de la prevención del delito.

Dentro del avance que ha presentado la IA en cuanto a la falsificación de documentos, se encuentra que esta aumenta su sofisticación y su grado de realismo. Las herramientas generadoras de texto, imágenes o videos que usan la IA, al momento de escribir esta investigación, pueden producir documentos falsificados cada vez más difíciles de distinguir de los originales, incluyendo una capacidad elevada para crear firmas y sellos, que comúnmente se utilizan como medida de protección frente a las falsificaciones.

El segundo punto de avance que presenta la IA frente a este delito es que la facilidad de acceso a las herramientas con estas capacidades va en aumento, no solo en el acceso a la tecnología sino también en la facilidad de uso.

El tercer punto de avance negativo que presenta la IA es la difícil detección de los documentos falsificados. Aunque este se relaciona con el primer avance, lo que se presenta es que, ante el análisis de expertos peritos, se ha podido desarrollar una aceptación involuntaria de falsificaciones documentales, lo cual

ya supone una preocupación importante dentro del análisis.

El cuarto punto de avance negativo y preocupante que presenta la IA es el aumento de actividades delictivas, frente a cuatro delitos; como lo son el fraude financiero, la falsificación de identidad, el lavado de activos y la falsificación de documentos legales, todo esto facilitado por las herramientas que usan como base la inteligencia artificial.

Estos cuatro puntos de avance negativo generan un efecto colateral general definido como la pérdida de la confianza del público en general en los sistemas y procesos que, en el momento actual, revisan la autenticidad de la documentación en diferentes ámbitos, tales como las transacciones financieras, el ámbito contractual, y los procesos judiciales en materia probatoria.

Antecedentes de países con legislación respecto a la inteligencia artificial

La pieza más completa de legislación que proporciona una primera aproximación a las diferentes variables regulables que tiene la inteligencia artificial, la ha emitido el Parlamento Europeo desde abril de 2021. La Comisión Europea propuso este primer borrador regulatorio en la Unión Europea, donde se reconoce los diferentes usos que tiene la tecnología en cuestión y cómo se clasifican según el riesgo que representan para el usuario y la sociedad en general.

Dentro de esta nueva normativa, se ha establecido que los proveedores y usuarios tendrán una serie de obligaciones según el tipo de riesgo que conlleva el uso de esta tecnología. Se han definido dos categorías como (Riesgo inaceptable) y (Alto riesgo).

El riesgo inaceptable tiene una caracterización específica en la cual se consideran como una amenaza potencial para las personas y los órdenes sociales, por lo cual serán censuradas y prohibidas. Se deberán incluir dentro de esta categoría a las IA que respondan a una función de manipulación cognitiva conductual de las personas o grupos vulnerables; sistemas que funcionen como clasificador social, ofreciendo una clasificación de las personas por su comportamiento, estatus socioeconómico u otras características personales; también serán los que incluyan sistemas de

identificación biométrica o de categorización de personas; y por último los que desarrollen sistemas de identificación biométrica remota y en tiempo real.

Se deja un aparte dentro de esta normativa que exime de la prohibición a los sistemas de identificación biométrica cuando sean utilizados exclusivamente por los servicios de seguridad estatal, lo cual estará basado en una aprobación del juez, en caso de búsquedas selectivas en bases de datos.

Dentro de la categoría de alto riesgo estarán incluidos los sistemas de IA que afecten la seguridad o los derechos fundamentales de los individuos. La UE ha dividido esta categoría en otras dos, que incluirá a los sistemas que ya se encuentran sujetos a la legislación de seguridad de productos y a los sistemas de IA que son de un área específica.

Para la región latinoamericana, ya existen ciertas leyes en términos de protección de datos que presentan un avance frente a las nuevas tecnologías y los desafíos que estas plantean en relación con los derechos fundamentales de los individuos. Sin embargo, hasta la fecha, en la región no se presenta una legislación inicial que incluya a la inteligencia artificial como objeto de regulación.

