Federación Latinoamericana de Bancos – FELABAN

EL USO MALICIOSO DE LA INTELIGENCIA ARTIFICIAL (IA)

EN EL LAVADO DE DINERO

Criminalidad tecnológica y regulación proactiva

"En la era digital, el lavado de dinero ya no ocurre en la sombra, sino en redes, plataformas y canales que operan a la vista de todos. El verdadero reto es ver, entender y actuar".

Autor:
Kattia Narvaez Copeticon
Analista de Cumplimiento Normativo y Monitoreo
Unidad de Prevención y Cumplimiento
Banco Económico S.A.

Santa Cruz – Bolivia

Sobre la autora

Kattia Narvaez Copeticon es Licenciada en Ciencias Jurídicas egresada de la Universidad Autónoma Gabriel Rene Moreno (UAGRM), con una trayectoria profesional de más de 20 años como abogada. Está certificada como *Anti-Money Laundering Certified Associate (AMLCA)* por la Florida International Bankers Association (FIBA).

Desde hace 16 años se desempeña en el sector financiero, con una sólida experiencia en áreas de cumplimiento, especialmente en prevención de lavado de activos y financiamiento del terrorismo (PLA/FT). Ha ejercido funciones como Analista y Oficial de Cumplimiento. Su experiencia abarca la implementación de políticas antilavado, la gestión de riesgos, la supervisión de reportes regulatorios y la formación en prevención de delitos financieros.

Combina una sólida base jurídica con un enfoque técnico-operativo, promoviendo prácticas éticas en la lucha contra el lavado de activos.

Agradecimientos

Quiero expresar mi sincero agradecimiento a todas las personas que me brindaron su apoyo durante la elaboración de esta monografía.

En especial, agradezco al Lic. Ramiro Uribe y a mis colegas de trabajo en Banco Económico S.A. por su constante respaldo, consejos y motivación, los cuales fueron fundamentales para llevar adelante este proyecto.

También agradezco a mi familia y amigos por su comprensión y apoyo incondicional en los momentos de dedicación y esfuerzo.

Finalmente, reconozco la importancia de todas las fuentes consultadas y el compromiso de quienes trabajan por un uso ético y responsable de la tecnología en la lucha contra el lavado de dinero.

Santa Cruz de la Sierra, Bolivia, 18 de Junio de 2025

Señores:

Federación Latinoamericana de Bancos – FELABAN

Presente.-

Ref.: DECLARACION

En cumplimiento de lo dispuesto en el artículo 8 del Reglamento del XIV Concurso Latinoamericano de Monografías sobre Prevención del Lavado de Activos y Financiamiento del Terrorismo, relativo al procedimiento de presentación, declaro lo siguiente:

a) El trabajo presentado cumple con las condiciones del concurso.
b) Autorizo exclusivamente a la Federación Latinoamericana de Bancos para que (por si o por quien ésta designe) edite, extracte o de cualquier manera reproduzca el presente trabajo, trátese o no, del trabajo ganador.
c) Acepto todas las condiciones del concurso, reconociendo que el dictamen del Jurado es irrecurrible.
d) No publicare, ni divulgare el trabajo presentado hasta tanto no se dé a conocer la monografía ganadora.

Asimismo, el autor aclara que la elaboración y contenido del mismo son de exclusiva responsabilidad del autor, quien se pone a disposición para cualquier comentario o consulta (knarvaez@baneco.com.bo)

Kattia Narvaez Copeticon

C.I. 4724583 SC

Índice

Resumen Ejecutivo

Esta monografía analiza el impacto de la inteligencia artificial (IA) en el contexto del lavado de dinero, destacando tanto sus aplicaciones positivas como sus posibles usos maliciosos por parte de redes criminales. El avance de la tecnología ha facilitado nuevas formas de criminalidad, entre ellas el uso de algoritmos, plataformas digitales y criptomonedas para ocultar y mover fondos de origen ilícito.

Se examinan los riesgos emergentes asociados al uso indebido de la IA, como la automatización de actividades financieras ilícitas, la creación de identidades falsas y la evasión de controles financieros tradicionales. Asimismo, se identifican los desafíos que enfrentan los gobiernos y las instituciones financieras para responder a estas amenazas, incluyendo la falta de marcos legales actualizados y la limitada capacidad técnica para supervisar tecnologías complejas.

A través de un enfoque proactivo, la investigación propone medidas para fortalecer la regulación, promover el uso ético de la IA y fomentar la cooperación internacional. También se presentan recomendaciones basadas en estándares internacionales como los del Grupo de Acción Financiera Internacional (GAFI/FATF), así como en buenas prácticas aplicadas en distintos países.

En conclusión, si bien la IA representa un riesgo cuando es utilizada con fines ilícitos, también puede ser una herramienta poderosa para prevenir y detectar delitos financieros, siempre que su uso se fundamente por principios éticos, una regulación eficaz y una supervisión constante.

Introducción general

En los últimos años, la tecnología ha avanzado muy rápido y ha cambiado muchas cosas en nuestra vida diaria, incluyendo cómo funcionan los bancos y los sistemas financieros. Una de las tecnologías más importantes hoy en día es la inteligencia artificial (IA), que permite a las computadoras analizar datos, tomar decisiones y automatizar procesos.

Aunque la IA puede ser muy útil para mejorar la seguridad y detectar actividades ilegales, también puede ser usada por personas con malas intenciones. Algunos delincuentes están usando esta tecnología para cometer delitos más difíciles de detectar, como el lavado de dinero, que consiste en hacer que dinero obtenido de forma ilegal aparente ser legal.

El objetivo de esta monografía es explicar cómo los criminales pueden usar la inteligencia artificial para lavar dinero y qué riesgos representa esto para la sociedad. También se hablará sobre cómo los gobiernos y las instituciones pueden actuar de forma preventiva, es decir, adelantarse a los problemas, con leyes y controles adecuados.

Este trabajo busca ayudar a entender mejor los peligros del mal uso de la tecnología y proponer formas de proteger el sistema financiero sin frenar la innovación.

1. Introducción

1.1. Planteamiento del problema

El avance de la tecnología ha transformado la forma en que operan las finanzas, los negocios y la vida cotidiana. Herramientas como la inteligencia artificial (IA) han sido creadas para facilitar procesos, analizar grandes volúmenes de datos y mejorar la eficiencia tanto en el sector financiero, como en otros sectores. Sin embargo, estas mismas tecnologías también están siendo utilizadas por personas con fines ilegales, como el lavado de dinero.

Actualmente, los delincuentes pueden usar la IA para automatizar operaciones, simular identidades, analizar sistemas de control y mover dinero ilícito sin ser detectados fácilmente. Esto representa un gran desafío para las autoridades y los sistemas de control tradicionales, que muchas veces no están preparados para responder ante métodos tan sofisticados.

Se estima que el lavado de dinero representa entre el 2% y el 5% del PIB mundial, lo que equivale a más de 2 billones de dólares al año. Esta cifra, reportada por la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), evidencia la magnitud del problema a nivel global y subraya la necesidad urgente de adoptar medidas eficaces para prevenir y combatir este delito financiero.

Por eso, es fundamental entender cómo se está utilizando la IA para el lavado de dinero, qué riesgos representa esta tendencia, y qué medidas pueden tomarse para asegurar que la tecnología se use de forma segura, ética y responsable.

1.2. Justificación e importancia del tema

Este tema es importante porque la inteligencia artificial (IA) se está usando cada vez más en todo el mundo, incluso en los bancos y sistemas financieros. Aunque esta tecnología trae muchos beneficios, también puede ser usada por personas para cometer delitos, como el lavado de dinero.

El lavado de dinero es un problema muy serio porque ayuda a que el dinero de actividades ilegales aparente ser legal. Cuando los delincuentes usan IA para hacerlo, es más difícil descubrirlo y detenerlo.

Por eso, es necesario estudiar cómo se está usando la IA en este tipo de delitos, para entender los riesgos y ayudar a crear leyes o reglas que eviten que esto siga pasando. También es importante para proteger la economía y la seguridad del país.

1.3. Objetivos de la investigación

1.3.1. Objetivo general:

Analizar cómo la inteligencia artificial (IA) puede ser usada por delincuentes para lavar dinero y qué medidas se pueden tomar para prevenirlo mediante una regulación más proactiva.

1.3.2. Objetivos específicos:

- Explicar qué es la criminalidad tecnológica y cómo se relaciona con el lavado de dinero.
- Identificar las formas en que la IA puede ser usada para cometer este delito.
- Describir los riesgos que esto representa para el sistema financiero.
- Revisar qué leyes o reglas existen actualmente para controlar esta situación.
- Proponer posibles soluciones o mejoras en la regulación para prevenir el uso malicioso de la IA.

1.4. Metodología utilizada

Para realizar esta monografía se utilizó una metodología de tipo **documental y descriptiva**. Por lo que significa que se buscó, leyó y analizó información de fuentes confiables como libros, artículos académicos, informes internacionales (como los del GAFI) y documentos legales sobre inteligencia artificial, lavado de dinero y criminalidad tecnológica.

También se revisaron casos reales y noticias recientes para entender mejor cómo los delincuentes pueden usar la inteligencia artificial (IA) en actividades ilegales. Toda esta información se organizó y explicó de manera clara para responder a los objetivos planteados y proponer soluciones que ayuden a mejorar la regulación.

