EL PACCTO 2.0
EU-LAC Partnership on justice and security

INFORME TÉCNICO LEGISLATIVO SOBRE TIPIFICACIÓN DE DELITOS COMETIDOS MEDIANTE SISTEMAS DE INTELIGENCIA ARTIFICIAL

TEGUCIGALPA

Edición: Programa EL PACCTO 2.0

Coordinado por:

EXPERTISE FRANCE
GROUPE AFD

Autores

Marc Reina Tortosa, Emilie Breyne, Alfonso Peralta, Cristos Velasco y Thomas Cassuto

Con la colaboración de:

Foro de Presidentes y Presidentas de Poderes Legislativos de Centroamérica y la Cuenca del Caribe – FOPREL

Derechos de uso: Este documento ha sido elaborado para el programa EL PACCTO 2.0, con el apoyo financiero de la Unión Europea. Sin embargo, solo refleja las opiniones de los autores y no las del programa ni las de la Unión Europea. EL PACCTO 2.0 y la Unión Europea no se hacen responsables de las consecuencias que puedan derivarse de la reutilización de esta publicación.

Edición no venal

Madrid, septiembre de 2025

info@elpaccto.eu
Avenida del Partenón, 16-18, 3ª planta
28042 – Madrid (España)

ÍNDICE

RESUMEN EJECUTIVO

La Inteligencia Artificial (IA) evoluciona a una velocidad sin precedentes. Está presente en casi todos los sectores de la vida cotidiana. Los grupos de delincuencia organizada lo están integrando en su operativa diaria para ampliar y mejorar capacidades, explotar vulnerabilidades, abrir nuevos mercados ilícitos, y ampliar su dominio del espacio y del ciberespacio, ya sea de modo directo o mediante personas físicas o jurídicas facilitadoras (*brokers*).

La capacidad del crimen organizado para innovar y adaptarse a nuevas tendencias y tecnologías no es nueva. Se dio en su momento con el surgimiento de internet o el desarrollo de vehículos no tripulados. En este sentido, la IA representa un desafío mayor debido a su rápida penetración en la sociedad y por los riesgos que entraña.

No obstante, la IA, bien utilizada, puede ser un vector fundamental de innovación, desarrollo económico y apoyo al conjunto de la sociedad. Puede transformar la economía por completo, y puede ser un elemento clave para agilizar el trabajo de tanto el sector público como el privado.

El potencial de la IA para revolucionar la administración de justicia y la investigación criminal es innegable y ha habido avances fundamentales en la materia en países como Argentina, Brasil, Chile, Colombia, Costa Rica, España, Francia o Países Bajos, entre otros. Para mitigar riesgos y poder tener una respuesta adecuada y adaptada a la realidad en materia judicial y de seguridad, es esencial disponer de un marco normativo adecuado, moderno y flexible que permita a los Estados actuar en materia administrativa, civil o penal cuando se requiera.

Este informe técnico legislativo analiza los aspectos clave de las nuevas tendencias vinculadas a la inteligencia artificial en los sectores de justicia y seguridad, aquellos delitos que se cometen y la legislación vigente en los 9 países del Foro de Presidentes y Presidentas de Poderes Legislativos de Centroamérica y la Cuenca del Caribe (FOPREL). La finalidad última del informe técnico legislativo es avanzar en la tipificación armonizada de aquellos delitos facilitados, cometidos o perfeccionados mediante herramientas y sistemas de IA.

1. INTRODUCCIÓN

Los países de América Central, México y la Cuenca del Caribe se encuentran actualmente en una encrucijada en materia de inteligencia artificial (IA) y nuevas tecnologías emergentes. Mientras que algunos de los países han dado avances muy claros en regulación, estrategia y fomento del desarrollo de ecosistemas locales con financiación pública, privado o mixta, en aspectos clave de la IA, otros no han conseguido sumarse a lo que probablemente es la mayor revolución desde la propia Revolución Industrial.

En el marco de los países del Foro de Presidentes y Presidentas de Poderes Legislativos de Centroamérica y la Cuenca del Caribe (FOPREL), estados como Belice, Costa Rica, El Salvador, Honduras, México, Panamá y República Dominicana se han adherido a distintas iniciativas regionales para impulsar una IA más ética, dando fruto a la Declaración de Santiago (2023) para "promover una inteligencia artificial ética en América Latina y el Caribe" y la Declaración de Montevideo y la hoja de ruta (2024), la cual busca promover una mayor gobernanza de la IA así como impulsar un desarrollo normativo regional, ambas declaraciones promovidas por el Banco de Desarrollo de América Latina y el Caribe (CAF) y UNESCO.

En otro foro regional impulsado por Colombia llamado Cumbre Ministerial Latinoamericana y del Caribe por la Inteligencia Artificial 'ColombIA', adoptó la Declaración de Cartagena de Indias para la Gobernanza, la Construcción de Ecosistemas de Inteligencia Artificial (IA) y el Fomento de la Educación en IA de manera Ética y Responsable en América Latina y el Caribe. Países del FOPREL como Costa Rica, Guatemala, Honduras, Panamá y República Dominicana fueron firmantes de la declaración.

No obstante, las iniciativas tomadas en materia de IA por los países de Centroamérica y la Cuenca del Caribe han sido limitadas y muy dispares individualmente. Costa Rica, por ejemplo, obtuvo el sexto lugar en América Latina y el Caribe dentro del *Governmental AI Readiness Idex* de 2024 de Oxford Insights, seguida de México (8º), República Dominicana (9º) y Panamá (10º). Las autoridades costarricenses han desarrollado varios proyectos piloto de uso de la IA vinculados al monitoreo de obras públicas y prevención de la corrupción (dIAra),[1] la identificación de facturas falsas por parte del Ministerio de Hacienda a través del proyecto "Hacienda Digital", o el desarrollo de la IA para mejor administrar la justicia, con ejemplos como "Nymiz" donde el Poder Judicial ha desarrollado esta aplicación para garantizar el cumplimiento de la Ley 8968 sobre protección de datos personales, la cual permite anonimizar automáticamente documentos judiciales antes de su publicación.

Sin embargo, aparte del desarrollo estratégico, ético y de gobernanza desarrollado en Costa Rica, la mayoría de los países de Centroamérica, México y la Cuenca del Caribe se han quedado sustancialmente retrasados.

En el ámbito de la seguridad y justicia, el acelerado desarrollo de sistemas de IA y tecnologías emergentes como blockchain ha generado nuevas oportunidades, pero también desafíos significativos en materia de responsabilidad penal. Los sistemas de IA, en particular aquellas que operan de forma autónoma o semiautónoma, pueden ser utilizadas para cometer actos ilícitos, dificultando la atribución de responsabilidad penal conforme a los marcos legales tradicionales.

En los últimos meses se ha visto un incremento exponencial en el conjunto de América Latina y el Caribe, así como en Europa, Estados Unidos y Asia, de delitos facilitados,

[1] Proyecto de Dispositivo de Inteligencia Artificial para Reconocimientos y Alertas (dIAra), desarrollado por la Contraloría General de la República de Costa Rica en el área de anticorrupción. Disponible en: https://www.opengovpartnership.org/es/the-open-gov-challenge/costa-rica-artificial-intelligence-alerts-citizen-control-public-infrastructure/?utm_source=chatgpt.com

sistematizados y evolucionados mediante sistemas de IA como los deepfake, los fraudes complejos, el uso de la ingeniería social para focalizar ataques informáticos como los malware, ransomware y phishing automatizados y adaptados mediante herramientas de IA, delitos vinculados a la producción de material sintético o semisintético de abuso sexual a menores y el uso de vehículos autónomos para el tráfico de drogas, homicidios o actos subversivos del orden público, entre otros.

En este marco, algunos países han empezado a regular el uso de la IA vinculada al delito. Ejemplos pueden encontrarse en:

- Ley Retírenlo (*Take it down Act*) de Estados Unidos (2025), la cual obliga a las plataformas tecnológicas a eliminar deepfakes íntimos no consensuados;
- Ley SREN (*Loi Visant à Sécuriser et à Réguler l'Espace Numérique*) de Francia (2024), que complementa el artículo 226-8 del Código Penal francés, y busca regular el entorno digital, proteger a los menores de la pornografía en línea y combatir el fraude en línea. Además, prohíbe explícitamente el intercambio no consentido de contenidos deepfake;
- Ley de Seguridad en Línea (*Online Safety Act*) del Reino Unido (2023) penaliza deepfakes explícitos o que causen daño intencionalmente;

Como se puede apreciar, las normativas vigentes están muy focalizadas en penalizar y controlar los riesgos vinculados a los deepfake, pero no contemplan, en la mayoría de los casos una visión completa del conjunto de delitos cometidos o facilitados mediante sistemas y herramientas de IA. Delitos que en muchos casos evolucionan a una velocidad vertiginosa y que no tienen por qué estar vinculados directamente a grupos de crimen organizado en el sentido estricto del artículo 2.a) de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional (UNTOC, por sus siglas en inglés). En efecto, muchos de los delitos facilitados mediante IA pueden ser cometidos tanto por una persona física como una persona jurídica, a veces incluso sin saber que es delito, lo cual no le exime de responsabilidad (principio de *ignorantia iuris non excusat*), y sin una coordinación o cooperación necesaria con otras personas físicas o jurídicas. Esto se da en delitos menores como el fraude a aseguradoras, donde la persona física o jurídica falsifica de modo hiperrealista un hecho con la manipulación de imágenes o la producción de facturas falsas a través de herramientas de IA como ChatGPT o la producción de contenido sexual (semi)sintético.

En consecuencia, mientras la innovación tecnológica avanza y su uso en la vida cotidiana de los ciudadanos está cada vez más presente, la innovación criminal y la diversificación del portafolio de delitos también crece. Los Estados deben adaptar el modo en el que analizar, investigan y tipifican los delitos para adaptarse a dicha innovación y la rapidez en la que surgen.

En este sentido, este informe tiene por objeto analizar la necesidad de tipificar nuevos delitos asociados al uso de la inteligencia artificial, o de adaptar tipos penales existentes, así como considerar esquemas apropiados de imputación, control y sanción. Para ello se

abordarán en profundidad aspectos conceptuales de la IA, las tendencias criminales actuales, su impacto, los desafíos a los que nos enfrentamos y las posibles soluciones legislativas que tenemos para abordarlos. Además, se analizarán los desarrollos normativos en materia de IA y en materia digital de los 9 países del FOPREL. Finalmente, el presente informe técnico legislativo presentará recomendaciones de desarrollo normativo, así como recomendaciones generales para los Estados.

2. MARCO CONCEPTUAL Y CARACTERIZACIÓN DE LOS SISTEMAS Y HERRAMIENTAS DE IA

Con una presencia en incremento exponencial en los últimos años y meses en el día a día de la ciudadanía y de las instituciones estatales en su conjunto, la caracterización de la IA y tener claras las definiciones exactas de cada modelo, sistema o concepto es clave para poder entender su desarrollo actual.

2.1. DEFINICIONES

Inteligencia Artificial (IA)	La IA es una disciplina autónoma que puede definirse como el conjunto de sistemas informáticos que, mediante algoritmos y procesamiento de datos, son capaces de emprender, ejecutar y resolver una variedad de tareas complejas utilizando capacidades similares a ciertos procesos cognitivos humanos como el razonamiento, la predicción, la optimización y automatización de tareas, la toma de decisiones o el aprendizaje, entre otros**.**
Algoritmos (de IA)	Un algoritmo es un conjunto de instrucciones para resolver un problema y, en un algoritmo de IA, esas instrucciones están diseñadas para dar a las computadoras la capacidad de aprender por sí mismas cómo resolver el problema.
Modelos de IA	Un modelo de IA puede definirse como una herramienta preconstruida que contiene el resultado de un proceso de aprendizaje (o entrenamiento) al estar expuesto a datos.
Datos de entrenamiento (*training data*)	Datos de cualquier tipo utilizados para entrenar y enseñar a los modelos de IA cómo reconocer patrones, tendencias, realizar predicciones y tomar decisiones.
Inteligencia Artificial General (*Artificial General Intelligence*)	La inteligencia artificial general es una evolución teorética e hipotética en la que un sistema de IA puede igualar o superar las capacidades cognitivas de los seres humanos en cualquier tarea o función.