Se presenta que la gran mayoría de legislación de este tema en la región cuenta con el elemento diferenciador, en dónde además de poseer una normativa clara, poseen una autoridad administrativa que permite el cumplimiento de esta; sólo dos de los países que poseen esta legislación no cuentan con esta autoridad, lo cual indicaría una operatividad regulatoria inexistente dentro de esta jurisdicción.

Dentro de esta tabla de construcción propia se ha desarrollado una breve descripción de los países de la región que cuentan con la normativa descrita anteriormente:

País	Normativa	Autoridad administrativa como mecanismo de protección de derechos
Argentina	Ley nacional N° 25.326 de 2000 y Decreto Ejecutivo Presidencial N° 1558 de 2001.	Dirección Nacional de Protección de Datos Personales y Agencia de Acceso a la Información Pública.
Uruguay	Ley N° 18.331 de 2008 y Decreto Ejecutivo N° 414 de 2009.	Unidad Reguladora y de Control de Datos Personales.
México	Ley federal de protección de datos personales en posesión de los particulares del 5 de julio de 2010.	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos.
Perú	Ley N° 29.733 de 2011.	Dirección General de Protección de Datos Personales.
Costa Rica	Ley N° 8.969 de 2011.	Agencia para la Protección de Datos Personales.
Colombia	Ley N° 1.581 de 2012 y Decreto Ejecutivo N° 1.377 de 2013.	Superintendencia de Industria y Comercio.
Brasil	Ley Federal N° 13.709 de 2018.	Autoridade Nacional de Proteção de Dados.
Panamá	Ley N° 81 de 2019.	Autoridad Nacional de Transparencia y Acceso a la Información.
Chile	Ley Marco de Ciberseguridad e Infraestructura Crítica.	Agencia Nacional de Ciberseguridad de Chile
República Dominicana	Ley N° 172 de 2013	No tiene autoridad administrativa

Tabla 1 : Normativa protección de datos personales en Latinoamérica.



En este contexto, so pena de la existencia de la regulación normativa que sigue las corrientes evolutivas del derecho actuales, en la región latinoamericana solo Chile ha publicado en el mes de abril de 2024 la Ley Marco de Ciberseguridad e Infraestructura Crítica, en donde se establecen las disposiciones generales frente a las estructuras estatales informáticas, los métodos de protección frente a la creciente amenaza cibernética, así como el establecimiento de la autoridad administrativa llamada Agencia Nacional de Ciberseguridad de Chile.

Esta normativa ha utilizado positivamente las normas de protección de datos de la región latinoamericana como guía de los principios que debería incorporar en aras de la protección ética de la ciberseguridad. Lo cual muestra que algunos gobiernos ya están tomando medidas preventivas frente a la problemática de la IA desregulada.

Los efectos del uso de la IA en cuanto a la falsificación de documentos

Se entiende que la Grafología Forense es el estudio de manuscritos, con el fin de establecer su veracidad o falsedad e identificar a su autor o autores. A través de la Grafología Forense se pueden aplicar diferentes métodos establecidos para obtener resultados positivos frente al esclarecimiento de delitos. (Sáenz y Hernández, 2019)

En teoría, el análisis y el estudio de elementos como las firmas llevado a cabo por un perito puede proporcionar a los órganos investigativos, las suficientes bases técnicas para establecer cuándo se trate de posibles falsificaciones.

Dentro de estos análisis que se les hace a los documentos en términos generales se revisan, las inclinaciones que tienen las líneas de la escritura, dimensiones, ritmo y rapidez, y el flujo del trazo, también la presión y el espaciado entre líneas se realiza para revelar aspectos de la escritura de la persona.

Estas técnicas han sido de gran utilidad para los organismos investigativos como herramienta probatoria dentro de los procesos judiciales durante las últimas décadas, pero con la entrada operativa de la IA como herramienta alternativa para la falsificación, el desafío de probar la autenticidad de un documento aumenta.

Las herramientas como Only Fakeⁱ, una herramienta de inteligencia artificial que fue encontrada dentro de la Dark Web. Esta herramienta ofrecía servicios de falsificación de documentos a precios bajos, los cuales estaban protegidos por el uso de criptomonedas complejas de rastrear, incluso en la Dark Web. Se afirmó teóricamente de tener una capacidad generadora de miles de documentos diarios, lo que extendió la preocupación en 26 países donde se alcanzó a verificar su funcionamiento, porque logró replicar efectivamente documentos de identidad y pasaportes de estas nacionalidades.