2. Marco Conceptual y antecedentes

En este punto se define los conceptos clave que sustentan la investigación, permitiendo comprender el contexto en el que convergen la criminalidad tecnológica, el lavado de dinero y el uso de la inteligencia artificial (IA) en el ámbito financiero. A través de este marco teórico se establecen las bases para analizar los riesgos, oportunidades y desafíos que surgen de dicha convergencia.

2.1. Definición de la criminalidad tecnológica

La criminalidad tecnológica, también conocida como ciberdelincuencia o delito informático, se refiere al conjunto de actividades ilícitas que utilizan sistemas informáticos, redes digitales o tecnologías emergentes como medio, objetivo o instrumento del delito. Esta forma de criminalidad ha evolucionado con el avance de las tecnologías de la información, diversificándose en tipos y aumentando su impacto económico y social.

2.2. Concepto del lavado de dinero

El lavado de dinero es el proceso por el cual las personas tratan de hacer que el dinero que obtuvieron de actividades ilegales (como narcotráfico, corrupción o trata de personas, entre otros delitos precedentes) aparente ser legal. Esto se hace en tres pasos:

a) **Colocación:** el dinero entra al sistema financiero.
b) **Estratificación o Transformación:** se mueve entre cuentas o diferentes productos financieros para esconder su origen, a fin de hacer difícil su seguimiento contable.
c) **Integración:** finalmente se mezcla con dinero legal y pasa a formar parte de la economía formal.

El lavado de dinero es un delito grave porque permite que los criminales sigan operando y afecta a la economía de los países.

2.3. Inteligencia Artificial (IA): conceptos básicos

La inteligencia artificial (IA) es una rama de la informática que se ocupa del desarrollo de sistemas capaces de realizar tareas que normalmente requieren inteligencia humana, como el reconocimiento de patrones, la toma de decisiones, el aprendizaje y el procesamiento del lenguaje natural.

Entre las principales técnicas y componentes de la IA se encuentran:

- **Machine learning (aprendizaje automático):** algoritmos que aprenden de datos para predecir o clasificar comportamientos.
- **Deep learning:** redes neuronales profundas que permiten analizar grandes volúmenes de información no estructurada.
- **Procesamiento de lenguaje natural (NLP):** interpretación automática de textos, voz o comunicaciones humanas.

- **Visión por computadora:** análisis automatizado de imágenes y videos.

2.4. Relación entre inteligencia artificial y delitos financieros

La inteligencia artificial (IA) puede ser usada para automatizar procesos ilegales y dificultar su detección. Por ejemplo, puede ayudar a mover grandes cantidades de dinero rápidamente, generar identidades falsas o manipular datos. Por eso, entender cómo se usa la IA en delitos financieros, como el lavado de dinero, es clave para crear regulaciones más eficaces y proteger el sistema financiero.

A continuación algunos ejemplos, de cómo se puede usar la IA en actividades ilegales:

- **Mover dinero rápidamente:** la IA puede hacer transferencias en muchas cuentas en poco tiempo, para que no se pueda ver de dónde viene el dinero.
- **Crear cuentas o empresas falsas:** los delincuentes pueden usar IA para hacer documentos falsos y abrir cuentas bancarias que parecen reales.
- **Ocultar el origen ilícito de los fondos:** mediante técnicas avanzadas, la IA puede transformar operaciones financieras derivadas de actividades ilícitas en transacciones aparentemente legales.
- **Utilizar activos virtuales para encubrir fondos ilegales:** la combinación de IA y criptomonedas permite ocultar transacciones mediante mecanismos de anonimato y descentralización.
- **Lavado de dinero automatizado:** la IA puede mover fondos entre múltiples cuentas o jurisdicciones para ocultar su origen ilícito.
- **Transferencias estructuradas o fraccionadas:** la IA puede ser utilizada para diseñar esquemas de transferencias, con el objetivo de evitar los umbrales que activan reportes automáticos por movimientos inusuales.

- **Manipulación de mercados o fraudes financieros:** la IA puede usar algoritmos para distorsionar el mercado y evadir controles mediante transacciones automatizadas.
- **Uso de bots para realizar operaciones falsas o encubiertas:** la IA puede emplear bots para manipular precios y evadir controles mediante transacciones simuladas o difíciles de rastrear.

A su vez, las instituciones financieras están adoptando IA como defensa, aplicándola en sistemas de detección de fraude, monitoreo transaccional y segmentación de riesgos. Este doble uso de la tecnología plantea el desafío de desarrollar marcos regulatorios que incentiven su uso responsable y eviten su explotación con fines criminales.

Así como la IA puede ser utilizada para cometer fraudes financieros, también se aplica en soluciones tecnológicas conocidas como RegTech. Estas herramientas permiten a bancos, fintechs y autoridades automatizar procesos de cumplimiento normativo, monitorear riesgos en tiempo real y detectar actividades sospechosas con mayor precisión. Su implementación representa una oportunidad concreta para modernizar la supervisión financiera y aumentar la eficacia en la lucha contra delitos financieros en entornos digitales.

3. Funcionamiento de la Inteligencia Artificial (IA)

La inteligencia artificial (IA) se basa en el uso de **algoritmos**, que son instrucciones que le dicen a la máquina qué hacer. Estos algoritmos pueden aprender de los datos que se les da, mejorando su rendimiento con el tiempo. A esto se le llama **aprendizaje automático** o machine learning.

3.1. Aplicaciones comunes de la IA:

- **En el sector financiero:** la IA ayuda a detectar fraudes, analizar riesgos, automatizar procesos de atención al cliente y gestionar inversiones.

- **En la salud:** se usa para ayudar a diagnosticar enfermedades a partir de estudios médicos.
- **En la seguridad:** puede identificar comportamientos sospechosos o controlar cámaras de vigilancia.
- **En la vida diaria:** está presente en asistentes virtuales (como Siri o Alexa), redes sociales, publicidad digital, etc.

La IA tiene muchos beneficios, pero también puede ser usada de forma negativa. Por eso, es importante entender cómo funciona y cómo puede ser utilizada tanto para el bien como para cometer delitos, como veremos en los próximos apartados.

3.2. ¿Por qué la IA se considera un problema?

Porque estas herramientas permiten que los delitos se realicen con más rapidez, a mayor escala y con menor riesgo de ser descubiertos. Además, muchas instituciones aún no están preparadas para detectar este tipo de amenazas avanzadas.

Debido a esto, es fundamental que las leyes y las autoridades se actualicen y entiendan cómo funciona la inteligencia artificial (IA), para poder regular su uso y prevenir que sea utilizada con fines ilegales.

3.3. Aplicaciones de la IA en soluciones RegTech

Las RegTech son tecnologías diseñadas para ayudar a las instituciones financieras a cumplir con sus obligaciones regulatorias de forma más eficiente, automatizada y segura. Estas soluciones, potenciadas por inteligencia artificial (IA), han revolucionado el campo del cumplimiento normativo y la supervisión, facilitando la detección temprana de riesgos financieros y mejorando los procesos de monitoreo y control.

La IA desempeña un papel clave en las RegTech, permitiendo analizar grandes volúmenes de datos en tiempo real, identificar patrones inusuales, reducir errores humanos y optimizar recursos. A continuación se describen algunas de las principales aplicaciones de la IA dentro del ecosistema RegTech:

- **Monitoreo transaccional automatizado:** La IA permite analizar de manera continua millones de transacciones para detectar comportamientos atípicos o potencialmente delictivos, como movimientos estructurados, patrones repetitivos o desvíos de fondos. A diferencia de los sistemas tradicionales basados en reglas estáticas, los modelos basados en machine learning pueden adaptarse y evolucionar a medida que surgen nuevas amenazas.
- **Verificación de identidad digital (e-KYC):** A través del reconocimiento facial, biometría y procesamiento de lenguaje natural, los sistemas de e-KYC basados en IA pueden verificar identidades de forma remota, rápida y precisa. Esto reduce el riesgo de fraude de identidad y facilita el cumplimiento de las normas Conozca a su cliente (KYC) y Prevención de lavado de dinero.
- **Análisis predictivo de riesgos:** Los algoritmos de IA pueden prever la probabilidad de que ciertos clientes, operaciones o productos financieros estén vinculados a actividades sospechosas. Esto permite a las entidades priorizar investigaciones y asignar recursos de manera más efectiva.
- **Gestión de reportes y cumplimiento normativo:** La IA también se emplea para generar reportes regulatorios de forma automatizada, asegurando consistencia y trazabilidad, así como para monitorear cambios en marcos legales y adaptar rápidamente las políticas internas de cumplimiento.

En un entorno financiero cada vez más digital y complejo, las RegTech basadas en IA representan una respuesta innovadora y necesaria frente al auge de la criminalidad tecnológica y los desafíos de supervisión. Su implementación no solo fortalece la transparencia y la trazabilidad, sino que también ayuda a reducir costos, aumentar la eficiencia y mejorar la capacidad de reacción ante riesgos emergentes como el lavado de dinero mediante métodos tecnológicos avanzados.