Aprendizaje profundo (*deep learning*)	El aprendizaje profundo es una rama avanzada del aprendizaje automático que se especializa en el manejo de problemas más desafiantes y datos complejos, utilizando arquitecturas de redes neuronales artificiales que imitan cómo funcionan los cerebros humanos y animales.
Aprendizaje autónomo o automático (*machine learning* – ML)	Sistemas que aprenden de los datos para realizar tareas como clasificar imágenes, estimar ventas y detectar transacciones bancarias sospechosas. En la actualidad, ML es una sub-área de la IA.
Aprendizaje por refuerzo (*Reinforcement Learning*)	Un tipo de aprendizaje automático en el que los agentes de IA y sistemas aprenden interactuando con un entorno y recibiendo recompensas o penalizaciones por sus acciones
Redes neuronales (*neural networks*)	Una red neuronal es un método de la IA que enseña a las computadoras a procesar datos de una manera similar a como lo hace el cerebro humano.
Redes generativas antagónicas (Generative Adversarial Networks – GANs)	Arquitectura de aprendizaje profundo mediante modelos de ML en el que dos redes neuronales compiten entre sí para ser más precisas en sus predicciones. Las GAN generan nuevos datos más auténticos a partir de un conjunto de datos de entrenamiento determinados.
Procesamiento del lenguaje natural (*Natural language processing* – NLP)	Aplicación de la IA que se focaliza en tareas relacionadas con el procesamiento, entendimiento y producción de lenguaje humano (texto y habla), con lo que facilita la interacción y comunicación entre humanos y máquinas.
Grandes Modelos de Lenguaje (*Large Language Models* – LLMs)	Sistemas de IA de enorme magnitud que se entrenan con millones o miles de millones de conjuntos de datos de texto para comprender y generar un lenguaje similar al humano.
Visión por ordenador (*Computer vision*)	La visión por ordenador es un campo de la inteligencia artificial que permite a los ordenadores «ver» e interpretar imágenes y vídeos de forma similar a la visión humana.
IA Generativa (*Generative AI*)	Sistemas que han sido entrenados para crear contenido nuevo, como texto, imágenes, música o algoritmos y sistemas, como resultado del aprendizaje de patrones a partir de datos existentes.
Agentes IA (*AI Agents*)	Sistemas autónomos que perciben, deciden y actúan en nombre de los usuarios. Demuestran razonamiento, planificación y memoria, y pueden tomar decisiones, aprender y adaptarse al contexto.
Sesgo de IA (*AI Bias*)	Sesgos producidos en la toma de decisiones de la IA que están vinculados a sesgos en los datos utilizados para su entrenamiento.

2.2. CARACTERIZACIÓN DE LOS SISTEMAS DE IA

Debido al aprendizaje profundo y a otros desarrollos teóricos y tecnológicos recientes, el sector de la IA evoluciona a una velocidad sin precedentes, con cambios mensuales. No obstante, a modo conceptual, los sistemas de IA pueden caracterizarse en dos tipos principales: según su funcionalidad y según sus capacidades.

Aunque la tecnología ha evolucionado enormemente desde su publicación, según el científico Arend Hintze (Hintze; 2016), existen cuatro tipos de IA según su funcionalidad:

- **Máquinas recreativas**. Son aquellos sistemas más básicos que operan en función de unas normas definidas y que son (o eran) puramente recreativos. Estos no tienen la capacidad de formar recuerdos ni de utilizar experiencias pasadas para fundamentar las decisiones actuales. Ejemplos de ello serían la Deep Blue, la supercomputadora de IBM que a finales de la década de 1990 batía a los grandes maestros internacionales del ajedrez; y el motor de recomendaciones de Netflix, el cual procesa datos dependiendo del historial de visualizaciones que tienes en la plataforma.
- **IA de Memoria limitada**. A diferencia de la IA de Máquina Reactiva, este tipo de IA puede recordar eventos y resultados pasados y monitorear objetos o situaciones específicos a lo largo del tiempo. La IA de Memoria Limitada puede usar datos del pasado y del presente para decidir el curso de acción con mayor probabilidad de lograr el resultado deseado. En este sentido, pueden reconocer patrones de comportamiento y adaptarse a ellos. Ejemplos de ello podemos encontrarlos en los coches autónomos, los cuales se basaban en datos de conducción y experiencias pregrabadas, y toman decisiones basados en aspectos conocidos y prácticos. No obstante, en los modelos avanzados, este no sería el caso. Otro ejemplo estaría en los asistentes virtuales popularmente conocidos como Siri, Alexa, Google Assistant, Cortana, los cuales combinan NLPs y sistemas de memoria limitada para entender cuestiones y solicitudes, y tomar decisiones.
- **Teoría de la mente IA**. Es una clase funcional de IA que se sitúa por debajo de la IA General. Aunque se trata de una forma de IA no realizada en la actualidad, la IA con funcionalidad de Teoría de la Mente comprendería los pensamientos y emociones de otras entidades. Esta comprensión puede afectar al modo en que la IA interactúa con quienes la rodean. En teoría, esto permitiría a la IA simular relaciones similares a las humanas.
- **Autoconciencia o "Emotion AI"**. Este es el nivel más elevado de IA que existiría, similar a una super IA, donde el sistema tiene autoconciencia, percepción de sí misma y está comando decisiones como un ser humano. Su desarrollo es, hasta la fecha, puramente teórico, aunque los avances en la materia son importantes.

Sistemas de IA según sus capacidades y el nivel de "inteligencia":

- La **Inteligencia Artificial Estrecha**, también conocida como IA Débil, es el único tipo de IA que existe en la actualidad. Puede entrenarse para realizar una tarea única o limitada, a menudo mucho más rápido y mejor de lo que puede hacerlo una mente. No obstante, en algunos modelos más avanzados puede realizar distintas tareas. Algunas características clave son que operan dentro de un conjunto restringido de funciones y reglas programadas, no tienen consciencia ni comprensión del contexto en el que operan y tampoco pueden aprender fuera de su área limitada. Ejemplos pueden encontrarse en sistemas de recomendación y orientación de Netflix, Amazon y Spotify, asistentes virtuales como Alexa, Siri o Google Assistant, en modelos de reconocimiento

biométrico y su software de accesibilidad, o en aplicaciones de “texto a habla” o “habla a texto” (*text-to-speech*) como las de ElevenLabs, Murf AI o Speechify.

- **Inteligencia Artificial General**, también conocida como IA Fuerte, es, hasta la fecha actual, un concepto teórico. La IAG tendría capacidad de aprender, razonar y aplicar conocimientos de su “área de expertise” a otro sin necesidad de una reprogramación. Esto significa que sus características están muy vinculadas al aprendizaje autónomo, capacidad de razonamiento abstracto, flexibilidad para aplicar conocimientos y potencial de mejorar su programación inicial para tomar decisiones complejas sin intervención humana. Modelos avanzados, como GPT-4 o DeepMind, han mostrado un alto nivel de comprensión contextual, todavía no pueden replicar la inteligencia humana en su totalidad. La investigación en neurociencia computacional y redes neuronales avanzadas busca cerrar esta brecha en las próximas décadas. Potenciales aplicaciones se darían, por ejemplo, en robots autónomos con capacidades de aprendizaje y adaptación a tiempo real (concepto clave en materia de seguridad y delito en los próximos años), IA con habilidades de desarrollo tecnológico y científico.
- **Superinteligencia de IA**. Es un nivel hipotético de IA que superaría las capacidades cognitivas humanas en todos o la mayor parte de aspectos. Sus principales características serían el proceso de grandes volúmenes de información y toma de decisiones a velocidades muy altas, habilidad para automejorarse y aprender sin intervención humana o la resolución de problemas científicos y tecnológicos. Este nivel de IA, además del anterior, supondría un desafío global en materia de ética y control humano, así como riesgos de seguridad e impacto en la sociedad.

3. CONTEXTO SOBRE EL USO DE LA IA Y DELITOS COMETIDOS

El uso de la inteligencia artificial para multitud de finalidades ha aumentado exponencialmente en los últimos dos años y representa una creciente amenaza.[2] Desde asistentes virtuales a agentes de IA en centros de atención y procesamiento de texto y voz, pasando por su uso en diagnósticos clínicos, investigación científica, análisis de grandes datos, control remoto de vehículos no tripulados, marketing o su uso en redes sociales, entre otros. La IA está en casi todos los aspectos de nuestras vidas, incluido el sector público además su uso para cometer delitos.

En los sectores de justicia y seguridad, su uso ha crecido sustancialmente en los últimos años, particularmente en operadores de justicia y, en menor medida para la investigación criminal. Según un estudio realizado por la Organización de las Naciones Unidas para la

[2] Europol, (2025) *European Union Serious and Organised Crime Threat Assessment – The changing DNA of serious and organised crime*, Publications Office of the European Union, Luxembourg.

Educación, la Ciencia y la Cultura (UNESCO), el 44% de los operadores de justicia de 96 países utilizan herramientas de IA[3] como sintetizadores de texto, elaborar borradores de documentos legales o para realizar investigación legislativa, con la finalidad de agilizar su trabajo diario. Es por este motivo, que UNESCO desarrolló en 2024 el primer borrador de Directrices para el uso de la IA en los sistemas judiciales,[4] las cuales establecen 13 principios fundamentales como la protección de derechos humanos, seguridad de la información, transparencia, responsabilidad y auditabilidad, y explicabilidad, entre otros. Las Directrices vienen dadas siguiendo el trabajo realizado por la UNESCO con la Caja de herramientas mundial sobre AI y el Estado de Derecho (2023). [5]

La Caja de herramientas ofrece un marco pedagógico y práctico para jueces, fiscales, defensores públicos, formadores y universidades. Su objetivo es fomentar el uso ético y responsable de la IA en los sistemas judiciales, asegurando que se respeten los derechos humanos, la transparencia y la rendición de cuentas. Aunque las autoridades de seguridad no están directamente mencionadas, sus principios básicos también pueden aplicarse a organismos policiales, particularmente a aquellas unidades de policía judicial.

