



XXIX CONGRESO
HEMISFERICO

EL USO MALICIOSO DE LA INTELIGENCIA ARTIFICIAL (IA) EN EL LAVADO DE DINERO

Criminalidad Tecnológica y
Regulación proactiva

Kattia Narvaez Copeticon

 **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**



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.

La inteligencia artificial (IA)

“La inteligencia artificial se refiere a sistemas diseñados para operar con distintos niveles de autonomía y que, mediante la recopilación y procesamiento de datos, pueden inferir cómo lograr un conjunto determinado de objetivos utilizando métodos de predicción, recomendación o toma de decisiones, influyendo en entornos físicos o virtuales.”

Unión Europea

Delitos financieros

“Son conductas tipificadas por la ley que implican el uso indebido de sistemas, instrumentos o servicios financieros con el propósito de obtener beneficios ilícitos, ocultar el origen o destino de activos, o facilitar otras actividades criminales. Incluyen, entre otros, el blanqueo de capitales, la financiación del terrorismo, el fraude, la corrupción, el soborno, la malversación de fondos, la manipulación de mercados y la evasión fiscal.”

ONU y GAFI



"Dos Rostros, Un Mismo Cerebro"



El uso ético de la IA



Aplicaciones de la IA en soluciones RegTech



Monitoreo
transaccional
automatizado



Verificación de
identidad digital
(e-KYC)



Análisis predictivo
de negocios

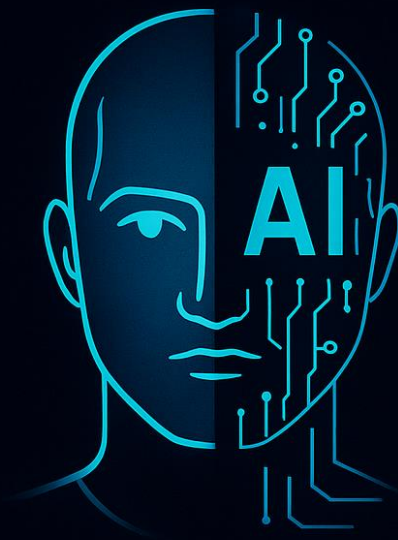


Gestión de reportes
y cumplimiento
normativo



El uso malicioso de la IA

Formas en que se utiliza la IA para cometer delitos:



Automatizar
operaciones
ilegales



Generar
documentos
falsos



Detectar y
evitar
controles

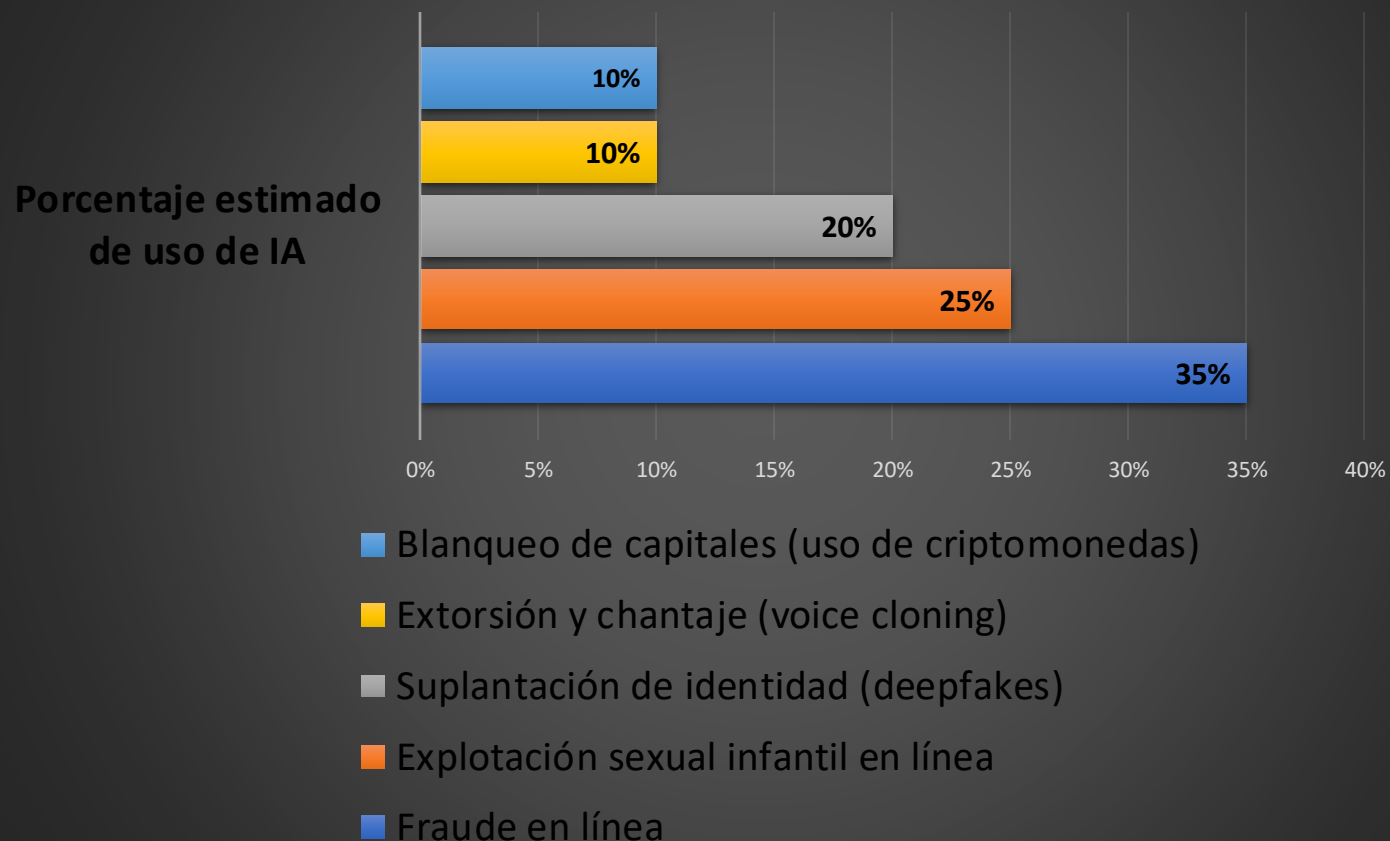


Crear
identidades
falsas



El uso malicioso de la IA

Casos de uso malicioso de IA (por tipo de delito)



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

“Cuando la Inteligencia Artificial se vuelve Criminal”

Fraude con deepfakes en empresa energética en Reino Unido (2020). Daño económico más de 200.000 euros

Estafa mediante videos manipulados con IA generativa para inversión en criptoactivos en España (2025). Daño económico más de 19 millones de euros

WSJ PRO

Estafadores utilizaron IA para imitar la voz del director ejecutivo en un caso inusual de ciberdelito

Las estafas que utilizan inteligencia artificial son un nuevo desafío para las empresas

Por Catherine Stupp

Operación conjunta de la Policía Nacional y la Guardia Civil

Detenidas seis personas por estafar más de 19 millones de euros usando inteligencia artificial

Lavado de Dinero, mediante criptomonedas vinculadas a ciberataques norcoreanos en Estados Unidos (2025). Se estima un blanqueo de 73 millones de dólares