4. Características principales de la criminalidad tecnológica

La criminalidad tecnológica representa uno de los mayores desafíos para los sistemas legales y de seguridad actuales, ya que combina rapidez, anonimato y alcance internacional; entre sus características principales tenemos las siguientes:

- **Uso de herramientas tecnológicas**: los delincuentes emplean software, redes, sistemas automatizados o plataformas digitales para cometer sus actos.
- **Dificultad para rastrear:** muchas veces estos delitos se cometen desde otro país, lo que dificulta la investigación.
- **Alta velocidad de ejecución:** las transacciones o acciones delictivas pueden realizarse en segundos.
- **Impacto global:** un delito tecnológico puede afectar a personas, empresas o instituciones en varios países al mismo tiempo.
- **Constante evolución:** los métodos y técnicas cambian rápidamente, lo que obliga a las autoridades a actualizarse continuamente.

4.1. El papel de la tecnología en la facilitación del lavado de dinero

La tecnología ha hecho que muchas actividades sean más rápidas y eficientes. Sin embargo, también ha sido aprovechada por los delincuentes para facilitar el lavado de

dinero. Antes, este delito se realizaba principalmente con dinero en efectivo, negocios o inversiones de manera presencial. Ahora, gracias al internet y a las nuevas herramientas digitales, es posible mover grandes sumas de dinero de forma casi invisible.

El avance tecnológico, si bien ha traído grandes beneficios, también ha sido aprovechado por redes delictivas. De hecho, **Europol advierte que más del 60% de las redes criminales en Europa utilizan tecnologías digitales para facilitar actividades como el lavado de dinero, el fraude y la evasión de controles**. Esto evidencia que los grupos delictivos han incorporado herramientas digitales para operar de forma más rápida, global y anónima.

La tecnología permite que los delincuentes oculten el origen del dinero ilegal más fácilmente, lo transfieran a diferentes países y lo integren en la economía sin ser detectados. Además, al tratarse de procesos digitales, muchas veces es difícil rastrear quién está realmente detrás de las operaciones, especialmente cuando se utilizan sistemas automatizados, criptomonedas o redes encriptadas.

4.2. Métodos tecnológicos empleados en el lavado de dinero

Los delincuentes han encontrado nuevas formas de usar la tecnología para lavar dinero. A continuación, se explican tres de las más comunes:

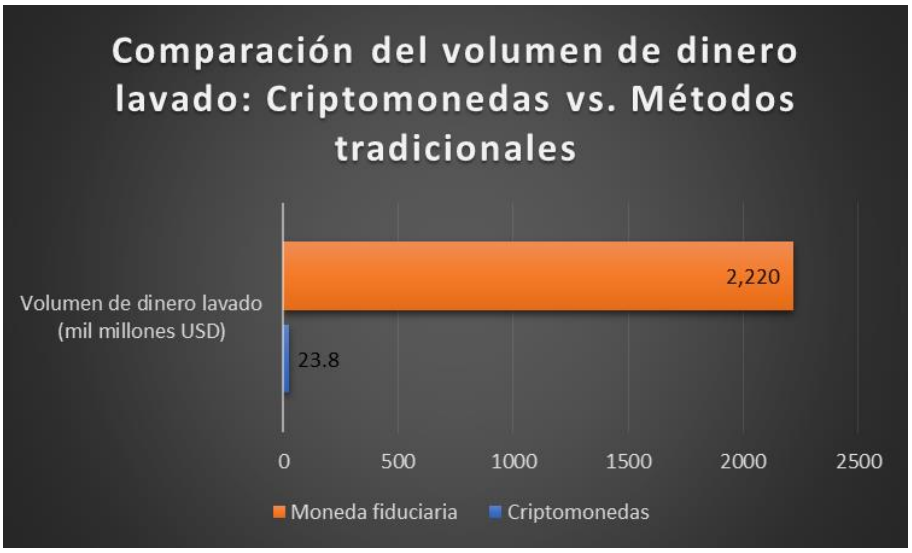
4.2.1. Criptomonedas y tecnologías blockchain

Las criptomonedas, son monedas digitales que se pueden usar para comprar y vender sin necesidad de un banco. Son rápidas, globales y en muchos casos anónimas, lo que las hace atractivas para el lavado de dinero.

El blockchain, la tecnología detrás de estas monedas, registra todas las transacciones de forma permanente. Sin embargo, este registro no siempre muestra claramente quién está detrás de cada operación, ya que los usuarios pueden mantener su identidad oculta.

Algunos delincuentes aprovechan esta característica y utilizan servicios llamados “mezcladores” o “tumblers”, que mueven criptomonedas entre muchas cuentas para dificultar el seguimiento del dinero.

Gráfico 1: Volumen estimado de lavado de dinero por método (en mil millones de USD)



Fuente: Elaboración propia basada en datos de Chainalysis y ONUDD.

Este gráfico muestra el volumen estimado de lavado de dinero realizado a través de criptomonedas comparado con el lavado de dinero mediante moneda fiduciaria. Aunque el lavado de dinero con criptomonedas alcanza los 23.8 mil millones de dólares, la mayor parte del lavado de dinero sigue realizándose con moneda tradicional, que suma aproximadamente 2.22 billones de dólares. Esto indica que, si bien las criptomonedas son un método emergente y creciente para ocultar fondos ilícitos, las formas tradicionales siguen dominando. La regulación y los controles deben adaptarse para enfrentar ambos métodos, especialmente ante la evolución tecnológica.

Un ejemplo reciente muestra cómo estas tecnologías están siendo utilizadas con fines delictivos: **una red criminal desmantelada en Europa logró mover más de 75 millones de euros en solo un año mediante el uso de criptomonedas**. Durante la operación, las

autoridades incautaron **26,4 millones de euros en criptoactivos**, lo que evidencia el uso sofisticado y transnacional de tecnologías digitales para el lavado de dinero.

Aunque el blockchain puede ser una herramienta útil para la transparencia financiera cuando se utiliza correctamente, también representa un reto para las autoridades, ya que requiere conocimientos técnicos y recursos especializados para rastrear fondos ilegales.

4.2.2. Plataformas digitales y pagos electrónicos

Aplicaciones de pago como PayPal, apps bancarias o billeteras móviles permiten enviar dinero de un lugar a otro en segundos. Aunque son muy útiles para las personas y los negocios, también pueden ser usadas por criminales para mover dinero ilegal sin ser detectados.

Además, los delincuentes pueden abrir cuentas falsas o usar identidades robadas para mover fondos sin dejar rastro real. Algunas plataformas no verifican bien la identidad de los usuarios, lo que facilita el uso con fines delictivos.

4.2.3. Uso de inteligencia artificial y algoritmos avanzados

La inteligencia artificial (IA) puede ser usada para automatizar el lavado de dinero. Por ejemplo, un programa puede hacer cientos de transferencias pequeñas para evitar que los bancos detecten una operación sospechosa. También puede generar documentos falsos, predecir cuándo es más seguro mover dinero o engañar a los sistemas de seguridad.

La IA aprende de los datos y se adapta. Esto significa que, si los controles cambian, los algoritmos también pueden cambiar su comportamiento para evitar ser detectados.

4.3. Riesgos y desafíos emergentes en el ámbito tecnológico

El uso de tecnología en el lavado de dinero trae muchos **riesgos nuevos** y **problemas** que antes no existían. Ahora los delincuentes tienen más formas de esconder el dinero y es más difícil para las autoridades encontrarlos.

Algunos de los principales desafíos son:

- **Es difícil seguir el rastro del dinero:** como las transferencias se hacen por internet y en pocos segundos, muchas veces es complicado saber de dónde vino el dinero o a dónde fue.
- **Las leyes no siempre están actualizadas:** las tecnologías como las criptomonedas o la inteligencia artificial son muy nuevas, y en muchos países todavía no hay reglas claras para controlarlas.
- **La tecnología avanza muy rápido:** los criminales cambian sus métodos constantemente, pero las leyes y los sistemas de control tardan más en adaptarse.
- **Se puede esconder la identidad fácilmente:** muchas veces los delincuentes usan nombres falsos o programas que los hacen parecer otras personas, lo que hace más difícil saber quién está detrás.

Por todo esto, es muy importante que los gobiernos, el sistema financiero y las autoridades trabajen juntos, se mantengan actualizados y creen nuevas formas de prevenir que la tecnología sea usada con fines criminales.

5. La IA como Herramienta Maliciosa en el Lavado de Dinero

Antes de abordar los usos maliciosos de la inteligencia artificial (IA) en el contexto del lavado de dinero, es fundamental comprender primero sus aplicaciones legítimas dentro del sector financiero. Esto permite reconocer que, si bien la IA puede ser empleada con fines ilícitos, también representa una herramienta poderosa para mejorar la eficiencia, la seguridad y el

cumplimiento normativo en las instituciones financieras. A continuación, se describen algunas de las formas en que esta tecnología está transformando positivamente el ecosistema financiero, como paso previo para analizar sus posibles usos indebidos.