Un ejemplo práctico de uso de la IA en el sistema judicial se dio en enero de 2023, donde un juez colombiano utilizó ChatGPT para razonar y redactar una sentencia danto la razón a la demandante para exonerarla del pago de citas médicas, terapias y transportes a centros hospitalarios debido a que la familia no cuenta con recursos económicos para hacerse cargo.[6] A raíz de esto, en agosto de 2024, la Corte Constitucional de Colombia dictaminó[7] que, en efecto, el niño estaba exento de pagar las cuotas requeridas y destacó la importancia de la IA como herramienta para gestionar tareas y asistir en la redacción de decisiones judiciales. No obstante, la Corte subrayó la necesidad de establecer principios y límites para no comprometer el derecho al debido proceso, así como la independencia e integridad del poder judicial debido a posibles sesgos.[8]

Otros países de América Latina y el Caribe también utilizan herramientas de IA para agilizar el trabajo y la administración de justicia. El Poder Judicial de Costa Rica, por ejemplo, tiene un sistema de IA para tipificar de documentos para materia cobratoria, el cual clasifica automáticamente más de 140,000 escritos mensuales en materia de cobros. En 2024, la herramienta del Poder Judicial costarricense logró clasificar más de 900,000 documentos sin

[3] Una encuesta de la UNESCO revela lagunas críticas en la formación en IA de los operadores judiciales (2024). Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura. Disponible en: https://www.unesco.org/en/articles/unesco-survey-uncovers-critical-gaps-ai-training-among-judicial-operators

[4] Gutiérrez, J.D. (2024), *Documento de consulta pública: Directrices de la UNESCO para el uso de sistemas de inteligencia artificial en juzgados y tribunales*. UNESCO. CI/DIT/2024/GL/01. Disponible en: https://unesdoc.unesco.org/ark:/48223/pf0000390781_spa

[5] Stankovich, M., Feldfeber, I., Quiroga, Y., Ciolfi Felice, M., y Marivate, V. (2023), Kit de herramientas global sobre IA y el estado de derecho para el poder judicial. UNESCO. CI/DIT/2023/AIRoL/01. Disponible en: https://unesdoc.unesco.org/ark:/48223/pf0000387331_spa

[6] *Colombia: Resuelven primer caso con ayuda de robot ChatGPT* (2023), DW. Disponible en: https://www.dw.com/es/resuelven-en-colombia-el-primer-caso-jur%C3%ADdico-con-la-ayuda-de-robot-chatgpt/a-64597510

[7] Sentencia T-323 de 2024, *Uso de herramientas de inteligencia artificial generativas en procesos judiciales de tutela*, Corte Constitucional de la República de Colombia, Sala Segunda de Revisión. Disponible en: https://www.diarioconstitucional.cl/wp-content/uploads/2024/08/Vea-sentencia-Corte-Constitucional-de-Colombia-T-323-24.pdf

[8] *Inteligencia Artificial en la sala de audiencias: Fallo histórico de la Corte Constitucional de Colombia cita las herramientas de IA de la UNESCO* (2024), UNESCO. Disponible en: https://www.unesco.org/es/articles/inteligencia-artificial-en-la-sala-de-audiencias-fallo-historico-de-la-corte-constitucional-de?hub=701

intervención humana, con un ahorro equivalente al trabajo de 34 personas a tiempo completo.

El Ministerio Público de Chile desarrolló el Fiscal HeredIA® con la finalidad de agilizar el trabajo de los fiscales, analizar mayor volumen de datos e interconexiones entre investigaciones con el objetivo de identificar grupos y redes criminales operando en el país que cometen delitos de alta complejidad. Así mismo, el Ministerio Público Federal del Brasil ha desarrollado o comprado más de 15 herramientas basadas en IA para facilitar su trabajo, agilizarlo y cooperar con otros organismos de justicia y defensa pública del país. Herramientas que van desde la transcripción automática de audio y vídeo, hasta la extracción inteligente de información de expedientes o la automatización de solicitudes de casos judiciales del Tribunal Supremo de Justicia, pasando por alertas automáticas de gestión de personal, envío de correos o identificar publicaciones de interés a nivel internacional.

En materia de investigación criminal[9] hay multitud de herramientas que se han desarrollado en los últimos años para el análisis de riesgo y policía predictiva (ejemplos del sistema Correctional Offender Management Profiling for Alternative Sanctions – COMPAS en Estados Unidos; o del programa Eurocop PredCrime desarrollado en España para la predicción y prevención de delitos), reconocimiento facial (ej. Sistema FRS de ABIS), balística forense y análisis forense de restos de personas (ej. proyecto de Superposición craneofacial[10]), reconstrucción y análisis de escena del crimen (ej. proyecto de la Comisión Europea VALCRI – Visual Analytics for Sense-Making in Criminal Intelligence Analysis), análisis masivo de datos (ej. IBM Security i2 Analyst's Notebook; o COPKIT) o el análisis y evaluación de pruebas (ej. AVENUE – Analysis of Video Evidence with Novel Enhanced Understanding Engine del programa Horizonte 2020 de la UE, o de ROXANNE – Real-time network, text and speech analytics for combating organised crime and terrorism).

Las herramientas y sistemas de IA tienen, sin embargo, desafíos, retos y dificultades que hay que tener en cuenta. Estos son principalmente sesgos vinculados a los datos que se utilizan para entrenar los modelos de IA. Sesgos que pueden ser de género, raza, ideología o religión. En este contexto, es importante remarcar este punto que debe ser propiamente considerado por las autoridades judiciales, pero también policiales cuando se investiga y se analizan pruebas obtenidas mediante estas herramientas. Además, recientemente se han producido alertas sobre la manipulación de pruebas por parte de abogados o funcionarios públicos con finalidades distintas. Si bien este es un campo incipiente, la manipulación de pruebas es algo que irá aumentando exponencialmente a medida que los sistemas de IA integren muchas más herramientas de deepfake, se complejicen y desconozcamos tanto los algoritmos utilizados como su funcionamiento en interno para tomar decisiones. En este sentido, el concepto de "caja negra" cobra una importancia mayor cuando hablamos de validez de pruebas.

[9] Cristos Velasco, Jean Garcia Periche, Juan De Dios Gómez Gómez, Miguel Bueno Benedí (2024). *Inteligencia Artificial y Crimen Organizado*. Programa EL PACCTO 2.0 de la UE.

[10] Práxedes Martínez-Moreno, Andrea Valsecchi, Pablo Mesejo, Óscar Ibañez, Sergio Damas (2024), *Evidence evaluation in craniofacial superimposition using likelihood ratios. Information Fusion*. Disponible en: https://doi.org/10.1016/j.inffus.2024.102489

Estos puntos deben ser tenidos en cuenta cuando se desarrolla normativa especializada vinculada a la IA y el delito, ya que tanto los deepfake como la falsificación de pruebas son herramientas de doble filo. Los desafíos jurídicos y de responsabilidad penal serán múltiples.

En relación con la utilización de la IA para facilitar, cometer o complejizar delitos, su evolución ha sido exponencial en los últimos dos años. Delitos como la falsificación documental y las estafas se han perfeccionado y están al alcance de cualquier persona física o jurídica de modo sencillo. Además, han surgido plataformas y empresas con fachada aparentemente legítima donde puedes comprar programas de malware, algoritmos de phishing o pagar ataques informáticos (denegación de servicio – DDOS; Man-in-the Middle – MitM; Sniffing, Soofing). Ejemplos de dichas plataformas los encontramos en Xanthorox AI o WormGPT.[11] En estas plataformas se automatiza un modelo de negocio basado en crimen como servicio (*crime-as-a-service*[12] cuya finalidad es ofrecer herramientas predesarrolladas para que cualquiera pueda utilizarlas pagando una suscripción y donde la empresa se queda un porcentaje de ganancias. Modelo de negocio que es ampliamente utilizado por las redes criminales de alto nivel y grandes grupos criminales, los cuales emplean brokers o facilitadores especializados en una temática específica (ciberseguridad y ciberdelincuencia, logística, lavado de activos, etc.)

En este contexto, el análisis de los delitos facilitados y/o cometidos mediante sistemas y herramientas de IA resulta imperativo si buscamos tipificar dichos delitos propiamente. No obstante, es necesario subrayar la evolución constante de los delitos y el uso de la IA. A modo de ejemplo, producir una factura falsa o un parte de incidencia mediante plataformas de creación de deepfakes o los mismos ChatGPT o GROK era una utopía hace menos de 2 años. En la actualidad, estas plataformas pueden elaborar una factura falsa con todos los elementos necesarios, incluido un número de IVA y de registro de empresa, en cuestión de segundos.

3.1. TENDENCIAS CRIMINALES Y DELITOS COMETIDOS MEDIANTE SISTEMAS Y HERRAMIENTAS DE IA

Las formas en la que la IA puede ser empleada para la comisión de delitos pueden ser categorizadas en dos según Blauth et al. (2022):[13] aquellas en las que se abusa de sus vulnerabilidades (abuso malicioso de la IA) y aquellas en las que se usa la IA para la comisión de un crimen (uso malicioso de la IA).[14] Aunque los más comunes en cuanto a impacto para

[11] Juan Manuel Aguilar Antonio (2025), *Redes Criminales de Alto Riesgo que utilizan la Inteligencia Artificial para la Comisión de Delitos*. EL PACCTO 2.0.
[12] Europol EC3, *The Internet Organized Crime Threat Assessment (IOCTA),* Chapter 3.1 Crime-as-a-Service. Overview at: https://www.europol.europa.eu/iocta/2014/chap-3-1-view1.html#:~:text=
[13] Blauth, T. F., Gstrein, O. J., & Zwitter, A. (2022). Artificial Intelligence Crime: An Overview of Malicious Use and Abuse of AI. IEEE Access, 10, 77110–77122. Disponible en: https://doi.org/10.1109/ACCESS.2022.3191790
[14] Cristos Velasco, Jean Garcia Periche, Juan De Dios Gómez Gómez, Miguel Bueno Benedí (2024). *Inteligencia Artificial y Crimen Organizado*. Programa EL PACCTO 2.0 de la UE.

la ciudadanía son la segunda categoría, la primera categoría tiene una relevancia mayor ya que compromete los sistemas y herramientas de IA, potenciando el efecto malicioso.

Así mismo, los delitos cometidos, facilitados o realizados mediante IA pueden estar interconectados los unos con los otros. Este es el caso, por ejemplo, de la ingeniería social para lanzar ataques específicos focalizados en el robo de datos (*data as a target*[15]), incluidos los biométricos, que dan lugar a suplantación de identidad virtual o física para cometer otros delitos, como el fraude sofisticado mediante IA o la manipulación de la información. Y todo esto realizado mediante códigos de malware o phishing desarrollados o mejorados a través de herramientas de IA comunes para el conjunto de la ciudadanía.

Las redes criminales de alto riesgo aprovechan la IA para fines como (i) el reclutamiento y radicalización de niños y adolescentes; (ii) la optimización de rutas de tráfico ilícito, principalmente drogas; (iii) la ingeniería social a gran escala; (iv) la sofisticación de malware y ataques informáticos con finalidades que pueden ir desde la obtención de datos para luego revenderlos a otros grupos criminales (*data as a commodity*[16]) o con fines lucrativos; (v) la identificación de vulnerabilidades en sistemas de seguridad e infraestructuras críticas; (vi) la identificación de agentes encubiertos; o, incluso, (vii) la suplantación de identidad para infiltrarse en organismos públicos.

Si tenemos en cuenta las dos categorías establecidas por Blauth et al., podemos distinguir distintas tendencias criminales y delitos que han ido surgiendo recientemente.

3.1.1. ABUSO MALICIOSO DE LA IA

Dentro de la categoría de abuso malicioso de las vulnerabilidades de la IA podemos encontrar distintas tendencias criminales catalogadas en tres bloques principales:

Ataques a la integridad de la IA

Son ataques diseñados para corromper los datos, algoritmos o decisiones de un sistema de IA, sin que el sistema o sus usuarios lo detecten fácilmente. El atacante no intenta apagar o destruir el sistema, sino alterarlo de forma encubierta para lograr sus fines.

Ejemplo de ello es el "**slopsquatting**".[17] Esta es una nueva ciberamenaza que compromete toda la cadena de suministro de software en un solo clic. El slopsquatting se apoya en los errores de los propios modelos de lenguaje (machine learning), lo que permite crear una puerta trasera perfecta (para "**ataques de puerta trasera**" – *backdoor attacks*) para el sistema que los ingenieros van a crear, reforzar o perfeccionar cuando utilicen herramientas de IA como GPT4, GROK 4, CodeLlama o DeepSeek. En este sentido, la

[15] Internet Organised Crime Threat Assessment – IOCTA (2025), Steal, deal and repeat – How cybercriminals trade and exploit your data. European Union Agency for Law Enforcement Cooperation (EUROPOL). ISBN 978-92-9414-027-2. Doi: 10.2813/4926508
[16] Ibid.
[17] M. Luz Domínguez (2025), *Slopsquatting: una nueva ciberamenaza para empresas que automatizan el desarrollo con IA*. Bit Life Media. Disponible en: https://bitlifemedia.com/2025/04/slopsquatting-una-nueva-ciberamenaza-para-empresas-que-automatizan-el-desarrollo-con-ia/

amenaza queda dormida hasta que un desarrollador utiliza un paquete de datos específico que está infectado, construye su herramienta y la empiezan a utilizar empresas privadas y públicas, así como la ciudadanía. El potencial de enriquecimiento ilícito y de espionaje es muy grande. Además, si esta herramienta creada con una puerta trasera se utiliza en sistemas judiciales o para la investigación criminal, puede ser un riesgo serio para la manipulación de pruebas, testimonios, documentos o sentencias, llevando a decisiones judiciales erróneas de suma gravedad.