La problemática que suscitó esta herramienta encontrada en la Dark Web y con medios tan sofisticados de encubrimiento de pagos, revivió la necesidad de discutir cómo asegurar la autenticidad de los documentos de identidad y otros temas relacionados con la tecnología masificada.

Una de las propuestas es el uso de herramientas biométricas como mecanismo de autenticación tanto de la identidad como de los documentos, una herramienta que presentó resultados conformes a la necesidad para el año 2023, en el momento de esta investigación, las capacidades de la IA han aumentado incluso hasta el punto de llegar a falsificar elementos biométricos de identificación.

Este aumento desmedido en los avances de la tecnología de IA, están causando un paulatino incremento en la desconfianza en el derecho y la normativa para luchar en contra de la ciberdelincuencia, que día tras día encuentran más herramientas para defraudar la buena fe de las personas.

Desarrollo jurídico y normativo de la tipografía forense en Colombia

“La tipografía ha sido uno de los sistemas más antiguos que se usaba para la elaboración de papel moneda, este sistema involucra una impresión directa e indirecta. Que implicaba el uso de moldes en relieve con tinta en ellos. que se conocen comúnmente con el nombre de tipos, estos se colocaban sobre el papel, dejando una impresión cuando entraban en contacto con él”. (Sáenz y Hernández, 2019)

Todas las características que dominan a estos tipos, solo son apreciables mediante los lentes del microscopio; las características resaltan apreciando la

marca que dejan los moldes, donde el diseño de cada uno tiene un patrón de diseño exclusivo, con diferentes puntos, terminaciones o particularidades, que dificultaron las imitaciones o que mediante un análisis especializado garantiza la autenticidad de los mismos documentos. (Sáenz y Hernández, 2019)

Inclusive con la llegada de los computadores personales y el uso de editores de texto en la década de 1990, las falsificaciones de documentos evolucionaron para usar la tecnología como herramienta; con esto en mente, los peritos llegaron a usar los mismos métodos de confrontación documental para así encontrar las imperceptibles características de seguridad que se diseñaban para asegurar la autenticidad. (Cano, 2010)

Aun con el ejercicio de confrontación entre tipografías auténticas y falsificadas, el procedimiento realizado por el perito se basa en un análisis riguroso de las descripciones de los cotejos anteriores en cuanto a la originalidad, reparando en las diferencias que surgían bajo los preceptos científicos, incluso tomando en cuenta la máquina de impresión que se usaba como un elemento de verificación de la autenticidad.

El uso de Blockchain, Mecanismos de Ciberseguridad y Tipografía de uso exclusivo en la lucha contra la falsificación documental

El blockchain, en términos generales, es una cadena de bloques virtuales que utiliza una estructura de datos. La información se agrupa en bloques, y cada uno de ellos contiene metainformación relacionada con el bloque anterior en una línea temporal, lo que permite un seguimiento seguro. De esta manera, con la ayuda de la criptografía, la información contenida en un bloque no puede ser editada o alterada sin modificar los bloques que la preceden. (Pérez y Pabón, 2021)

A partir de esta funcionalidad, se ha desarrollado la capacidad de permitir que la información de datos públicos relacionados contenga un histórico irrefutable, en forma de registro contable distribuido que inicialmente se utilizó para garantizar la seguridad de las criptomonedas.

Cuando se alcanza un consenso sobre la integridad de los datos entre los participantes de las redes, no se necesita una entidad centralizada de confianza para garantizar esta información. Por lo cual, su

confianza en general se basa en la fortaleza de la red emisora, aunque se prevé que con el aumento de la capacidad de los sistemas de IA, pueda tener una operatividad a un rango de tiempo medio.