5.1. Aplicaciones legítimas de la IA en el sector financiero

La inteligencia artificial (IA) es muy útil en el mundo financiero. Muchos bancos y empresas usan esta tecnología para hacer su trabajo más rápido, seguro y eficiente. Algunas de las **formas buenas** en las que se usa la IA son:

- **Detectar fraudes:** la IA puede revisar miles de transacciones y detectar si hay algo sospechoso.
- **Atención al cliente:** muchos bancos usan chatbots (robots que responden) para ayudar a los clientes.
- **Evaluar riesgos:** la IA ayuda a decidir si dar un crédito o una tarjeta, analizando la situación financiera de las personas.
- **Prevenir el lavado de dinero:** también se usa para identificar patrones raros que podrían indicar lavado de dinero.

En este contexto, las tecnologías RegTech potenciadas por IA están transformando positivamente el cumplimiento regulatorio. Estas soluciones permiten automatizar tareas complejas como el monitoreo transaccional, la verificación de identidad (e-KYC), la gestión del riesgo y la generación de reportes regulatorios, todo en tiempo real. Gracias a la IA, las RegTech pueden adaptarse rápidamente a nuevas amenazas, reducir errores humanos y aumentar la eficiencia de los procesos de cumplimiento.

Además, contribuyen a que las instituciones financieras cumplan con normativas internacionales y locales de forma más eficaz, minimizando los costos operativos y aumentando la transparencia. Esto representa un avance significativo frente a métodos

tradicionales, y al mismo tiempo, una herramienta poderosa para prevenir el uso indebido del sistema financiero por parte de actores criminales.

En suma, la IA aplicada en RegTech no solo mejora la seguridad y eficiencia de los servicios financieros, sino que también fortalece la resiliencia del sistema ante riesgos emergentes, como el lavado de dinero digital y los fraudes automatizados.

5.2. Usos maliciosos de la IA por delincuentes para evadir controles

Aunque la inteligencia artificial (IA) fue creada para ayudar, también puede ser mal utilizada por delincuentes. Algunas formas en que se utiliza la IA para cometer delitos y evitar ser detectados son:

- **Automatizar operaciones ilegales**: los criminales pueden programar la IA para mover dinero de forma automática, haciendo que aparente ser legal.
- **Generar documentos falsos**: con IA, pueden crear identificaciones, facturas o contratos que parecen reales.
- **Detectar y evitar controles**: los delincuentes pueden entrenar sistemas para aprender cómo funcionan los controles bancarios y así burlarlos.
- **Crear identidades digitales falsas**: usando IA pueden crear personas que no existen, para abrir cuentas o registrar empresas.

Estos usos hacen que el lavado de dinero sea más difícil de detectar y que los delincuentes se vuelvan más sofisticados. De hecho, **Europol ha advertido que la inteligencia artificial está siendo utilizada por organizaciones delictivas para automatizar operaciones ilegales, falsificar identidades y evadir los sistemas tradicionales de verificación**. Además, señala que la IA está reforzando delitos como el tráfico de personas, el fraude en línea y el lavado de dinero, generando nuevas formas de criminalidad tecnológica.

El siguiente gráfico ilustra las principales tecnologías utilizadas por redes criminales en sus actividades ilícitas:

Gráfico 2: Principales tecnologías utilizadas por redes criminales

Fuente: *Elaboración propia basada en datos de Europol, IOCTA 2023.*

El gráfico anterior muestra las principales tecnologías empleadas por redes criminales en sus actividades ilícitas. Se observa que el **ransomware** lidera con un 35% de uso, seguido por **phishing y spear phishing** con un 25%. Las **plataformas de malware como servicio (MaaS)** representan un 20%, mientras que las **redes de comunicaciones encriptadas** y el uso de **deepfakes e inteligencia artificial para fraudes** constituyen el 15% y 5%, respectivamente.

Esta distribución destaca la creciente sofisticación de las redes criminales, que no solo emplean tecnologías avanzadas para ejecutar delitos, sino que también las utilizan para diversificar y ampliar sus operaciones a nivel global.

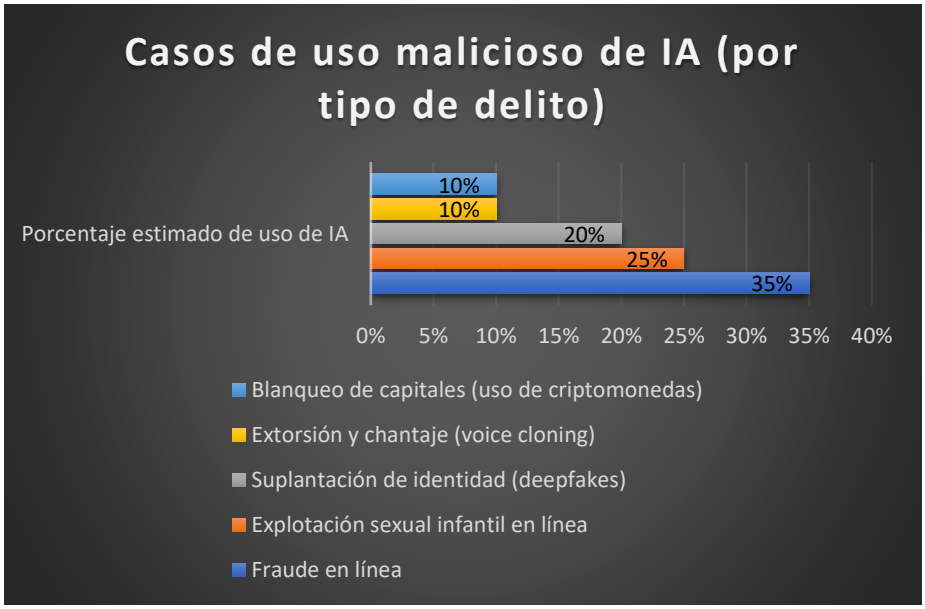
5.3. Casos prácticos y análisis de ejemplos de uso indebido

Aunque muchas veces no se conocen los detalles por temas legales o de seguridad, **existen casos conocidos** donde la inteligencia artificial (IA) fue usada de manera maliciosa:

- **Bots que abren cuentas falsas:** en varios países se han descubierto programas automáticos que abren cuentas bancarias usando documentos robados o falsificados.
- **Mezcla de criptomonedas:** algunas IA son utilizadas para mover dinero en criptomonedas a través de muchas cuentas, dificultando saber de dónde viene.
- **Facturación falsa:** hay programas que crean muchas facturas y empresas ficticias para "justificar" ingresos que en realidad vienen de delitos.
- **Deepfakes:** tecnologías basadas en IA que generan videos o audios falsos para engañar a autoridades o bancos.

Estos ejemplos muestran cómo la IA puede ser usada de forma muy peligrosa si no se controla bien.

Gráfico 3: Casos de uso malicioso de IA (por tipo de delito)



Fuente: Elaboración propia basada en datos de Europol (2025). SOCTA 2025

El gráfico anterior ilustra los principales delitos facilitados por el uso malicioso de la inteligencia artificial, según el informe SOCTA 2025 de Europol. Se observa que el **fraude en línea** lidera con un 35% de incidencia, seguido por la **explotación sexual infantil en línea** con un 25%. Otras actividades delictivas incluyen **suplantación de identidad** (20%), **extorsión y chantaje** (10%) y **blanqueo de capitales** (10%).

Estas cifras reflejan cómo la IA ha transformado el panorama del crimen organizado, permitiendo a los delincuentes operar con mayor rapidez, alcance y sofisticación. La automatización de fraudes, la creación de contenido falso y la evasión de sistemas de control son solo algunas de las estrategias que han sido potenciadas por el uso de tecnologías avanzadas.

5.3.1. Suplantación de identidad mediante deepfakes y desvío de fondos corporativos

Caso Real: *Fraude con deepfakes en empresa energética – Caso "CEO Fraud" en Reino Unido (2020)*

En 2020, la empresa energética europea *Compass Group* sufrió un fraude de suplantación de identidad mediante deepfakes que resultó en el desvío de más de 200,000 euros. Los delincuentes utilizaron tecnología de deepfake para imitar la voz del director ejecutivo y convencer al gerente financiero de transferir fondos a cuentas bancarias controladas por los criminales. Este incidente fue uno de los primeros casos documentados en que la inteligencia artificial se empleó para cometer un fraude corporativo sofisticado.

Implicaciones Técnicas y Legales:

a) Técnicas Utilizadas:

- **Deepfakes de voz:** Emulación avanzada de la voz del CEO para dar órdenes fraudulentas.
- **Ingeniería social asistida por IA:** Combinación de técnicas psicológicas y tecnológicas para manipular a empleados.

b) Implicaciones Legales:

- **Fraude y suplantación de identidad: Uso** ilegal de identidad digital para obtener beneficios económicos ilícitos.
- **Violación de controles internos:** Fallos en los protocolos de autorización financiera que facilitaron la transferencia fraudulenta.

Recomendaciones del GAFI Aplicables:

- **Recomendación 10 Debida diligencia del cliente (CDD):** Requiere que las organizaciones verifiquen cuidadosamente las instrucciones financieras para prevenir fraudes.
- **Recomendación 15 Nuevas tecnologías:** Alienta a los países a identificar riesgos emergentes asociados con tecnologías como los deepfakes y desarrollar controles preventivos.
- **Recomendación 23 Medidas de transparencia para transacciones financieras:** Promueve protocolos para verificar transacciones inusuales y evitar movimientos fraudulentos.