Otros tipos comunes de ataques de integridad son el "**typosquatting**", que explotan errores tipográficos al escribir nombres de paquetes; el **envenenamiento de datos** (*data poisoning*), aunque parecido y del mismo estilo que el slopsquatting, este consiste en insertar datos maliciosos en el conjunto de entrenamiento de modelos de modo voluntario o involuntario. El resultado del envenenamiento de datos es que el modelo aprende patrones erróneos y puede, por ejemplo, aprender que ciertos tipos de malware no son peligrosos.

Resultados inesperados o no deseados derivados del comportamiento autónomo de la IA

Los resultados derivados del comportamiento de la IA como la **discriminación algorítmica** o los **sesgos clínicos** son efectos no intencionales que emergen cuando un sistema de IA actúa de forma que sus diseñadores o usuarios no previeron, incluso sin intervención maliciosa directa. Es decir, el sistema toma decisiones automáticas con sesgos sistemáticos que afectan derechos fundamentales. Ejemplos de ello pueden darse en la contratación o no de un empleado específico donde ha habido un proceso de selección en la que la IA ha intervenido, la decisión de otorgar un crédito o una ayuda financiera a una persona, o una decisión judicial basada en sesgos o errores de análisis e interpretación de datos, o en un accidente cometido por un vehículo autónomo que toma decisiones inesperadas ante situaciones complejas. En estos casos es importante reflexionar sobre a quién pertenece la responsabilidad administrativa, civil o penal correspondiente.

Ataques de inferencia de membresía (Membership Inference Attacks - MIA)

Técnica en la que un atacante trata de determinar si un dato específico (por ejemplo, una imagen, una historia clínica o un perfil financiero) fue utilizado o no para entrenar un modelo de IA. Este tipo de ataques **violan directamente la privacidad** de los individuos, pueden ser utilizados para la extorsión, ingeniería social o ataques posteriores como el un **ataque de inversión de modelo** que busque reconstruir características de entrada (por ejemplo, el rostro o perfil de una persona) a partir de la salida del modelo o de su estructura interna. Además, estos ataques y pueden estar muy vinculados a otros tipos de abusos maliciosos como el slopsquatting o los ataques de puerta trasera.

3.1.2. USO MALICIOSO DE LA IA

El uso malicioso de la inteligencia artificial es la segunda categoría establecida por Blauth et al. (2022) y se refiere a situaciones en las que individuos, grupos u organizaciones utilizan sistemas de IA de forma deliberada para causar daño, manipular, espiar o cometer delitos. A diferencia del abuso técnico o no intencional de la IA, aquí hay una intención explícita de perjudicar. Una clasificación de los distintos usos maliciosos o, simplemente para simplificar, de los delitos cometidos con IA son:

Delitos contra la información y la privacidad

Deepfakes. A modo simple, el deepfake es un vídeo, imagen o voces manipuladas o creadas de modo sintético mediante IA Generativa sobre personas haciendo o diciendo cosas que parcialmente o nunca ocurrieron. Los deepfake pueden tener un impacto público muy visible, particularmente cuando afectan a instituciones públicas, se producen en momentos electorales o tienen como objetivo menores y mujeres. Un ejemplo paradigmático se dio tras el fallecimiento del Papa Jorge Mario Bergoglio (Papa Francisco), donde los fraudes digitales vinculados a vídeos sintéticos falsos del Papa Francisco se utilizaron para el robo de información personal y datos sensibles como números de cuentas bancarias, pasaportes o documentos de identidad para cometer delitos o posteriormente ser revendidos (los **datos como mercancía de la economía de la ciberdelincuencia** – *data as a commodity of the cybercrime economy*[18]), o mediante vídeos falsos producidos con herramientas de IA para desinformar, manipular o simplemente robar información sensible de toda aquella persona que accediera y diera click en el enlace.

Los deepfakes de voz o video utilizados para aprobar transacciones o acceder a cuentas mediante engaño a sistemas de verificación biométrica están asociados con la clonación de identidad bancaria.

Manipulación de información: uso de sistemas de IA generativa y modelos de lenguaje (LLM) para crear, alterar o distribuir contenido falso o engañoso, con el fin de influir en creencias, emociones, decisiones o comportamientos sociales y políticos. Ejemplos pueden darse en la generación de noticias falsas o deepfakes con impacto político, social o reputacional, aunque los grupos criminales y terroristas también los utilizan para manipular percepciones e influir en las decisiones de la ciudadanía o de las instituciones públicas.

Si bien la manipulación de la información ya existe desde hace muchos decenios, el surgimiento de los deepfake ultra realistas en los últimos años hace que nos planteemos la creación de una subclasificación específica dentro de la manipulación de la información, ya que pueden servir para multitud de fraudes, influencia electoral, derrocar gobiernos, modificar percepciones, lucrar masivamente a grupos criminales, producir y potenciar el abuso sexual a menores y los delitos contra la intimidad.

[18] Internet Organised Crime Threat Assessment – IOCTA (2025), Steal, deal and repeat – How cybercriminals trade and exploit your data. European Union Agency for Law Enforcement Cooperation (EUROPOL). ISBN 978-92-9414-027-2. Doi: 10.2813/4926508

Ataques de phishing con IA. Forma avanzada de estafa donde se emplea IA para automatizar, personalizar y escalar ataques de suplantación de identidad, haciéndose pasar por una entidad confiable como un banco, una empresa, una red social o un individuo. Este tipo de estafa es mucho más creíble, difícil de detectar, utiliza ingeniería social y puede estar personalizada. Además, comparado con el phishing tradicional, esta tiene mayor adaptabilidad ya que es dinámica y aprende de errores, tiene un componente muy realista y puede utilizar voz, imagen y tono de ciertas personas.

En 2024, un empleado del departamento financiero de una empresa multinacional de diseño e ingeniería llamada "Arup" fue engañado para que pagara 25 millones de dólares a unos estafadores que utilizaron tecnología deepfake para hacerse pasar por el director financiero de la empresa en una videoconferencia.[19] Para entrenar la IA que produjo el deepfake, los criminales utilizaron videoconferencias pasadas de los ejecutivos de la empresa para recrear un escenario en el que el director financiero, junto con otros empleados solicitan hacer distintos depósitos u transferencias bancarias.[20] Este ejemplo dado también estaría directamente vinculado a otra tipología de delito como la **clonación de identidad bancaria** (deepfakes de voz o video utilizados para aprobar transacciones o acceder a cuentas mediante engaño a sistemas de verificación biométrica).

- **Smishing**. Es un tipo de phishing donde los hackers utilizan ingeniería social para atacar a sus víctimas mediante mensajes de texto o SMS con la finalidad de engañarlos para descargar malware, compartir información sensible o enviar dinero a criminales. Este tipo de estafa en los últimos tiempos se combina con el sms spoofing. El SMS no solo te pide que hagas una acción con tu banco, sino que se agrupa en la cadena de SMS con el resto de las notificaciones de autorizaciones de pago legítimas del banco Lo que en definitiva se pretende es a través de la suplantación de la entidad bancaria, haciéndose pasar por ella, introduciendo un mensaje dentro del mismo hilo de los mensajes legítimos y verdaderos de la entidad, con un tono de urgencia, que la víctima pinche en el enlace y autorice los dispositivos del atacante para de esta manera tomar el control de la aplicación y las credenciales bancarias.
- **Vishing**. Combinación de *«voice»* y *«phishing»*, el vishing se basa en la manipulación de los usuarios mediante llamadas telefónicas falsificadas que parecen proceder de fuentes legítimas. Entre sus riesgos podemos destacar la suplantación de identidad, el acceso no autorizado a cuentas bancarias y la divulgación de información sensible.

Delitos financieros y económicos

[19] Heather Chen and Kathleen Magramo (2024), Finance worker pays out $25 million after video call with deepfake 'chief financial officer'. CNN. Disponible en: https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk

[20] Cristos Velasco, Jean Garcia Periche, Juan De Dios Gómez Gómez, Miguel Bueno Benedí (2024). *Inteligencia Artificial y Crimen Organizado*. Programa EL PACCTO 2.0 de la UE.

Fraudes (y estafas) automatizados. Los fraudes con IA son una forma sofisticada y emergente de delitos en los que se utilizan sistemas de IA, principalmente bots, para engañar, manipular o estafar con fines ilícitos y, generalmente, lucrativos. Los fraudes pueden ser desde muy simples e individualizados a altamente complejos y automatizados mediante otras herramientas de IA. Bots que realizan suplantación de identidad, estafas por phishing o manipulación bursátil.

- **Fraudes en reclamaciones de bajo nivel**. Categoría incipiente que surge con la IA Generativa y, particularmente, con la popularización de herramientas para el desarrollo de imágenes, textos y documentos sintéticos. Un ejemplo es la manipulación de fotografías sobre accidentes con automóviles, individuos u otros para defraudar a compañías de seguros. Otro fraude de bajo nivel que se ha detectado es el uso de estas mismas herramientas para crear facturas falsas y defraudar a la hacienda pública, así como a personas físicas y jurídicas.
- **Fraudes bancarios y financieros predictivos.** Forma sofisticada de manipulación de mercados financieros usando IA para detectar vulnerabilidades, anticipar movimientos, simular comportamientos legítimos para evadir controles, manipular el mercado, operar fraudulentamente (**trading algorítmico malicioso**) y explotar el comportamiento de usuarios, mercados y empresas con fines ilícitos. En terminología de mercados financieros, la IA ha permitido automatizar el **spoofing** y **layering** *(AI-driven market spoofing* y *AI-driven layering)*. El spoofing es la realización de órdenes de compra o venta con intención de cancelarlas poco después sin que sean realmente ejecutadas pero que permiten manipular el mercado temporalmente, creando una falsa impresión de demanda o oferta. El layering es más elaborado que el spoofing y se realiza con la realización de múltiples órdenes a distinto precio para crear una falsa sensación de gran volumen de operaciones y gran interés en los activos.

Lavado de activos. Desde el uso de algoritmos que optimizan rutas de transacciones en criptomonedas para ocultar trazas, hasta modelos de IA que generan patrones de transacciones aparentemente legítimas para disfrazar fondos de procedencia ilícita, pasando por el uso de bots y herramientas para automatizar transferencias en múltiples jurisdicciones de modo regular con la finalidad de explotar lagunas regulatorias y dificultar la trazabilidad. Estos ejemplos del uso de la IA para el lavado de activos implican el uso de algoritmos, sistemas de aprendizaje autónomo o herramientas automatizadas para ocultar el origen de fondos, facilitar transacciones encubiertas o eludir sistemas de detección de lavado. En este sentido, se han dado casos reales del uso de mezcladores de criptomonedas (mixers) con algoritmos de IA para ocultar transacciones en blockchains.[21]

Manipulación de crédito y seguros. Uso de herramientas de IA, principalmente modelos de redes generativas antagónicas (GANs) para alterar datos, engañar o manipular sistemas

[21] EUROPOL, UNA DE LAS LAVANDERÍAS CRIPTOMONEDAS MÁS GRANDES DE LA CUBIERTA SEXISTA LAVADA, 15 DE MARZO 2023, EN: HTTPS://WWW.EUROPOL.EUROPA.EU/MEDIA-PRESS/NEWSROOM/NEWS/ONE-OF-DARKWEBS-LARGEST-CRYPTOCURRENCY-LAUNDROMATS-WASHED-OUT

de evaluación u obtener beneficios ilícitos en el sector crediticio o de seguros mediante la falsificación de perfiles crediticios, la falsificación documental, el uso de algoritmos de IA para identificar vulnerabilidades en el sistema de scoring crediticio u otros sistemas.