En términos de seguridad y confianza, la tecnología blockchain ha enfocado su capacidad en proporcionar esto a los usuarios, debido a la alta capacidad de transparencia, como su imposibilidad de modificar los datos después de haber sido registrados en las cadenas de bloque. (Padilla, 2020)

La transparencia proviene de que las transacciones y operaciones realizadas dentro de la red son públicas y visibles para todos los usuarios. Esto implica que la accesibilidad y la verificación de los datos son realizables por cualquier persona. Además, esta tecnología es inmutable, ya que una vez que los datos fueron registrados dentro de la cadena, no pueden cambiarse o eliminarse, lo que garantiza que la información sea confiable y precisa y no haya sido manipulada por terceros.

En su funcionalidad estándar, esta tecnología ha protegido la privacidad y la integridad de los datos de los usuarios, fortaleciendo el sistema de prevención de fraudes y robos de información.

En segundo lugar, la tecnología blockchain, para el momento de esta investigación, se ha establecido como un activo valioso en la prevención de las falsificaciones, tanto en la protección de derechos de autor como en patentes de medicamentos, garantizando la autenticidad a los consumidores finales mediante el registro de información en bloques. (Padilla, 2020)

Una de las cuestiones más importantes a definir en los mecanismos de protección basados en blockchain es el tipo de gobernanza que se necesitará en el futuro para la toma de decisiones y la resolución de controversias que puedan surgir dentro de la red.

Esta gobernanza debe basarse bajo los principios de justicia, transparencia y la democracia, en aras de crear una comunidad más justa y pluralista dentro de la misma.

Dentro de las preocupaciones actuales frente a esta tecnología, que se encuentra también en una evolución constante, está la cuestión ética que garantice un uso adecuado de la misma frente a los



usos que se le den a futuro, especialmente con la posible creación de monopolios con mayor capacidad de cómputo y operatividad, los cuales podrían ejercer un control que genere posiciones abusivas en las transacciones y la creación de bloques.

Ataques Sybil: Una amenaza a considerar

Después de revisar toda la información disponible sobre el tema de los blockchains, se ha observado que el diseño debe considerar una amenaza cibernética, en la cual la IA generadora podría utilizar este tipo de ataque en contra del producto.

Las amenazas cibernéticas siempre estarán en constante evolución. Entre ellas, se destacan los ataques Sybil, los cuales son una forma de ataque en redes descentralizadas donde un usuario activo crea múltiples identidades falsas o nodos en la red para ganar una posición dominante y manipular la percepción de la red. Estos nodos adicionales pueden utilizarse para propagar información falsificada, manipular registros o tomar control desproporcionado de la red. (Valencia, 2020)

Como estrategia de protección en contra de este tipo de ataques cibernéticos, se deben estudiar y desarrollar a corto plazo mecanismos altamente estrictos de identificación y acceso a los nodos de la red, basándose preferiblemente en un historial reputacional de la misma red.

Además, se recomienda que las redes blockchain que protegen cada una de las tipografías de uso exclusivo implementen algoritmos robustos como “proof of work” (PoW), “proof of stake” (PoS) o “proof of authority” (PoA), para crear una alta capacidad de resistencia frente a ataques con la IA.

Como tercera estrategia, se sugiere que todas las redes de blockchain que protegen el producto tipográfico establezcan una limitación de uso validado por otros participantes de la misma red, y mantengan un monitoreo constante del uso de la tipografía dentro de los documentos emitidos por las instituciones, con el fin de detectar anomalías o actividades sospechosas.

El Caso Cuatrecasas: Primera institución en tener tipografía de uso exclusivo

La firma de abogados española Cuatrecasas fue la primera institución legal en incorporar de manera

visionaria una nueva identidad visual que incluyó una tipografía exclusiva, diseñada para ser utilizada en todos los documentos emitidos por la firma con el objetivo de dificultar la falsificación documental. (Rodríguez, 2017)

Este caso presenta especial relevancia debido a que durante el año 2017, se dio a conocer el caso de corrupción conocido como CalibriGate (Rodríguez, 2017). Este caso reveló una serie de irregularidades en documentos que usaron la tipografía Calibri anterior al lanzamiento de la misma.