Reflexión Final

Este caso demuestra el peligro real que representan los deepfakes en el ámbito corporativo, donde la automatización y sofisticación tecnológica pueden ser utilizadas para engañar y manipular a empleados responsables de transferencias financieras. La prevención requiere un fortalecimiento de los controles internos y el desarrollo de herramientas tecnológicas que permitan detectar manipulaciones audiovisuales en tiempo real.

5.3.2. Uso de chatbots y asistentes de IA en esquemas de fraude con inversión (Scam-as-a-Service)

Caso Real: *Fraude con chatbots en inversiones basado en IA – Operación "CryptoScamBot" (Estados Unidos, 2023)*

En 2023, la Comisión de Bolsa y Valores de Estados Unidos (SEC) detectó una red criminal que utilizaba chatbots con inteligencia artificial para operar esquemas fraudulentos de inversión en criptomonedas. Los chatbots interactuaban automáticamente con víctimas potenciales, guiándolas para realizar inversiones falsas en plataformas no reguladas. Estos asistentes de IA podían mantener conversaciones complejas, personalizadas y persuasivas, lo que aumentaba la confianza de las víctimas y facilitaba el robo de fondos.

La operación denominada "CryptoScamBot" afectó a cientos de inversores, causando pérdidas superiores a 30 millones de dólares. Las autoridades desmantelaron la red, arrestando a los principales responsables y bloqueando las plataformas fraudulentas.

Implicaciones Técnicas y Legales

a) Técnicas Utilizadas:

- **Chatbots basados en IA:** Automatizaban el contacto con víctimas mediante mensajería instantánea y redes sociales, simulando asesores financieros humanos.
- **Interacciones personalizadas:** Los bots adaptaban sus respuestas según las reacciones del usuario, incrementando la efectividad del fraude.

b) Implicaciones Legales:

- **Fraude financiero:** La utilización de IA para inducir inversiones falsas constituye un delito grave de estafa.
- **Lavado de dinero:** Los fondos robados eran posteriormente blanqueados mediante transacciones complejas y múltiples cuentas bancarias.

Recomendaciones del GAFI Aplicables

- **Recomendación 10 Debida diligencia del cliente (CDD):** Exhorta a las instituciones financieras a implementar controles estrictos para identificar a clientes y operaciones sospechosas, especialmente en contextos digitales automatizados.

- **Recomendación 15 Nuevas tecnologías:** Insta a los países a identificar y mitigar riesgos derivados del uso de tecnologías emergentes como la IA.
- **Recomendación 16 Registro de operaciones sospechosas:** Obligación de reportar actividades inusuales, fundamental para detectar esquemas automatizados de fraude.

Reflexión Final

La automatización del fraude mediante chatbots y asistentes de IA representa un nuevo nivel de sofisticación en los esquemas Scam-as-a-Service. Las entidades regulatorias y financieras deben actualizar sus sistemas de monitoreo y detección para hacer frente a estos riesgos emergentes, integrando tecnologías contra fraudes digitales y fortaleciendo la educación financiera de los usuarios.

5.3.3. Automatización del "smurfing" con IA y bots financieros

Caso Real: *Operación Coinblack-Wendimine (España, 2025)*

En abril de 2025, la Guardia Civil y la Policía Nacional de España desarticularon una organización criminal que estafó más de 19 millones de euros a 208 víctimas mediante el uso de vídeos manipulados con inteligencia artificial (IA). Los delincuentes emplearon IA generativa para crear vídeos falsos en los que personajes famosos animaban a invertir en criptomonedas. Una vez que las víctimas realizaron las inversiones, los estafadores utilizaban bots financieros para dividir los fondos en múltiples transacciones pequeñas, una técnica conocida como "smurfing", para evitar la detección por parte de las autoridades financieras. Esta operación, denominada Coinblack-Wendimine, resultó en la detención de seis personas, incluyendo al líder de la red, quien planeaba huir a Dubái. Se incautaron dispositivos electrónicos, documentación falsa y un arma simulada.

Implicaciones Técnicas y Legales

a) Técnicas Utilizadas:

- **IA Generativa:** Se emplearon herramientas de IA para crear vídeos falsos que simulaban anuncios de inversión con figuras públicas, engañando a las víctimas para que depositaran fondos en plataformas fraudulentas.
- **Bots Financieros:** Una vez recibidos los fondos, se utilizaron bots para realizar múltiples transacciones pequeñas, distribuyendo el dinero en diversas cuentas para evitar alertas por actividades sospechosas.

b) Implicaciones Legales:

- **Estafa y Fraude:** Los delincuentes engañaron a las víctimas mediante representaciones falsas, obteniendo fondos de manera ilícita.
- **Lavado de Dinero:** La técnica de "smurfing" (pitufeo) permitió ocultar el origen ilícito de los fondos, facilitando su integración en el sistema financiero.
- **Falsificación de Documentos:** La creación de identidades y documentos falsos mediante IA generativa constituyó un delito adicional.

Recomendaciones del GAFI Aplicables

- **Recomendación 10 Debida Diligencia del Cliente (CDD):** Las instituciones financieras deben implementar procedimientos de CDD para verificar la identidad de sus clientes. La utilización de identidades falsas creadas por IA generativa subraya la necesidad de fortalecer estos procedimientos para detectar y prevenir fraudes.
- **Recomendación 24 Transparencia y Beneficiarios Finales de Personas Jurídicas:** Es esencial que las autoridades competentes tengan acceso a información precisa sobre los beneficiarios finales de las entidades legales. La creación de empresas pantalla mediante IA generativa puede dificultar esta transparencia, por lo que se deben implementar medidas para garantizar la identificación de los beneficiarios reales.

- **Recomendación 15 Nuevas Tecnologías:** El GAFI insta a los países a evaluar y mitigar los riesgos asociados con el uso de nuevas tecnologías. La IA generativa representa una herramienta poderosa para la creación de identidades y documentos falsos, por lo que es crucial desarrollar estrategias para contrarrestar su uso malicioso en actividades financieras ilícitas.

Reflexión Final

Este caso evidencia cómo la automatización del "smurfing" mediante el uso de IA y bots financieros puede facilitar actividades ilícitas como el lavado de dinero. Es imperativo que las instituciones financieras y las autoridades competentes fortalezcan sus sistemas de verificación y control para detectar y prevenir el uso malicioso de estas tecnologías. Además, se debe promover la cooperación internacional para abordar los desafíos que presentan las nuevas tecnologías en el ámbito del crimen financiero.

5.3.4. Lavado de dinero mediante mercados ilícitos en línea y servicios financieros no regulados

Caso Real: *Huione Group, Camboya (Estados Unidos, 2021 - 2025)*

En mayo de 2025, el Departamento del Tesoro de Estados Unidos propuso prohibir a Huione Group el acceso al sistema financiero estadounidense, calificándolo como una "preocupación primaria de lavado de dinero". Se alega que Huione facilitó el lavado de al menos $4 mil millones en fondos ilícitos entre agosto de 2021 y enero de 2025, incluyendo al menos $73 millones en criptomonedas vinculadas a ciberataques norcoreanos y operaciones de fraude en línea como "pig butchering". Huione Pay, una unidad de Huione, recibió más de $150,000 en criptomonedas de una billetera asociada al grupo de hackers norcoreano Lazarus. Huione Pay afirmó no haber sabido que recibió fondos indirectamente de estos ataques.

Implicaciones Técnicas y Legales

a) Técnicas Utilizadas:

- **Uso de plataformas financieras no reguladas (Huione Pay):** Huione operaba un sistema de pagos alternativo que facilitaba transacciones en múltiples monedas, incluidas criptomonedas, sin cumplir con los estándares internacionales de debida diligencia.
- **Lavado de criptomonedas:** Se detectaron al menos $73 millones en criptomonedas vinculadas a ciberataques, incluidos fondos del grupo de hackers norcoreano Lazarus. Las criptos fueron canalizadas a través de Huione Pay y otras entidades relacionadas.
- **Estructuración y uso de "empresas fachada":** Fondos fueron fragmentados y canalizados a través de múltiples cuentas y empresas de fachada registradas en Asia, lo que dificultaba el rastreo.
- **Apoyo a esquemas de fraude tipo "pig butchering":** Huione fue vinculada a plataformas de estafa que combinaban manipulación emocional con fraudes financieros, captando víctimas principalmente en EE. UU. y Asia.
- **Transferencias transfronterizas sin controles AML/CFT:** Las operaciones involucraron movimientos de fondos entre múltiples jurisdicciones con bajo nivel de supervisión o sin regulación AML, dificultando la cooperación internacional.

b) Implicaciones Legales:

- Revocación de licencia bancaria: El Banco Nacional de Camboya revocó la licencia bancaria de Huione Pay debido a su incumplimiento de las regulaciones existentes y las recomendaciones de los reguladores.
- Propuesta de sanción por parte de EE. UU.: El Departamento del Tesoro de EE. UU. propuso prohibir a Huione Group el acceso al sistema financiero estadounidense, calificándolo como una "preocupación primaria de lavado de dinero".

- Congelación de fondos por parte de Tether: Tether congeló más de $29 millones en su stablecoin USDT asociados con Huione Guarantee, debido a actividades presuntamente vinculadas a operaciones fraudulentas y transnacionales.