Delitos contra las personas

Material de abuso sexual infantil mediante IA (MASI). La manipulación, producción y distribución de material de abuso sexual infantil creado parcial o completamente mediante IA Generativa está en aumento debido a su facilidad en producción, acceso y número de plataformas que lo permiten. Informes como la Evaluación de la amenaza del crimen organizado en Internet (IOCTA; 2025)[22] de Europol lo constatan, y operaciones como Cumberland,[23] apoyada por Europol arrestó a 25 sospechosos de formar parte de un grupo criminal organizado cuyos miembros distribuían imágenes sintéticas de menores producidas mediante IA. La falta de legislación específica para abordar este crimen es un desafío mayor para las autoridades de justicia y seguridad. El MASI incluye imágenes sintéticas, avatares generados por IA, vídeos falsos realistas y textos o historietas sexualizadas. Además, está directamente vinculada al **grooming** asistido por IA.

Delitos contra la intimidad y conductas de ciberviolencia. Delitos como la sextorsión automatizada, los deepfakes no consensuados (principalmente videos de pornografía falsa con rostros reales), el acoso automatizado como el cyberbullying, la difamación automatizada, el grooming o el stalking predictivo son conductas de ciberviolencia y contra la intimidad de las personas que han ido aumento en los últimos años amparadas por la disponibilidad de herramientas de IA. Las principales víctimas son Mujeres y niñas.

Delitos de hackeo

Los delitos de hackeo asistido mediante sistemas de IA aprovechan las capacidades de la IA para automatizar, escalar y perfeccionar sus ataques con la finalidad de evitar o complicar su detección, prevención y rastrero. Además, han surgido empresas con apariencia legítima que permiten de forma sencilla automatizar y descentralizar ciberataques mediante IA. Plataformas que llevan al máximo exponente el concepto de crimen como servicio (*crime-as-a-service* o *CaaS*) y se promocionan en el internet abierto además de en el darknet y el deepweb. Ejemplos de dichas empresas son Xanthoros AI, FunkSec o los Dark LLMs.

Uso de la IA para generar o potenciar código. Sistemas como Watsonx Code Assistant, Grok 4 o ChatGPT pueden corregir, reforzar o mejorar un código fuente de un malware. Su uso es posible por cualquier usuario registrado en las plataformas. Aunque la limitación de revisión, corrección, mejora y refuerzo de algoritmos es compleja y no puede discernir entre

[22] Europol (2025), Internet Organised Crime Threat Assessment – IOCTA: *Steal, deal and repeat – How cybercriminals trade and exploit your data*. European Union Agency for Law Enforcement Cooperation (EUROPOL). ISBN 978-92-9414-027-2. Doi: 10.2813/4926508

[23] Europol (2025), *25 arrested in global hit against AI-generated child sexual abuse material*. Disponible en: https://www.europol.europa.eu/media-press/newsroom/news/25-arrested-in-global-hit-against-ai-generated-child-sexual-abuse-material

buen código y código utilizado para ciberataques, es importante tenerlo en cuenta por el doble riesgo que existe. Por un lado, la infiltración en empresas y sistemas en su fase de diseño, infectando completamente la cadena de procesos y servicios de personas jurídicas; y, por otro, la automatización y perfeccionamiento de algoritmos, haciendo que su detección, prevención y represión sea más complicada. Sin embargo, hasta la actualidad, el código generado mediante modelos que se han entrenado con machine learning no son capaces del todo de desarrollar aspectos realmente complejos de un malware. Esta es una amenaza a medio y largo plazo con la que se debe estar preparado.

Ciberataques tradicionales sofisticados mediante IA:

- **Ataques de denegación de servicio – DDoS.** Las redes de bots impulsadas por IA pueden generar ataques más voluminosos y complejos, sobrecargando los sistemas objetivo. Así mismo, sistemas de IA pueden adaptar en tiempo real los ataques, analizar patrones de tráfico en la red y aprender a mimetizarlos para parecer legítimos.

- **Man-in-theMiddle (MitM)**. Ataque de interceptación de comunicaciones entre dos o más interlocutores con la finalidad de conocer o alterar las comunicaciones entre los individuos, lo que podría dar lugar a violaciones de datos, violaciones de la privacidad y pérdidas económicas. Una sofisticación actual es el **sniffing**, el cual consiste en capturar el tráfico de red que circula entre dos dispositivos con el objetivo de espiar, interceptar o robar información confidencial. La IA transforma la pasividad del sniffing tradicional a un proceso semiactivo, automatizado, flexible, inteligente y escalable.

- **Malware y ransomware.** El malware es cualquier código de software o programa informático, incluidos ransomware, troyanos y spyware, creado o escrito intencionadamente para dañar, obtener datos de los sistemas informáticos o de sus usuarios, robar credenciales o mantener rehenes a dispositivos con fines de obtención de importantes beneficios. A diferencia del malware tradicional, el malware con IA adapta su comportamiento para evitar detección, es decir, es polimórfico. En 2023, investigadores de ciberseguridad de HYAS publicaron la prueba de concepto de EyeSpy, una cepa de malware totalmente autónoma con IA que, según dijeron, puede razonar, elaborar estrategias y ejecutar ciberataques por sí sola.[24]

- La principal diferencia entre el malware y el ransomware es la especificidad del ransomware para retener como rehenes los datos confidenciales o dispositivos de una víctima, amenazando con su borrado, su inacceso o la venta de los mismos a terceros si no paga un rescate específico. En la actualidad, algunos de los ransomwares automatizados con IA se focalizan en buscar y mantener objetivos valiosos. Según el Índice de Inteligencia sobre Amenazas de 2025 de IBM X-Force, los ransomware son el

[24] Jeff Sims (2023), *Introducing EyeSpy: A Cognitive Threat Agent*. Hayas. Disponible en: https://www.hyas.com/blog/eyespy-proof-of-concept

28% de los casos de malware identificados.[25] En febrero de 2024, Change Healthcare, una filial de UnitedHealth Group y uno de los principales procesadores de reclamaciones médicas de Estados Unidos, fue víctima de un ataque de ransomware. Los atacantes, el grupo BlackCat (ALPHV), se infiltraron en los sistemas de la empresa. Robaron datos confidenciales e instalaron un ransomware que paralizó las operaciones. El impacto económico se ha calculado en 2 mil 870 millones de dólares.[26]

Delitos vinculados al uso de sistemas y vehículos autónomos

EL uso de sistemas autónomos como vehículos autónomos, armas autónomas o herramientas de ataque cibernético autónomas representa una categoría emergente de delitos asistidos mediante IA. Gracias a algoritmos y sistemas de ML, así como de la incorporación de procesadores de recopilación, análisis y proceso de datos masivos a tiempo real, estas herramientas están diseñados para operar con cierta autonomía. Su uso en actividades delictivas como robos materiales, robo de datos, transporte de mercancías ilícitas, sabotajes, ataque a infraestructuras críticas o asesinatos selectivos se han incrementado en los últimos años.

Vehículos autónomos. La utilización de vehículos autónomos aéreos, terrestres, acuáticos y subacuáticos que utilizan sistemas de IA para algún tipo de funcionalidad es una realidad a raíz de la guerra en Ucrania. Estos sistemas están en constante evolución y el crimen organizado en América Latina y el Caribe, aunque también en Europa, lo emplea con distintas finalidades que cubren desde el transporte de droga mediante drones o enjambres de drones. La Junta Internacional de Fiscalización de Estupefacientes (JIFE) de las Naciones Unidas ya alertaba del uso de drones para el tráfico de droga, pero también para vigilar rutas de transporte. Países como Estados Unidos, México, Colombia, España y Francia ya han comunicado incidentes.[27] Recientemente la Armada colombiana capturó un narcosubmarino no tripulado y completamente autónomo equipado con una antena Starlink que podía transportar hasta 1.500 kg de droga u otra carga.[28]

Además, los cárteles de droga mexicanos han sido pioneros en el uso de vehículos aéreos no tripulados con una doble finalidad. Por un lado, el tráfico de droga entre México y Estados Unidos, donde la Patrulla Fronteriza estadounidense tiene registros del uso de unos 155 mil drones por parte del crimen organizado; y, por otro, su uso para el transporte y lanzamiento de explosivos o armas químicas y ataque a población civil, militar y de grupos criminales rivales. En este sentido, el Cartel de Jalisco Nueva Generación ha conformado

[25] IBM X-Force (2025), *Índice de Inteligencia sobre Amenazas de 2025: transformando ciberdefensa en ciberresiliencia*. IBM Institute for Business Value. Disponible en: https://www.ibm.com/thought-leadership/institute-business-value/report/2025-threat-intelligence-index

[26] Zack, Whittacker (2025), *How the ransomware attack at Change Healthcare went down: A Timeline*, Techcrunch, January 27, 2025. disponible en: https://techcrunch.com/2025/01/27/how-the-ransomware-attack-at-change-healthcare-went-down-a-timeline/

[27] Naciones Unidas (2025), *Junta Internacional de Fiscalización de Estupefacientes*, Informe 2024. ISBN 978-92-1-107118-4. Disponible en: https://www.incb.org/documents/Publications/AnnualReports/AR2024/Annual_Report/E-INCB-2024-1-SPA.pdf

[28] Pascual Estapé, J.A. (2025), Interceptan el primer narcosubmarino autónomo que usa los satélites Starlink para orientarse. 20 minutos – Computer Hoy. Disponible en: https://computerhoy.20minutos.es/tecnologia/primer-narcosubmarino-autonomo-usa-satelites-starlink-orientarse-1471183

una unidad especializada de control y desarrollo de drones llamada “Operadores Droneros”.[29]

Sistemas de armas de fuego autónomas. Los sistemas de armas letales autónomas (LAWS, por sus siglas en inglés), puede tomar decisiones sin intervención humana y realizar ataques en remoto. La utilización de sistemas de fuego autónomas está bien documentada, principalmente, en México, donde los carteles los utilizan junto a vehículos civiles blindados improvisados (narcotanques) con finalidades de ataque a otros grupos criminales o contra autoridades de seguridad y defensa.[30]

Delitos contra la propiedad intelectual

Plagio asistido por IA. Uso de herramientas de IA, principalmente IA Generativa como modelos de lenguaje, generadores de texto, imagen o software de reescritura, para copiar, parafrasear o reproducir obras protegidas por derechos de autor sin autorización, presentándolas como propias o sin dar el debido crédito. La generación de contenido o productos derivados, así como la creación de obras híbridas, sin citar fuentes ni tener las autorizaciones correspondientes también se considera delito de plagio asistido por IA. La generación de texto, imagen o software de reescritura puede realizarse con modelos de lenguaje como ChatGPT o GROK para generar texto, DALL-E y MidJourney para imágenes o vídeos, y QuillBot o SpinBot para parafrasear contenido y la reescritura.

Falsificación de productos. Delito vinculado a la propiedad intelectual, la falsificación de productos mediante herramientas de IA implica la creación, distribución o comercialización de productos falsificados que imitan marcas registradas, diseños protegidos o bienes originales, con el objetivo de engañar a consumidores y obtener beneficios ilícitos. Si bien la falsificación se da más en productos textiles y de lujo, también se puede dar en productos farmacéuticos o incluso en diseños de materiales o componentes, teniendo una relación directa con el **espionaje industrial**.