Antes de la década de 2020, la preocupante situación frente a la falsificación documental dentro de las instituciones ya se presentaba como un problema robusto y con pocas opciones de mitigación. Esta preocupación llevó a aumentar la seguridad documental ofrecida por la institución. La implementación de una tipografía exclusiva se destacaba como una medida eficaz, que impedía que personas fuera de la red pudieran generar documentos con la misma.

4. DISCUSION

Estamos frente a un camino sin retorno; nuestro modo de pensar y forma de vida ahora es parte, para bien o mal, de los avances tecnológicos. Rechazar lo desconocido no es solución, como tampoco aceptarla sin más; es necesario desarrollar un pensamiento tecnológico crítico, que se incorpore y se adapte al avance de la IA.

El desarrollo de este pensamiento tecnológico crítico implica reconocer que nuestra vida, en todas sus facetas, transcurre, en buena medida, mediada por la tecnología y que nos resultaría problemático prescindir de ella una vez la hemos incorporado. Implica, también, ser conscientes de lo expansivo que ha sido el estallido digital en todas las áreas, y que esto puede generar temor a catástrofes apocalípticas, pero este temor no impedirá que se acerquen cada vez más los sistemas inteligentes y las actividades humanas, las máquinas y las personas, la inteligencia natural y la artificial. (Botero, Gamboa y Valdivieso, 2024, p. 178)

Dentro de esta investigación se ha establecido la fundamentación en cuanto a la problemática que se presenta actualmente con la falsificación documental realizada a un grado de imperceptibilidad mediante

herramientas fundamentadas en IA, en donde se ha identificado la complejidad y el desafío de regular un área de una industria que cambia a pasos agigantados frente a mecanismos de evolución jurídica que no logran estar en el mismo nivel de evolución.

A partir de un análisis extensivo de los elementos descritos en la presente investigación, se ha brindado cumplimiento con el objetivo planteado; ya que se ha probado que la tipografía de uso exclusivo sería una solución a corto plazo en contra de la falsificación documental causada por la ciberdelincuencia y apoyada por herramientas de IA, todo basándose en las recomendaciones propuestas.

La GenIA o inteligencia artificial generativa representa uno de los más grandes peligros en la actualidad. Por lo tanto, con esta investigación también se insta a los gobiernos a fortalecer de manera apropiada sus marcos normativos frente a estas herramientas, que han sido ignoradas anteriormente.

Debido a que la tipografía de uso exclusivo con red de blockchain como producto del diseño legal requiere la participación de un grupo interdisciplinar que contribuya a la correcta disposición de los elementos que garanticen su eficacia, en donde se realiza este aporte a la academia para iniciar la discusión.

REFERENCIAS

- Botero, A., Gamboa, S., y Valdivieso, K. (2024). Reflexiones sobre la inteligencia artificial aplicada a la administración de justicia. *Revista Jurídica Mario Alario D'Filippo*, 16(33), 160–183. <https://doi.org/10.32997/2256-2796-vol.16-num.33-2024-4887>
- Cano Martínez. J. J. El peritaje informático y la evidencia digital en Colombia. Conceptos, retos y propuestas. Bogotá D.C. Colombia: Ediciones Uniandes. (2010).
- Calderón Ortega, M., Eslava Zapata, R., y Sánchez Castillo, V. (2024). Bioética y derecho: tendencias y líneas de investigación. *Revista Jurídica Mario Alario D'Filippo*, 16(33), 301–321. <https://doi.org/10.32997/2256-2796-vol.16-num.33-2024-4894>
- Carrillo de la Rosa, Y. (2024). La validez de las normas jurídicas en el ordenamiento jurídico colombiano. *Revista Jurídica Mario Alario D'Filippo*, 16(32), 131–155. <https://doi.org/10.32997/2256-2796-vol.16-num.32-2024-4761>
- Correa Fernández, M. de J., Luna Salas, F., y Pacheco Benjumea, M. P. (2022). Valor Probatorio del Documento Electrónico a la Luz de la Digitalización de la Justicia en Colombia. *Revista Jurídica Mario Alario D'Filippo*, 14(28), 302–324. <https://doi.org/10.32997/2256-2796-vol.14-num.28-2022-3976>
- Flórez. G. D. La Validez jurídica de los documentos electrónicos en Colombia a partir de su evolución legislativa y jurisprudencial. *Revista Verba Iuris*. (31) (2014). p 43-71.
- Forero. J y Rovira. J. La grafología forense como prueba pericial en el reconocimiento de la falsificación de firmas. Colombia. Universidad La Gran Colombia. Facultad de Derecho. (2014).
- López Oliva, J., Alarcón Peña, A., y Luna Salas, F. (2025). El proceso de investigación en el área del derecho: Análisis del diseño metodológico destinado al investigador de las ciencias jurídicas. *Revista Jurídica Mario Alario D'Filippo*, 17(35), 85–103. <https://doi.org/10.32997/2256-2796-vol.17-num.35-2025-5241>
- Luna Salas, F., Perona, R., & Carrillo de la Rosa, Y. (2023). Impacto y límites de la inteligencia artificial en la práctica jurídica. *Via Inveniendi Et Iudicandi*, 17(2). <https://doi.org/10.15332/19090528.8773>
- Melo. L. Régimen jurídico del blockchain: una prueba atípica. *Revista de Bioética y Derecho. Perspectivas Bioéticas*. (46) .(2019). p 101-116.
- Padilla Sánchez. J. A. Blockchain y contratos inteligentes: aproximación a sus problemáticas y retos jurídicos. *Revista de Derecho Privado*. (39). (2020). p 175 - 201.
- Pérez K., & Pabón A. (2021). Aspectos probatorios de la blockchain y el smart contract desde la perspectiva jurídica colombiana de la prueba