Recomendaciones del GAFI Aplicables

- **Recomendación 1 Enfoque basado en riesgo:** Los países deben identificar y evaluar los riesgos asociados a servicios financieros alternativos como Huione Pay y aplicar medidas proporcionales. Huione operó sin una supervisión adecuada, elevando el riesgo sistémico.
- **Recomendación 10 Diligencia debida del cliente (CDD):** Las plataformas como Huione Pay deberían estar obligadas a verificar la identidad de sus clientes y monitorear transacciones, lo que claramente no ocurrió en este caso.
- **Recomendación 15 Nuevas tecnologías:** Huione Pay permitió el uso de criptomonedas sin implementar controles adecuados para prevenir el lavado de dinero y financiamiento del terrorismo, incumpliendo con la recomendación sobre activos virtuales.
- **Recomendación 16 Transferencias electrónicas (Regla del Viajero):** No se aplicaron mecanismos para incluir información sobre el remitente y beneficiario en las transferencias, facilitando el anonimato.
- **Recomendación 40 Cooperación internacional:** El caso demuestra la necesidad de fortalecer la colaboración entre países frente a amenazas transnacionales que implican criptomonedas, fintechs y delitos cibernéticos.

Reflexión Final

El caso del Huione Group pone en evidencia una de las transformaciones más preocupantes del crimen organizado en la era digital: la fusión entre tecnologías emergentes, estructuras financieras opacas y redes criminales transnacionales. Lejos de

tratarse de una operación aislada, Huione representa un modelo sofisticado y escalable de ecosistema criminal digital, donde convergen el fraude, el lavado de dinero, las criptomonedas y, lo más alarmante, la trata de personas.

Este caso también expone las lagunas normativas y los desafíos regulatorios globales. Mientras las autoridades de EE. UU. y algunas organizaciones internacionales comienzan a reaccionar, el alcance y la velocidad de estas redes superan la capacidad de respuesta de muchos Estados. Plataformas como Huione Pay y Huione Guarantee operaron durante años con apariencia de legalidad, lo que evidencia la necesidad urgente de reforzar la supervisión sobre servicios fintech y exchanges cripto no regulados, especialmente en regiones vulnerables.

Por último, Huione revela que detrás de muchas estafas en línea —como el fraude tipo pig butchering— no solo hay víctimas financieras, sino también víctimas humanas invisibles: personas explotadas, forzadas a operar estos fraudes en condiciones de esclavitud moderna. El caso debe ser una llamada de atención a gobiernos, empresas tecnológicas y organismos internacionales para trabajar de forma coordinada en la detección, prevención y persecución de estos delitos complejos, donde lo financiero, lo digital y lo humano se entrelazan peligrosamente.

6. Vulnerabilidades y riesgos asociados al uso malicioso de IA

El mal uso de la inteligencia artificial genera **graves riesgos**, tanto para la seguridad financiera como para la sociedad. Algunos de estos riesgos son:

- **Difícil detección:** cuando la IA hace operaciones ilegales de forma muy parecida a las legales, es difícil para los sistemas de control descubrirlas.
- **Alta velocidad y volumen:** la IA puede hacer muchas operaciones en segundos, lo que complica aún más el control.

- **Falta de preparación de las autoridades:** muchas veces los gobiernos y los bancos no tienen los recursos o conocimientos para enfrentar este tipo de delitos.
- **Confianza en sistemas automáticos:** si los sistemas no están bien diseñados, los delincuentes pueden aprovecharlos para cometer fraudes sin que nadie lo note.

Por este motivo, es fundamental que existan reglas claras y actualizadas, así como profesionales capacitados, para prevenir que la IA se convierta en una herramienta para el delito.

7. Regulación Proactiva y Medidas Preventivas

7.1. Principios de la regulación proactiva en materia de lavado de dinero

La regulación proactiva significa adelantarse a los problemas antes de que ocurran. En el caso del lavado de dinero, esto quiere decir que las leyes y controles deben adaptarse rápidamente a las nuevas formas en que los delincuentes actúan, especialmente cuando usan tecnología e inteligencia artificial (IA).

Los principios básicos de una regulación proactiva son:

- Prevención antes que reacción: no esperar a que ocurra un delito para actuar.
- Actualización constante: las leyes deben adaptarse a los cambios tecnológicos.
- Colaboración entre sectores: gobiernos, bancos y empresas deben trabajar juntos.
- Enfoque en el riesgo: poner más atención en las actividades que presentan mayor peligro de ser usadas para el lavado de dinero.

7.2. Normativas internacionales y nacionales relevantes

7.2.1. Recomendaciones del GAFI/FATF

El GAFI (Grupo de Acción Financiera Internacional) es un organismo internacional que crea reglas para prevenir el lavado de dinero y el financiamiento del terrorismo. Algunas de sus principales recomendaciones son:

- Los países deben evaluar los riesgos y tener medidas según el nivel de peligro.
- Las instituciones financieras deben conocer a sus clientes (KYC – Know Your Customer), (e-KYC – Electronic Know Your Customer) y monitorear a sus transacciones (KYT – Know Your Transaction).
- Debe haber cooperación entre países para investigar y castigar estos delitos.
- Es necesario vigilar nuevas tecnologías, como la IA y las criptomonedas.

Además, el GAFI ha enfatizado la importancia de que los países actualicen sus marcos normativos para responder a los desafíos tecnológicos actuales. Sin embargo, según el Índice Basel AML 2023, aunque muchas jurisdicciones cuentan con buenas leyes sobre el papel, todavía enfrentan dificultades para aplicarlas eficazmente, especialmente frente a amenazas tecnológicas como la inteligencia artificial y las criptomonedas.

7.2.2. Legislación nacional y marco regulatorio aplicable

Cada país debe adaptar las recomendaciones del GAFI a su realidad. Esto incluye:

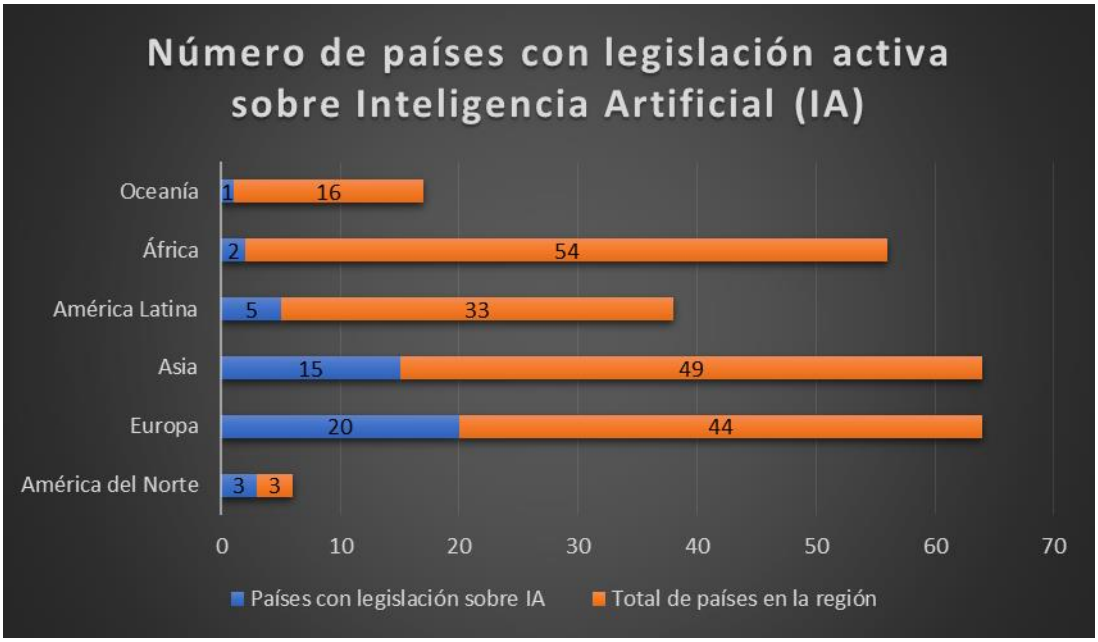
- Leyes contra el lavado de dinero y financiamiento del terrorismo.
- Normas para que los bancos y empresas tecnológicas reporten operaciones sospechosas.
- Regulación del uso de tecnologías financieras y criptomonedas.

En muchos países, estas leyes están siendo actualizadas para incluir temas relacionados con inteligencia artificial y ciberseguridad.

7.2.3. Estado actual de la regulación de IA en el mundo

La regulación de la inteligencia artificial es un tema que está tomando cada vez más relevancia a nivel global. Sin embargo, el avance en la creación de leyes y normativas varía considerablemente entre regiones. Mientras algunos continentes cuentan con numerosos países que han adoptado regulaciones activas sobre IA, otros todavía están en etapas iniciales de desarrollo normativo.

Gráfico 4: Número de países con regulación activa sobre inteligencia artificial por región



Fuente: Elaboración propia basada en datos de Center for AI and Digital Policy. (2024). AI Index 2024: AI and Policymaking

Este gráfico muestra que el avance regulatorio es desigual entre regiones. América del Norte ha logrado implementar normativas activas en todos sus países, mientras que otras regiones, como África y Oceanía, muestran avances limitados o incipientes.