3.2. DESAFÍOS JURÍDICOS: RESPONSABILIDAD DE PERSONAS FÍSICAS Y JURÍDICAS

La inteligencia artificial presenta multitud de desafíos y retos, algunos de los cuales ya se han mencionado en este documento, principalmente aquellos desafíos vinculados a los delitos cometidos, facilitados o sofisticados mediante IA. No obstante, existen multitud de desafíos que no se han tratado vinculados a la actualización normativa y reglamentaria requerida debido al surgimiento constante de nuevas tecnologías; adaptabilidad de la sociedad y de sus instituciones; creación de capacidades, conocimientos y habilidades

[29] Bayoud, A. (2025), *'Narcodrones': la nueva amenaza criminal en México*. France 24. Disponible en: https://www.france24.com/es/am%C3%A9rica-latina/20250616-narcodrones-la-nueva-amenaza-criminal-en-m%C3%A9xico
[30] Ziemer, H. (2025), *Illicit Innovation: Latin America Is Not Prepared to Fight Criminal Drones*. Center for Strategic and International Studies. Disponible en: https://www.csis.org/analysis/illicit-innovation-latin-america-not-prepared-fight-criminal-drones

(blandas y duras) en materia de IA y desarrollo tecnológico claves; capacidades de asimilación por parte de la sociedad, las empresas y la administración pública en cuanto a innovación y nuevas tecnologías; o la introducción y uso de la misma IA dentro tanto el sector público como privado, entre otras.

Uno de los temas menos tratados y más complejos à abordar es el desafío jurídico que representa la IA en materia de responsabilidad civil, penal y administrativa de las personas físicas y jurídicas.

Si bien en la actualidad los sistemas de IA no tienen voluntad ni consciencia, son parcialmente incapaces de tomar decisiones, carecen de intencionalidad (requisito de *mens rea*) como un ser humano puesto que no se ha llegado a desarrollar plenamente la IA General y, generalmente, siempre hay una acción humana directa o indirecta responsable de su creación, desarrollo y mantenimiento, la cuestión de la propia responsabilidad penal de la IA se dirige más hacia quién puede ser penal, civil y administrativamente responsable por un problema o delito cometido mediante IA.

En consecuencia, bajo la pregunta de si actualmente la "IA como sistema" puede ser penalmente responsable, la respuesta más directa es "no", ya que no posee consciencia, voluntad ni responsabilidad moral, y, por ende, no puede recibir sanción penal. Sin embargo, este es un aspecto que deberá ser revisado a medio y largo plazo debido a la evolución prevista de los modelos y sistemas de IA y la llegada de la IA Generativa. En este sentido, es posible que se deba analizar la posible existencia de responsabilidades legal limitada o la existencia de una personalidad jurídica electrónica, u otros mecanismos distintos. [31]

Nótese que la cuestión actual de la responsabilidad de la IA se centra exclusivamente en aquellos mecanismos y delitos donde interviene la IA con asistencia de una persona física o jurídica. La reciente evolución vinculada a Agentes de IA (*AI Agents* o *AI Agentics*) podría quedar fuera de este análisis si bien algunos de los Agentes de IA aún requieren una mínima intervención humana. En este sentido, es importante tener en cuenta que la interacción entre Agentes de IA sin interacción humana está en fase de experimentación y evolución, dando resultados realmente prometedores en 2025.

A la pregunta de si los diseñadores, desarrolladores, usuarios y operadores pueden tener responsabilidad penal por actos o delitos cometidos por sistemas de IA, la respuesta es "depende". Este aspecto dependerá de cada legislación nacional o regional.

Consecuentemente, uno de los principales desafíos es identificar al sujeto activo del delito cuando el acto es ejecutado por un sistema autónomo. En otras palabras, ¿quién puede ser el sujeto penalmente responsable? En estos casos, las opciones más consideradas son:

[31] Combarros Merino, Roberto. (2023), *Vehículos autónomos e inteligencia artificial: responsabilidad civil y productos defectuosos*. Universidad de León. Máster en Derecho de la Ciberseguridad y Entrono Digital. Disponible en: https://buleria.unileon.es/bitstream/handle/10612/17381/Combarros_Merino_Roberto.pdf?sequence=1

- Diseñadores y desarrolladores: en caso de que actuaran con negligencia o dolo en el diseño, entrenamiento o supervisión de un algoritmo, modelo o sistema de IA; o si se hubieran creado deliberadamente sistemas con funcionalidades delictivas, por ejemplo un bot para estafar o el desarrollo de plataformas que ofrecen y venden servicios (CaaS) de modo explícito con los que puedes cometer delitos como ocurre con las plataformas Xanthoros AI o FunkSec, anteriormente mencionadas.

- Usuarios, operadores: estos pueden ser responsables si se hace un uso indebido de sus sistemas, hubo una falta de supervisión o no se establecieron límites específicos para prevenir o dificultar el delito. Ejemplos se pueden encontrar en la responsabilidad de usuarios y operadores en la producción de material de abuso sexual infantil (MASI), deepfakes para manipular información o procesos electorales, lanzar ataques específicos o cometer homicidios (ejemplo de vehículos autónomos que identifican y eliminan objetivos).

- Responsabilidad de la persona jurídica (empresas proveedoras o plataformas): cuando se demuestre que una persona jurídica se ha beneficiado del delito, haya tolerado o facilitado el mismo, o incluso cuando no haya establecido medidas de control y prevención.

En el caso de la Unión Europea, la responsabilidad penal autónoma de la IA no existe, pero sí que podría existir cierta responsabilidad penal para quien utilice una herramienta y cometa un delito vinculado a, por ejemplo, la producción y distribución de material sintético de abuso sexual a menores, o deepkfakes vinculados a ciberviolencia o contra la intimidad.

El Reglamento de IA de la Unión Europea prohíbe ciertos usos maliciosos de la IA, establece un anexo específico para clasificar los sistemas de IA según su riesgo (inaceptable, alto, limitado y mínimo)[32] pero no crea responsabilidad autónoma de la IA. Lo que sí hace es poner de relieve la necesidad de regular la responsabilidad civil y administrativa de la IA sin entrar en mayor detalle. En este sentido, en septiembre de 2022, la Comisión Europea presentó un paquete de iniciativas que busca establecer una nueva normativa al respecto y facilita la interposición de demandas de responsabilidad civil subjetiva por daños y perjuicios. La propuesta de Directiva UE sobre responsabilidad en materia de IA[33] viene acompañada por la revisión de la Directiva sobre responsabilidad por los daños causados por productos defectuosos (85/374).

La Directiva de la UE sobre responsabilidad en materia de IA clasifica los sistemas de IA en dos grandes grupos parecidos al Anexo III del Reglamento Europeo de IA pero más simples. Por un lado, sistemas de alto riesgo (aquellos que tienen o pueden tener un impacto significativo en derechos fundamentales o que se utilizan en sectores críticos); y, por otro,

[32] Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial. Anexo III : Sistemas de IA de alto riesgo, Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32024R1689

[33] Comisión Europea (2022), Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la adopción de normas de responsabilidad civil extracontractual a la inteligencia artificial (Directiva sobre responsabilidad en materia de IA). COM(2022) 496 final | 2022/0303 (COD). Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52022PC0496

sistemas de uso general. Así mismo, la Directiva introduce la presunción de causalidad como elemento innovador, ya que se presumiría que, en caso de que un sistema de IA provoque daños, el responsable sería el desarrollador, el host o el usuario del sistema, a menos que demuestre lo contrario. Esto llevaría a la necesidad de que los diseñadores, creadores, fabricantes, operadores, hosts y usuarios contraten pólizas de seguro específicas que les cubran de posibles daños.

Si bien se ha avanzado técnicamente en aspectos de responsabilidad en materia de IA, de momento las propuestas normativas no han sido aprobadas ni en la Unión Europea ni en otro país conocido.

A modo de conclusión, existen desafíos vinculados al propio establecimiento de la responsabilidad, sea penal, civil o administrativa, en complejos modelos de IA debido a su naturaleza de "caja negra" ya que en muchos casos puede ser sumamente complicado determinar por qué el sistema actuó de esa forma, sobre todo cuando hablamos de discriminaciones, de actuaciones sesgadas o de decisiones autónomas sin (casi) interacción humana. Así mismo, en los desafíos también existe la complejidad de atribuir la responsabilidad a una o varios entes, ya sean personas físicas o jurídicas. Por ejemplo, en casos de producción de material de abuso sexual a menores, deepfakes sexuales o incluso automatización y perfeccionamiento de software para phishing, la responsabilidad penal puede recaer en tanto el operador, la plataforma que hospeda, el diseñador y creador del algoritmo inicial, ninguno de estas personas o todos a la vez.

4. ANÁLISIS COMPARADO EN MATERIA NORMATIVA E INICIATIVAS EN PAÍSES FUERA DE CENTROAMÉRICA Y EL CARIBE

4.1. ANÁLISIS COMPARATIVO DE LA NORMATIVA EN LOS PAÍSES DEL FOPREL EN MATERIA DE IA Y ASPECTOS DIGITALES

4.1.1. INTELIGENCIA ARTIFICIAL

País	Legislación penal vigente	Mención explícita de IA	Estrategia nacional de IA	Adhesión a foros e iniciativas internacionales en materia de IA	Observaciones sobre IA
Belice	Código penal (Edición revisada, 2000)	No	No, pero tiene una Estrategia industrial con IA	En octubre de 2023, Belice aprobó la firma de la Declaración de Santiago que busca impulsar un consejo regional para promover el diseño y despliegue de sistemas de IA basados en la ética, derechos humanos y dignidad.	Vacío normativo respecto a IA.
Costa Rica	Código Penal (1970) – Reformado	No	Estrategia Nacional de Inteligencia Artificial 2024-2027 (aprobada en 2024)	Parte de la Declaración de Santiago para promover una IA ética en América Latina y el Caribe (2024). Firmante de la Declaración de Montevideo "Para la construcción de un enfoque regional sobre la gobernanza de la Inteligencia Artificial y sus impactos en nuestra sociedad (2024).	El país más avanzado en marco ético de IA. Presentadas tres iniciativas legislativas para tipificar delitos cometidos mediante sistemas de IA. La Estrategia Nacional de IA incluye la implementación de *sandbox* regulatorios (apoyados por la Delegación de la UE en Costa Rica), creación de un Centro Nacional de Excelencia en IA, y mecanismos de monitoreo y evaluación. En marzo de 2025, 120 académicos costarricenses publicaron una carta abierta instando al Ejecutivo y al Congreso a actuar

					con urgencia en materia de IA con la creación de una Agencia Nacional de IA y un marco regulatorio sólido sin frenar la innovación.
El Salvador	Código Penal (1997)	No	No	Parte de la Declaración de Santiago para promover una IA ética en América Latina y el Caribe (2023). Firmante de la Declaración de Montevideo "Para la construcción de un enfoque regional sobre la gobernanza de la Inteligencia Artificial y sus impactos en nuestra sociedad (2024).	Define delitos informáticos, pero sin prever autonomía de sistemas ni mención a la IA.
Guatemala	Código Penal (1973) – Reformado	No	No	Parte de la Declaración de Santiago para promover una IA ética en América Latina y el Caribe (2023).	No considera delitos cometidos mediante IA
Honduras	Código Penal (2019)	No	No	Parte de la Declaración de Santiago para promover una IA ética en América Latina y el Caribe (2023). Firmante de la Declaración de Montevideo "Para la construcción de un enfoque regional sobre la gobernanza de la Inteligencia Artificial y sus impactos en nuestra sociedad (2024).	Avance importante en ciberseguridad, pero IA no es mencionado
México	Código Penal Federal	No	Estrategia Nacional de IA (2018). Propuesta de revisión por parte de la Alianza Nacional de IA – ANIA en 2024	Parte de la Declaración de Santiago para promover una IA ética en América Latina y el Caribe (2023). Firmante de la Declaración de Montevideo "Para la construcción de un enfoque regional sobre la gobernanza de la Inteligencia Artificial y sus impactos en nuestra sociedad (2024).	Discusión activa en Senado sobre ética y regulación de IA. Código Penal Federal: se han presentado iniciativas para incluir capítulos que penalicen deepfakes, fraudes, suplantación, extorsión y contenido sexual generado con IA — artículos propuestos 211 Bis-8 y 211 Bis-9; otra reforma propone aumento de penas en extorsión con IA a 15–22 años Códigos penales estatales: Sinaloa y Nayarit: sancionan manipulación de contenido íntimo mediante IA (Art. 185 Bis C y Art. 297 Ter), con penas de 3–6 años y multa Quintana Roo: el Art. 20 Bis establece aumento de penas (hasta 50 %) si delito se comete con IA.