- electrónica. Recuperado de:
<https://hdl.handle.net/10901/20240>.
- Pepe. E. G. Diseño tipográfico e identidad. Bold (nº2). Facultad de Bellas Artes. Universidad Nacional de La Plata. Argentina. (2015). p 56 - 66.
- Peña Cuellar, D., Vidal Lasso, A., y Buritica Salazar, A. (2024). El metaverso: un análisis desde la perspectiva de los derechos humanos. Revista Jurídica Mario Alario D'Filippo, 16(33), 202–218. <https://doi.org/10.32997/2256-2796-vol.16-num.33-2024-4889>
- Parlamento Europeo. Ley de IA de la UE: primera normativa sobre inteligencia artificial. EuroParlamento.(2023)
<https://www.europarl.europa.eu/topics/es/article/20230601STO93804/ley-de-ia-de-la-ue-primer-normativa-sobre-inteligencia-artificial>
- Rodríguez. D. Cuatrecasas, pioneros en aumentar la seguridad de sus clientes con una tipografía exclusiva para sus documentos. gráfica. (2017) Recuperado de: <https://grafica.info/tipografia-cuatrecasas-seguridad-clientes/>
- Rodríguez. D. Tipografía forense: el caso CalibriGate, una guía de cómo NO se debe falsificar un documento. gráfica. (2017). Recuperado de: <https://grafica.info/tipografia-forense-calibrigate/>
- Sáenz. D y Hernández. O. Documentología y Grafología Forense Colombia. (1º edición). Colombia. Ediciones USTA. Universidad Santo Tomás.(2019).
- Sanabria. G y Rodríguez. P. Inteligencia artificial en los procesos documentales de los archivos sonoros. Investigación bibliotecológica. ISSN 2448-8321.(2023). Recuperado el 03 de abril de 2024 de la base de datos https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-358X2022000400073
- Torres Guzmán, F., Escobar Díaz, H., y Franco Ortiz, V. (2025). Eutanasia Psiquiátrica en Colombia: Aproximación al Protocolo de Verificación de la Voluntad Autónoma desde el “Legal Design” y la Sostenibilidad Procesal . Revista Jurídica Mario Alario D'Filippo, 16(34), 338–361. <https://doi.org/10.32997/2256-2796-vol.16-num.34-2024-5048>
- Valencia-Ramírez. J. Derecho, tecnología e innovación: blockchain y contratos inteligentes. RITI Journal, Vol. 8. 16 (Julio-Diciembre 2020).doi: <https://doi.org/10.36825/RITI.08.16.005>.
-