REGULACIÓN

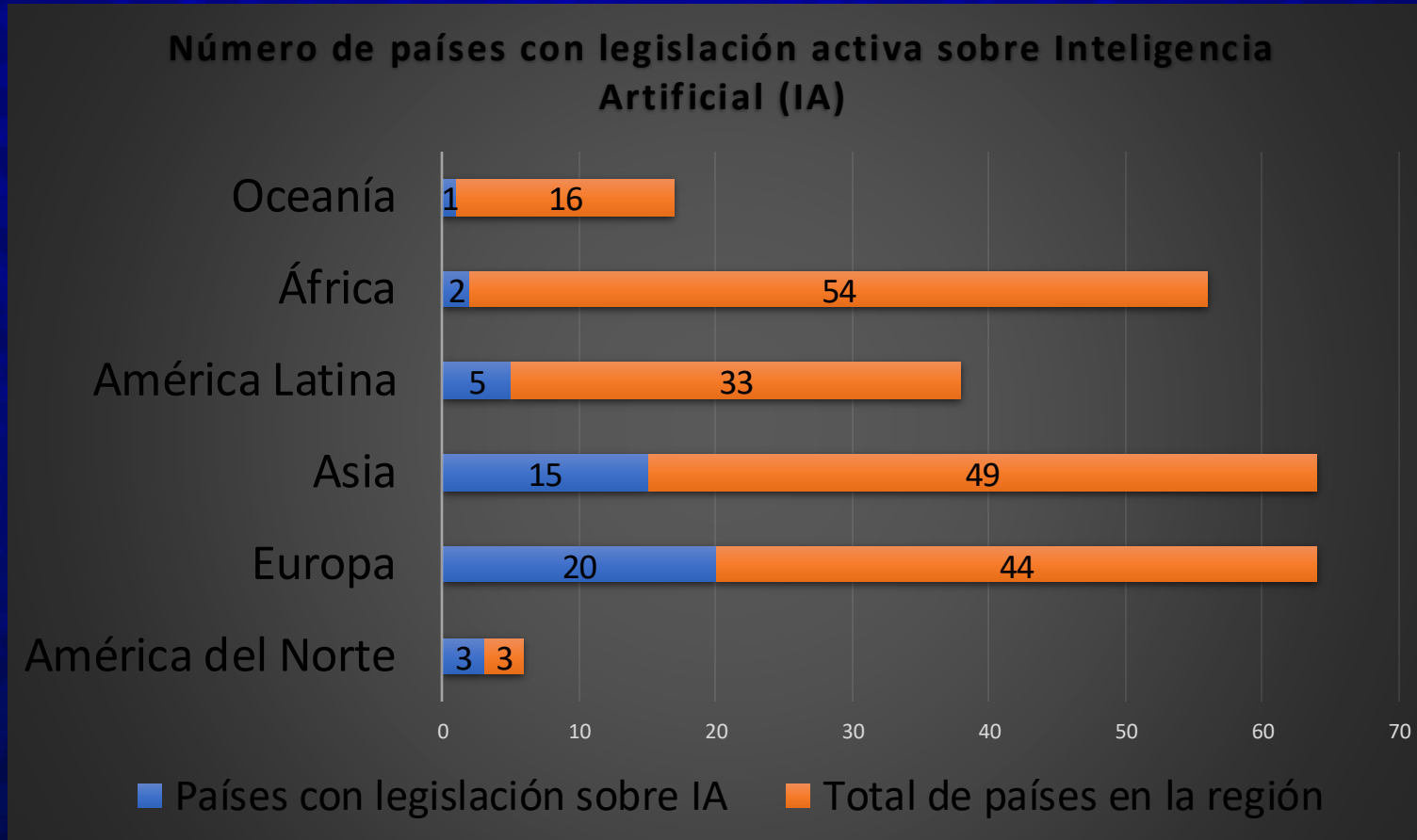
Compartir

El gobierno de EE. UU. comienza a separar al Grupo Huione de Camboya del sistema financiero.

La rama del Departamento del Tesoro que lucha contra los delitos financieros utilizó su salvaguarda más potente para proponer desmantelar la organización por considerarla un peligro de lavado de dinero.

POR JESSE HAMILTON | EDITADO POR NIKHILESH DE

Estado actual de la regulación en IA en el mundo



Fuente: Elaboración propia basada en datos de Centro de Inteligencia Artificial y Política Digital (EE.UU).

(2024)

La importancia de la regulación proactiva

Principios de la regulación proactiva en materia de lavado de dinero



Prevención
antes que
reacción



Actualización
constante



Colaboración
entre sectores



Enfoque en
el riesgo



Propuestas y recomendaciones

Ámbito de aplicación	Propuesta	Objetivo	Responsable sugerido
Supervisión Financiera	Capacitación continua en IA para auditores y analistas	Fortalecer capacidades técnicas para detectar operaciones inusuales	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

Reflexiones finales sobre la regulación proactiva y la IA



¡Muchas gracias! Agradezco su tiempo e interés.