Nicaragua	Código Penal (2008)	No	No		Enfocada en control de contenido digital, pero no en IA. No obstante, tanto el Acuerdo Administrativo 004-2020 como la Ley Especial de Ciberdelitos podrían ser utilizados para el monitoreo de empresas que desarrollen y ofrezcan servicios de IA
Panamá	Código Penal (2007)	No	No	Firmante de la Declaración de Montevideo "Para la construcción de un enfoque regional sobre la gobernanza de la Inteligencia Artificial y sus impactos en nuestra sociedad (2024).	Discusión activa sobre regulación, pero sin tipo penal aún. Proyecto de Ley de IA en trámite.
República Dominicana	Código Penal (en revisión)	No	Estrategia Nacional de Inteligencia Artificial – Versión 1.0 de octubre de 2023	Parte de la Declaración de Santiago para promover una IA ética en América Latina y el Caribe (203). Firmante de la Declaración de Montevideo "Para la construcción de un enfoque regional sobre la gobernanza de la Inteligencia Artificial y sus impactos en nuestra sociedad (2024). Hospedará la Tercera Cumbre ministerial sobre IA (octubre de 2025).	Avances en ciberdelito, pero sin abordar IA el ámbito penal. En 2023 se propuso actualizar legislación penal.

4.1.2. EN MATERIA DIGITAL (CIBERDELITOS, CIBERSEGURIDAD, PROTECCIÓN DE DATOS)

País	Reformas Digitales Recientes	Convención de Budapest sobre Ciberdelincuencia	Segundo Protocolo adicional de la Convención de Budapest	Protección de datos	Observaciones en materia digital
Belice	Agenda Digital Nacional 2022–2025, institucionalizando las iniciativas de e-Gobierno y ciberseguridad bajo el	No, pero su *Cybercrime Act* está alineada con la	No.	La Ley de Protección de Datos de Belice de 2021 (*Data Protection Act*) regula la recogida, el uso y la difusión de datos	En 2025, la Oficina del Primer Ministro y el Ministerio de Inversiones lanzaron la

	Ministerio de E-gobernanza. Sin mencionar explícitamente la IA, la agenda incluye proyectos que promueven la aplicación estratégica de nuevas tecnologías en el ámbito público. Desde 2020, cuenta con una unidad policial especializada (PITCU) en ciberdelitos y ha resultado en la aprobación de la *Cybercrime Act* 2020, alineada con la Convención de Budapest, así como la Estrategia Nacional de Ciberseguridad y Cibercrimen (2020).	Convención de Budapest.		personales. Establece principios para el tratamiento de datos personales, describe los derechos de los interesados e impone obligaciones a los responsables y procesadores de datos. La Ley también aborda las restricciones a la transferencia de datos, los mecanismos de aplicación y las sanciones en caso de infracción.	primera Política y Estrategia Global de Inversión en Servicios Digitales de Belice, centrada en el proyecto de Economía Naranja, con el apoyo del Banco Interamericano de Desarrollo (BID). La iniciativa busca impulsar el sector de la IA y de tecnologías para dar valor añadido a su economía vinculada a *outsourcing*.
Costa Rica	Ley 8148 de 2001 que se adiciona al Código Penal de Costa Rica. En 2012, se reformó la Sección VIII, Delitos Informáticos y Conexos del Título VII del Código Penal que modifica los artículos 167, 196, 196 bis, 214, 217 bis, 229 bis y 288 para aumentar las sanciones o penalizaciones (Ley 9048 de 2012).	Ratificada.	Signatario del Segundo Protocolo (13/06/2022). No ratificado.	Ley N°8968, Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales, publicada en el Diario Oficial La Gaceta el 5 de septiembre de 2011. Esta ley establece los derechos de las personas sobre sus datos personales y las obligaciones de quienes los tratan, prohíbe el tratamiento de datos sensibles y establece medidas de seguridad.	
El Salvador	Ley Especial contra Delitos Informáticos (2016). En la reforma de 2022 (Decreto N. 260) se incorporó el tratamiento de la evidencia digital para procesos judiciales.	No.	No.	Ley de Protección de Datos Personales (Decreto No. 144 de 2024). La Agencia de Ciberseguridad del Estado se encarga de controlar, inspeccionar, supervisar, sancionar y resolver controversias vinculadas a la aplicación de la Ley de Protección de Datos Personales.	El Salvador ha creado la Agencia de Ciberseguridad del Estado para supervisar la aplicación de estas leyes y emitir lineamientos para su cumplimiento.
Guatemala	Código Penal, Art. 274 (A-G), regula los delitos informáticos en donde se prevé la alteración, destrucción, manipulación, de registros o programas informáticos y el uso de información y utilización de programas destructivos.	Signatario. Invitado a ser parte. Estatuto de país observador.	No.	No existe una ley específica de protección de datos personales que abarque tanto el sector público como el privado. Sin embargo, la Ley de Acceso a la Información Pública (Decreto 57-2008) aborda parcialmente la protección de datos	

	Ley de Prevención y Protección contra la Ciberdelincuencia, aprobada mediante el Decreto 39-2022. Esta Ley fue aprobada por el Congreso de la Republica de Guatemala el 4 de agosto de 2022, pero suscito controversia y críticas por supuestas restricciones a la libertad de expresión y fue archivada.			personales al garantizar el derecho a conocer y proteger los datos personales de los ciudadanos en archivos estatales.	
Honduras	Ley Especial de Ciberdelitos (2020).	No.	No.	Ley de Transparencia y Acceso a la Información Pública (2006), es la herramienta principal que busca hacer efectiva la transparencia y garantizar la protección, clasificación y seguridad de la información pública, estableciendo también restricciones al acceso a la información de datos personales. En 2013, reforma al artículo 182 de la Constitución de la República en la cual el Estado reconoce la garantía del *Hábeas Data.*	
México	México incorporó una reforma en materia penal en junio de 2018 para castigar el delito de grooming (Art. 199 Septies Código Penal Federal) El Congreso mexicano publicó la *Ley contra el acoso digital*, mejor conocida como la *'Ley Olimpia'* la cual entró en vigor el 2 de junio de 2021 y por medio de la cual se reforman diversas disposiciones de la *Ley General de Acceso a las Mujeres a una Vida Libre de Violencia* y del Código Penal Federal y se tipifican como delito el divulgar, compartir, distribuir y publicar imágenes, videos o audios con contenido íntimo sexual de una persona	Signatario. Invitado a ser parte. Estatuto de país observador.	No.	Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP de 2025). La ley impone estándares de legalidad, transparencia, seguridad y responsabilidad proactiva. El nuevo Reglamento de la LFPDPP de 2025 se encuentra en proceso de elaboración. Desde 2025, la Secretaría Anticorrupción y Buen Gobierno, es la nueva autoridad encargada de la protección de datos personales.	Propuesta de reforma de la Ley Federal del Derecho de Autor con objeto de adaptarla a nuevas tecnologías y garantizar protección en el entorno digital. Esto incluiría el uso por parte de tecnológicas por parte de sus herramientas de IA así como de los resultados producidos.

	adulta sin su consentimiento (Art. 199 Octies Código Penal Federal) e incluso cuando las imágenes, videos o audios de contenido íntimo sexual que se divulguen, compartan, distribuyan o publiquen no correspondan a la persona que es señalada o identificada en los mismos (Art. 199 Nonies Código Penal Federal). No se hace mención explícita a la IA.				
Nicaragua	Ley General de Telecomunicaciones y Servicios Postales, Ley N°200 (1995), la cual establece un marco general institucional y jurídico que permite la regulación del sector de las telecomunicaciones. Con el Acuerdo Administrativo 004-2020 se reformó la Ley General para ampliar el control sobre las empresas encargadas de ofrecer servicios digitales y de telecomunicaciones. Ley Especial de Ciberdelitos (Ley 1042, 2020) objeto de prevenir, investigar, perseguir y sancionar los delitos cometidos "por medio de las tecnologías de la información y la comunicación, en perjuicio de personas naturales o jurídicas".	No.	No.	Ley de Protección de Datos Personales – Ley N°787 (2012).	Ley Especial de Ciberdelitos.
Panamá	Ley 61 de 2024 que "modifica y adiciona artículos al Código Penal y a la Ley 11 de 2015, sobre asistencia jurídica internacional en materia penal, y dicta otras disposiciones respecto a medidas contra la ciberdelincuencia, incluyendo suplantación, abuso infantil, acceso indebido y difusión no consentida de material íntimo.	Ratificada.	No.	Ley de Protección de Datos Personales de Panamá – Ley 81 de 26 de marzo de 2019, complementada por el Decreto Ejecutivo 285 de 28 de mayo de 2021, que la reglamenta. El Decreto define conceptos, requisitos de consentimiento, y derechos de los titulares, establece protocolos internos, evaluaciones de impacto y registros obligatorios, regula	

				transferencias internacionales de datos y sanciones administrativas, y establece la figura del Oficial de Protección de Datos.	
República Dominicana	Ley 53-07 sobre Crímenes y Delitos de Alta Tecnología.	Ratificada.	Signatario del Segundo Protocolo (30/01/2023). No ratificado.	Ley No. 172-13 (2013) sobre Protección de Datos Personales. Objetivo de proteger los datos personales de los ciudadanos en archivos, registros públicos y bancos de datos, así como garantizar que no se lesione el derecho al honor y a la intimidad de las personas, y también facilitar el acceso a la información que sobre las mismas se registre.	

4.2. OTRAS LEGISLACIONES VINCULADAS A LA IA A NIVEL INTERNACIONAL

Consejo de Europa

- El **Convenio Marco del Consejo de Europa sobre inteligencia artificial, derechos humanos, democracia y Estado de Derecho**[34] es el primer tratado internacional vinculante que regula el uso de la IA con un enfoque centrado en los derechos humanos, la democracia y el Estado de Derecho. Promueve el progreso y la innovación en IA, a la vez que gestiona los riesgos que puede plantear.

- Adoptado por el Consejo de Europa el 17 de mayo de 2024 y abierto a la firma desde el 5 de septiembre de 2024, este convenio busca establecer principios y obligaciones comunes para garantizar que los sistemas de IA sean éticos y respeten los valores fundamentales. Argentina, Costa Rica, México y Perú formaron parte de los 11 Estados no miembros del Consejo de Europa que participaron en las negociaciones del tratado. Este convenio ha sido firmado por 15 países y la Unión Europea, pero aún no ha entrado en vigor.

-

Unión Europea

- El **Reglamento de Inteligencia Artificial de la Unión Europea** (REIA, Ley de IA o *EU AI Act*)[35], aprobado en mayo de 2024 y publicado en el Diario Oficial de la UE el 12 de julio de 2024, es la primera legislación integral sobre IA a nivel mudial. Entró en vigor el 1 de agosto de 2024 y tiene un enfoque basado en riesgos para regular el desarrollo, despliegue y uso de sistemas de IA en la UE.

  La Ley de IA garantiza que los europeos puedan confiar en lo que la IA tiene para ofrecer. Si bien la mayoría de los sistemas de IA presentan un riesgo limitado a cero y pueden contribuir a resolver muchos desafíos sociales, ciertos sistemas de IA crean riesgos que debemos abordar para evitar resultados indeseables. Dichos riesgos se mencionan en su Anexo III, el cual comprende cuatro tipos o categorías de riesgo según el tipo de IA y su uso a los que se refiere el Artículon 6 Apartado 2 del mismo REIA: riesgo inaceptable, riesgo alto, riesgo limitado y riesgo mínimo.