Europa y Asia concentran la mayor cantidad de países con regulación activa sobre IA. Sin embargo, al analizar el porcentaje de países regulados respecto al total en cada región, el liderazgo cambia, revelando importantes diferencias en el grado de preparación frente a los desafíos que impone esta tecnología.

7.3. El rol de las Unidades de Inteligencia Financiera (UIF)

Las UIF son organismos encargados de recibir, analizar y compartir información financiera relacionada con posibles delitos. Su función principal es:

- Recibir reportes de operaciones sospechosas de los bancos y otras entidades.
- Analizar los datos para detectar patrones que puedan indicar lavado de dinero.
- Colaborar con otras autoridades (como policía o fiscalía) en las investigaciones.
- Recomendar mejoras en las políticas de prevención.

Con el avance de la tecnología, las UIF también deben capacitarse y modernizar sus herramientas para poder seguir el ritmo de los delincuentes.

7.4. Uso de tecnologías basadas en IA para la detección y prevención

Así como la IA puede ser usada para cometer delitos, también puede ser una gran aliada para prevenirlos. Algunas formas en que puede ayudar son:

- **Monitoreo automático de transacciones:** detectar movimientos raros o fuera del comportamiento normal del cliente.
- **Análisis de patrones complejos:** identificar señales que podrían pasar desapercibidas para una persona.
- **Alertas tempranas:** avisar rápidamente cuando se detecta una operación sospechosa.
- **Mejora en la gestión de riesgos:** la IA puede ayudar a las instituciones a decidir en qué casos poner más atención.

El uso responsable de la IA en la prevención del lavado de dinero permite actuar más rápido, ser más preciso y proteger mejor al sistema financiero.

7.5. RegTech: innovación en la supervisión y el cumplimiento normativo

Las RegTech (tecnologías regulatorias) utilizan inteligencia artificial, automatización y análisis de datos para mejorar el cumplimiento normativo en el sector financiero. En la prevención del lavado de dinero, estas herramientas permiten detectar operaciones sospechosas en tiempo real, automatizar el monitoreo transaccional y optimizar procesos como la verificación de identidad (KYC) y el análisis de riesgos.

Además de beneficiar a las instituciones financieras, **las RegTech también fortalecen la supervisión estatal** al proporcionar capacidades más dinámicas, predictivas y basadas en datos. Sin embargo, su implementación plantea desafíos como la protección de datos, la transparencia algorítmica y la necesidad de marcos legales actualizados.

En conjunto, las RegTech representan una oportunidad clave para modernizar la lucha contra los delitos financieros, equilibrando innovación tecnológica con una regulación eficaz.

8. Retos y Oportunidades

8.1. Desafíos en la implementación de regulación efectiva

Uno de los principales retos que enfrentan los países y las instituciones financieras es crear leyes y controles que realmente funcionen, especialmente cuando la tecnología cambia tan rápido. Algunos de los problemas más comunes son:

- **Falta de actualización en las leyes:** muchas normas fueron creadas cuando la tecnología actual no existía.

- **Desconocimiento técnico:** no todos los funcionarios o reguladores entienden cómo funciona la inteligencia artificial o las criptomonedas.
- **Limitación de recursos:** algunos países o instituciones no tienen dinero ni personal suficiente para invertir en sistemas modernos.
- **Coordinación internacional difícil:** como el lavado de dinero con tecnología puede cruzar fronteras, es difícil actuar si no hay colaboración entre países.

Además, uno de los principales desafíos es la capacidad técnica limitada de las autoridades para identificar y neutralizar operaciones de lavado de dinero facilitadas por IA. El ritmo lento de actualización normativa contrasta con la velocidad con la que evolucionan las tecnologías usadas por los criminales. Estos desafíos hacen que sea complicado detectar y detener el uso malicioso de la IA en el lavado de dinero.

8.2. Balance entre innovación tecnológica y control regulatorio

Es importante encontrar un **equilibrio** entre permitir el uso de nuevas tecnologías como la IA y, al mismo tiempo, **evitar que se usen para fines ilegales**. Si las reglas son muy estrictas, pueden limitar la innovación; si son muy débiles, pueden facilitar el delito.

Lo recomendable es:

- Apoyar el desarrollo tecnológico, pero con reglas claras y bien definidas.
- Supervisar el uso de la IA, sin impedir que las empresas mejoren sus servicios.
- Dialogar con expertos en tecnología, para que las leyes tengan sentido práctico.
- Probar nuevas ideas (sandbox regulatorio) antes de aplicarlas en todo el sistema financiero.

Este balance ayuda a proteger a las personas y al mismo tiempo impulsar el progreso.

8.3. Oportunidades que ofrece la IA para mejorar la prevención del lavado de dinero

Aunque la IA puede ser usada por delincuentes, también es una **herramienta muy poderosa para combatir el lavado de dinero**. Si se usa correctamente, puede ofrecer muchas ventajas, como:

- Detectar operaciones sospechosas rápidamente, incluso en millones de datos.
- Reducir los errores humanos, gracias a su capacidad de análisis preciso.
- Mejorar la toma de decisiones, ya que puede predecir comportamientos de riesgo.
- Ahorrar tiempo y recursos, automatizando tareas que antes eran lentas y manuales.

Además, la IA permite adoptar un enfoque proactivo, donde la supervisión ya no se limita a reaccionar después de que ocurre una operación ilícita, sino que actúa de forma preventiva, bloqueando movimientos sospechosos antes de que se concreten.

En este contexto, las RegTech basadas en inteligencia artificial representan una oportunidad concreta y transformadora para el cumplimiento normativo moderno. Estas tecnologías permiten a bancos, fintechs y autoridades reguladoras automatizar el monitoreo de transacciones, la verificación de identidades (e-KYC), la generación de reportes regulatorios y la evaluación de riesgos. Al integrarse en los sistemas financieros, las RegTech mejoran la trazabilidad del dinero, aumentan la transparencia y reducen los costos operativos.

Gracias a su flexibilidad y capacidad de aprendizaje continuo, las RegTech impulsadas por IA se adaptan con rapidez a nuevas tipologías delictivas y pueden colaborar con sistemas de inteligencia financiera para enfrentar desafíos transnacionales como el lavado de dinero digital, el uso de criptomonedas en mercados ilícitos y la fragmentación de operaciones a través de múltiples jurisdicciones.

9. Propuestas y Recomendaciones

El análisis desarrollado en esta monografía permite traducir los hallazgos en propuestas prácticas aplicables al ámbito profesional, institucional y normativo. La rápida evolución de las tecnologías asociadas a la inteligencia artificial exige respuestas ágiles, coordinadas y técnicamente sólidas por parte de las instituciones financieras, autoridades reguladoras y organismos de supervisión.

A continuación, se presenta una tabla con propuestas concretas que pueden ser implementadas a corto y mediano plazo:

Ámbito de aplicación	Propuesta	Objetivo	Responsable sugerido
Supervisión Financiera	Capacitación continua en IA para auditores, inspectores y analistas	Ampliar la capacidad de supervisión para identificar riesgos emergentes asociados al uso de la IA	UIF, reguladores, entidades supervisoras
Sector financiero (bancos, fintech)	Implementar soluciones RegTech con IA para monitoreo transaccional	Detectar patrones de riesgo en tiempo real	Bancos, fintech, proveedores de tecnología
Marco normativo	Actualizar normativas para incluir IA, criptomonedas y delitos digitales	Cerrar vacíos legales frente a nuevas amenazas	Legisladores, autoridades regulatorias
Cooperación internacional	Fomentar intercambio de información sobre delitos tecnológicos	Abordar el lavado de dinero transfronterizo	UIF, GAFI, organizaciones multilaterales
Educación y sensibilización	Campañas de concienciación sobre riesgos del mal uso de IA	Prevenir el uso indebido y fortalecer la ética en su aplicación	Gobiernos, ONG, medios, sector educativo
Empresas de tecnología	Desarrollar IA con enfoque ético y trazabilidad de algoritmos	Minimizar riesgos de uso malicioso desde el diseño	Desarrolladores, startups, tech companies

Estas propuestas buscan traducir el conocimiento académico en acciones prácticas que puedan ser adoptadas en contextos reales, con el fin de anticipar y mitigar los riesgos del uso malicioso de la inteligencia artificial en el lavado de dinero.

10. Conclusiones

10.1. Síntesis de los hallazgos principales

A lo largo de esta monografía se analizó cómo la inteligencia artificial (IA) puede ser utilizada tanto como una herramienta útil para prevenir delitos, como también un recurso peligroso en manos de los delincuentes. Se destacaron los siguientes puntos:

- La tecnología, y en especial la IA, ha cambiado la forma en que se cometen delitos financieros como el lavado de dinero.
- Las criptomonedas, las plataformas digitales y los sistemas automatizados permiten mover dinero de forma rápida y, muchas veces, sin ser detectados.
- Existen riesgos reales y crecientes en el uso indebido de la IA, que pueden superar la capacidad de respuesta de muchas autoridades.
- La regulación y la supervisión deben ser actualizadas constantemente para mantenerse al día con los avances tecnológicos.
- La cooperación internacional y el uso ético de la tecnología son fundamentales para frenar el lavado de dinero en el mundo actual.

10.2. Reflexiones finales sobre la regulación proactiva y la IA

Regular el uso de la inteligencia artificial no significa detener la innovación, sino **asegurar que se use de manera responsable y segura**. Una regulación proactiva permite adelantarse a los problemas, en lugar de actuar solo cuando ya es demasiado tarde.

Es necesario que las leyes y las políticas públicas se enfoquen en **prevenir**, y no solo en castigar. Esto implica trabajar de forma coordinada entre gobiernos, empresas tecnológicas, bancos y organismos internacionales.

También se debe promover el uso de la IA **con responsabilidad**, garantizando que se respeten los derechos de las personas, la privacidad y la transparencia.

10.3. Perspectivas futuras en la lucha contra el lavado de dinero

En el futuro, la lucha contra el lavado de dinero dependerá en gran medida de **cómo se usen las nuevas tecnologías**. Si bien los delincuentes seguirán buscando formas de aprovecharse de los avances tecnológicos, también habrá más herramientas para detectarlos y detenerlos.

Las perspectivas más importantes son:

- **Mayor uso de IA para prevenir delitos**, con sistemas cada vez más inteligentes y precisos.
- **Mayor colaboración internacional**, para enfrentar amenazas que cruzan fronteras.
- **Regulación más clara y adaptada a los tiempos actuales**, que permita equilibrar seguridad e innovación.
- **Formación y capacitación continua**, para que los profesionales puedan responder mejor a los nuevos desafíos.

En resumen, si se actúa de forma coordinada y responsable, la inteligencia artificial puede dejar de ser una amenaza y convertirse en una gran aliada en la lucha contra el lavado de dinero.

11. Contribución al Conocimiento Especializado en PLA/FT

La presente monografía aporta una visión integral y actualizada sobre el impacto que la inteligencia artificial (IA) puede tener en el ámbito del lavado de dinero, tanto desde el uso malicioso por parte de redes criminales como desde su aplicación en la detección y

prevención del delito. Al enfocarse en la **criminalidad tecnológica** y en la **necesidad de una regulación proactiva**, este trabajo se convierte en una herramienta relevante para profesionales, reguladores, entidades financieras y unidades de inteligencia financiera.

Además, al incorporar estadísticas recientes, gráficos comparativos y un enfoque práctico, se facilita la comprensión de los riesgos emergentes asociados a la IA y se brindan propuestas concretas para fortalecer los marcos normativos. Esta monografía también promueve una visión multidisciplinaria y colaborativa, reconociendo que la lucha contra el lavado de dinero requiere el trabajo conjunto de expertos en tecnología, derecho, finanzas y seguridad.

En síntesis, el trabajo contribuye de manera sustancial al conocimiento especializado en PLA/FT al:

- Identificar nuevas modalidades tecnológicas delictivas.
- Proponer el uso responsable de la IA como herramienta de cumplimiento.
- Analizar el estado actual de la regulación global sobre IA.
- Destacar el papel estratégico de las RegTech en la modernización de la supervisión financiera.
- Plantear recomendaciones adaptadas al contexto local e internacional.

12. Bibliografía

- Arner, D. W., Barberis, J., & Buckley, R. P. (2020). FinTech, RegTech and the reconceptualization of financial regulation. *Northwestern Journal of International Law & Business*.
- Basel Institute on Governance. (2023). *Basel AML Index 2023: Global Money Laundering Risk Assessment*. Recuperado de

https://baselgovernance.org/publications/basel-aml-index-2023

- Basel Institute on Governance. (2023, noviembre 13). *Basel AML Index 2023: Acción contra el lavado de dinero más urgente que nunca*. Recuperado de https://baselgovernance.org/news/basel-aml-index-2023-action-money-laundering-more-urgent-ever
- BBC News. (2020, septiembre 1). Fraudsters use AI to mimic boss's voice in £220,000 scam. *BBC News*. Recuperado de https://www.bbc.com/news/technology-53915345
- Center for AI and Digital Policy. (2024). *AI and Policymaking: AI Index 2024*. Recuperado de https://www.caidp.org
- Chainalysis. (2022). *Crypto Crime Report 2022*. Recuperado de https://www.chainalysis.com/crypto-crime-report-2022
- Comisión Económica para América Latina y el Caribe (CEPAL). (2021). *Transformación digital y gobernanza financiera en América Latina*. Naciones Unidas.
- CoinDesk. (2025, mayo 2). Huione Group de Camboya recibió $98 mil millones en criptomonedas, lo que llevó a una acción del gobierno de EE. UU.: Elliptic. *CoinDesk*. Recuperado de https://www.coindesk.com/business/2025/05/02/cambodian-huione-group-received-usd98b-in-crypto-leading-to-u-s-crackdown-elliptic
- Cointelegraph. (2025, mayo 2). El Departamento del Tesoro de EE. UU. busca cortar a Huione por vínculos con el crimen cibernético. *Cointelegraph*. Recuperado de https://cointelegraph.com/news/us-treasury-cutting-huione-banking-system-crypto-laundering-ties
- Departamento del Tesoro de los Estados Unidos. (2025, mayo 1). FinCEN identifica al grupo Huione, con sede en Camboya, como una institución financiera de preocupación primaria en materia de lavado de dinero y propone una regla para combatir estafas cibernéticas y robos. *U.S. Department of the Treasury*. Recuperado de

https://www.fincen.gov/news/news-releases/fincen-finds-cambodia-based-huione-group-be-primary-money-laundering-concern

- Europol. (2022). *European Money Mule Action (EMMA)*. *European Union Agency for Law Enforcement Cooperation*. Recuperado de https://www.europol.europa.eu
- Europol. (2023). *Internet Organised Crime Threat Assessment (IOCTA) 2023*. *European Union Agency for Law Enforcement Cooperation*. Recuperado de https://www.europol.europa.eu/publications-documents/internet-organised-crime-threat-assessment-iocta-2023
- Europol. (2023). *Serious and Organised Crime Threat Assessment (SOCTA) 2021*. *European Union Agency for Law Enforcement Cooperation*. Recuperado de https://op.europa.eu/en/publication-detail/-/publication/6e5575ce-c34b-11eb-a925-01aa75ed71a1
- Europol. (2025). *European Union Serious and Organised Crime Threat Assessment (SOCTA) 2025*. *European Union Agency for Law Enforcement Cooperation*. Recuperado de https://www.europol.europa.eu/
- Financial Action Task Force (FATF). (2020, septiembre 14). *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing*. Recuperado de https://www.fatf-gafi.org/en/publications/methodsandtrends/documents/virtual-assets-red-flag-indicators.html
- Financial Action Task Force (FATF). (2021). *Oportunidades y riesgos de la inteligencia artificial para la lucha contra el lavado de dinero y el financiamiento del terrorismo*. París: FATF.
- Financial Action Task Force (FATF). (2012, actualizada a 2023). *Las 40 Recomendaciones del GAFI*. Recuperado de https://www.fatf-gafi.org/

- International Monetary Fund (IMF). (2021, octubre 29). AI and RegTech. *Fondo Monetario Internacional*. Recuperado de https://www.imf.org/en/News/Articles/2021/10/29/sp102921-ai-and-regtechimf.org
- Pengjian Liang. (2024, noviembre). RegTech innovations streamlining compliance, reducing costs in the financial sector. *ResearchGate*. Recuperado de https://www.researchgate.net/publication/380208350_RegTech_innovations_streamlining_compliance_reducing_costs_in_the_financial_sectorresearchgate.net
- Pérez, M., & Gómez, J. (2022). *Inteligencia Artificial y delitos financieros: una mirada desde el Derecho Penal*. Editorial Jurídica Continental.
- Reuters. (2025, mayo 2). EE. UU. se prepara para prohibir a Huione de Camboya por presunto lavado de dinero. *Reuters*. Recuperado de https://www.reuters.com/sustainability/boards-policy-regulation/us-moves-ban-cambodias-huione-over-alleged-money-laundering-2025-05-02/
- Revelis. (2024, abril 3). AI in RegTech: how to optimize compliance controls. *Revelis*. Recuperado de https://www.revelis.eu/en/ai-in-regtech-how-to-optimize-compliance-controls/revelis.eu
- Rodríguez, C. (2021). El lavado de activos a través de tecnologías emergentes: desafíos regulatorios en América Latina. *Revista Latinoamericana de Derecho Financiero, 14*(2), 45-62.
- Swiss Quality Consulting. (2024, abril 3). AI and Machine Learning in RegTech: Transforming Risk Management and Compliance Monitoring. *Swiss Quality Consulting*. Recuperado de https://theswissquality.ch/ai-and-machine-learning-in-regtech-transforming-risk-management-and-compliance-monitoring/theswissquality.ch

- The Wall Street Journal. (2025, mayo 6). Dentro de los mercados en línea que facilitan las estafas 'pig butchering'. *The Wall Street Journal*. Recuperado de https://www.wsj.com/finance/currencies/cambodia-huione-pig-butchering-scam-f9d16ef9
- U.S. Securities and Exchange Commission (SEC). (2023, agosto 15). SEC charges defendants in $30 million cryptocurrency chatbot fraud scheme. *U.S. Securities and Exchange Commission*. Recuperado de https://www.sec.gov/news/press-release/2023-158