  En materia penal, la Comisión Europea lanzó una propuesta de directiva refundida sobre abuso y explotación sexual de menores, que incluye medidas para armonizar las definiciones y sanciones de los delitos en los países de la UE, abarcando también

[34] Consejo de Europa (2024), El Convenio Marco del Consejo de Europa sobre inteligencia artificial, derechos humanos, democracia y Estado de Derecho (CETS No. 225). Disponible en: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=225

[35] Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial, Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32024R1689

las actividades en el ciberespacio. En mayo de 2025 se incluyeron enmiendas por parte de la Comisión de Libertades Civiles del Parlamento Europeo con la finalidad de eliminar los plazos de prescripción para que las víctimas tengan tiempo de denunciar, así como el desarrollo de mecanismos de justicia y apoyo adaptados a la infancia. La directiva refundida aún debe pasar el trámite de discusiones entre el Consejo europeo y el Parlamento Europeo para que pueda, en algún momento, ser aprobada y entrar en vigor.[36]

- En Francia, la **Ley SREN** (*Loi Visant à Sécuriser et à Réguler l'Espace Numérique* - Loi n° 2024-449 del 21 de mayo de 2024), busca regular el entorno digital, proteger a los menores de la pornografía en línea y combatir el fraude en línea. En este sentido, la Ley SREN adapta o transpone el Reglamento europeo de Servicios Digitales (*Digital Services Act* – DSA) y el Reglamento europeo de Mercado Digital (*Digital Markets Act* – DMA) al ordenamiento francés. Además, como parte de la Ley SREN, Francia prohíbe explícitamente el intercambio no consentido de contenidos deepfake, a menos que sea obvio que el contenido se ha generado artificialmente.

- Los deepfakes y contenidos generados con IA se incorporan como nuevo delito penal (art. 226-8 CP): difusión de contenido IA sin consentimiento, con hasta 2 años de prisión y 45 000 € de multa. En materia sexual, aumento a 3 años y 75 000 €.

-

Reino Unido

- **Ley de seguridad en internet** (*Online Safety Act*) de 2023 penaliza la difusión de imágenes íntimas no consensuadas, incluyendo los deepfakes o imágenes y vídeos (semi)sintéticos, bajo la sección 66B. La ley ha tenido ciertas limitaciones y, en la actualidad, existe una propuesta de enmienda[37] al proyecto de ley de justicia penal para declarar ilegal la creación de deepfakes.

-

Estados Unidos

- En la actualidad no existe un marco federal unificado, como tal pero sí una aproximación sectorial para regular la responsabilidad derivada del uso malicioso de IA. Un ejemplo de ello es la recientemente aprobada "**Take It Down Act**".

  Aprobada en junio de 2025, la Take It Down Act introduce distintos elementos fundamentales como: i) prevé como delito federal distribuir o amenazar con distribuir imágenes íntimas sin consentimiento; ii) penalización con penas de prisión para cualquier persona que difunda y distribuya imágenes sexualmente explícitas sin consentimiento, ya sean reales o generadas por inteligencia artificial;

[36] Comisión Europea, *Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y el material de abuso sexual de menores y por la que se sustituye la Decisión marco* 2004/68/JAI del Consejo (versión refundida). COM(2024) 60 final. 2024/0035 (COD). https://eur-lex.europa.eu/resource.html?uri=cellar:a0335235-c5be-11ee-95d9-01aa75ed71a1.0020.02/DOC_1&format=PDF

[37] Criminal Justice Bill (2024). https://bills.parliament.uk/bills/3511

iii) responsabilidad civil para las empresas o plataformas que alojen el contenido producido y no lo eliminen en un plazo de 48 horas tras la notificación por parte de la víctima; iv) establece mecanismos para que las víctimas puedan denunciar la distribución de imágenes íntimas no consentidas y solicitar su eliminación de forma anónima, con protecciones contra represalias; y, v) exige que las plataformas realicen esfuerzos razonables para eliminar las copias de las imágenes.

RECOMENDACIONES PARA LOS PAÍSES DEL FOPREL

Aspectos generales

- La evolución de los sistemas de inteligencia artificial exige **respuestas normativas específicas** que garanticen la seguridad jurídica, la protección de derechos y la adecuada imputación penal. América Central, México y la cuenca del Caribe carecen de normativas penales específicas frente al fenómeno emergente de la inteligencia artificial como herramienta delictiva. Avanzar conjuntamente en este aspecto sería de mayor relevancia dado el crecimiento exponencial en el uso de herramientas de IA que están siendo utilizadas con propósitos delictivos por grupos del crimen organizado.
- El FOPREL debe jugar un papel clave como promotor de **armonización legislativa supranacional**, en consonancia con tratados y estándares internacionales sobre ciberdelito, privacidad y derechos digitales.
- Se recomienda avanzar hacia una **reforma penal regional coordinada**, que considere lo siguiente:
    - **Adaptar tipos clásicos** (fraude, sabotaje, daños informáticos, acceso ilícito, acoso, et.al.) para incluir medios automatizados o digitales avanzados.
    - **Incorporar agravantes** por el uso de IA, cuando el sistema haya potenciado el alcance, daño o anonimato del delito.
    - **Creación de nuevos tipos penales** (desarrollo y uso de vehículos autónomos, deepfakes)
    - El fortalecimiento de la **responsabilidad corporativa**
    - La promoción de **estándares técnicos mínimos** para el desarrollo y uso seguro y responsable de la IA.
- Se recomienda iniciar un **proceso legislativo participativo**, con consulta a expertos técnicos, juristas, academia y organizaciones civiles, para actualizar el marco penal frente a los riesgos emergentes de la IA. La creación de una **Comisión permanente de personas expertas nacionales e internacionales en materia de IA y delito** con la finalidad de abordar retos en la tipificación y la evolución constante del delito cometido, apoyado, fortalecido o automatizado mediante herramientas de IA.
- Es fundamental incluir disposiciones sobre **transparencia algorítmica, explicabilidad y trazabilidad**, así como criterios objetivos para imputar responsabilidad en entornos automatizados. La transparencia algorítmica es clave para entender, en el marco de un proceso penal, las decisiones tomadas por los sistemas de IA.

- Fortalecer la acción de los Estados mediante una **mayor cooperación y colaboración interregional e interinstitucional**. En este sentido, tener en cuenta desarrollos normativos en materia de IA que se han dado en otros países o regiones del mundo resulta esencial para avanzar en una armonización y homogenización de normativas que permitan mayor interoperabilidad y **faciliten la cooperación penal internacional**.
- Adherirse y alinear regulaciones tales como el **Convenio Marco del Consejo de Europa sobre Inteligencia Artificial**. El Convenio establece un enfoque común para garantizar que los sistemas de IA sean compatibles con los derechos humanos, la democracia y el Estado de Derecho, permitiendo al mismo tiempo la innovación y la confianza. Este convenio está plenamente alineado con otras iniciativas legislativas de IA como el Reglamento Europeo de IA.
- Legislación sobre **protección de datos personales** que tenga como finalidad acceder, rectificar, cancelar y oponerse al manejo de sus datos personales por parte de un tercero, en concordancia con estándares internacionales y europeos. La ley de protección de datos personales debería incluir salvaguardas específicas de protección de derechos fundamentales.
- **Establecer estándares y regulaciones** claras y armonizadas entre países y con otras regiones en materia de **conservación de datos selectivos y sensibles, así como el acceso rápido a metadatos**, cumpliendo con los principios fundamentales de necesidad y proporcionalidad. La finalidad última de establecer un marco regulatorio claro en materia de conservación de datos es proporcionar mayor seguridad jurídica y agilizar investigaciones transfronterizas vinculadas a crimen organizado. El trabajo con el sector privado será esencial para evitar bloqueos, sobrecostes y retrasos innecesarios.
- Promover la **alfabetización digital** (*AI literacy*), siguiendo ejemplos como el Reglamento europeo de IA u otras iniciativas como en Corea del Sur o China. Esto permitirá fortalecer los conocimientos dentro y fuera de la administración pública y de la ciudadanía, potenciar el desarrollo tecnológico y sensibilizar sobre riesgos y oportunidades vinculadas a la IA y el delito. El desarrollo de marcos educativos para la alfabetización digital y en materia de IA es una prioridad también incluida en la Hoja de Ruta acordada en la Declaración de Montevideo "para la construcción de un enfoque regional sobre gobernanza de la Inteligencia Artificial y sus impactos en nuestra sociedad" (2024)

Tipificación específica y creación de nuevos tipos penales

Se recomienda considerar la incorporación de figuras delictivas específicas, como:

- **Uso malicioso de IA**: Delito consistente en utilizar un sistema de IA para cometer fraude, suplantación, ciberataque, manipulación de información o daño a sistemas e infraestructuras críticas.

- **Creación o distribución de IA peligrosa y/o con fines delictivos**: Tipificación del acto de diseñar, entrenar o poner a disposición sistemas cuyo funcionamiento pueda causar daño grave y previsible. Ejemplo: “Quien desarrolle o utilice un sistema de inteligencia artificial con conocimiento de que será utilizado para cometer delitos contra la seguridad informática, la integridad de las personas o el orden público…”.
- **Deepfakes delictivos**. Penalización específica del uso de IA para generar contenidos sintéticos con fines ilícitos (extorsión, difamación, manipulación electoral, abuso sexual a menores, violencia de género, etc.).
- **Uso de IA para discriminación estructural o sesgo deliberado.** Aplicable en recursos humanos, crédito, justicia predictiva, etc. Regular, mediante una ley específica sobre IA y los delitos asociados o una normativa especializada, **la desinformación** y, particularmente, la desinformación electoral, así como los riesgos en el uso de algoritmos de aprendizaje automático para controlar informaciones o desinformaciones. Se podría tomar como base la Ley de Servicios Digitales de la UE, la cual regula de manera detallada y específica la difusión de desinformación en periodos electorales a través de obligaciones de transparencia, auditoría de algoritmos y mecanismos para eliminar contenido falso en sus artículos 26 y 30.
- **El uso de los vehículos autónomos para la comisión de delitos** (tráfico de bienes ilícitos, homicidios, intimidación, agresión, seguimiento, control territorial, etc.).

BIBLIOGRAFÍA

Bayoud, A. (2025), *'Narcodrones': la nueva amenaza criminal en México*. France 24. Disponible en: https://www.france24.com/es/am%C3%A9rica-latina/20250616-narcodrones-la-nueva-amenaza-criminal-en-m%C3%A9xico

Blauth, T. F., Gstrein, O. J., & Zwitter, A. (2022), *Artificial Intelligence Crime: An Overview of Malicious Use and Abuse of AI*. IEEE Access, 10, 77110–77122. Disponible en: https://doi.org/10.1109/ACCESS.2022.3191790

Christos Velasco, Jean Garcia Periche, Juan De Dios Gómez Gómez, Miguel Bueno Benedí (2024), *Inteligencia Artificial y Crimen Organizado*. Programa EL PACCTO 2.0 de la UE.

Combarros Merino, R. (2023), Vehículos autónomos e inteligência artificial: responsabilidad de civil y productos defectuosos. Universidad de León. Máster en Derecho de la Ciberseguridad y Entrono Digital. Disponible en: https://buleria.unileon.es/bitstream/handle/10612/17381/Combarros_Merino_Roberto.pdf?sequence=1

Comisión Europea, *Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la adopción de normas de responsabilidad civil extracontractual a la inteligencia artificial* (Directiva sobre responsabilidad en materia de IA). COM(2022) 496 final | 2022/0303 (COD). Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52022PC0496

Comisión Europea, *Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y el material de abuso sexual de menores y por la que se sustituye la Decisión marco* 2004/68/JAI del Consejo (versión refundida). COM(2024) 60 final. 2024/0035 (COD). https://eur-lex.europa.eu/resource.html?uri=cellar:a0335235-c5be-11ee-95d9-01aa75ed71a1.0020.02/DOC_1&format=PDF

Consejo de Europa (2024), El Convenio Marco del Consejo de Europa sobre inteligencia artificial, derechos humanos, democracia y Estado de Derecho (CETS No. 225). Disponible en: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=225

Daniel Casados, Paola Cicero et al., (2024) *Agenda Nacional Mexicana de Inteligencia Artificial*. Coalición IA2030Mx. Disponible en: https://wp.oecd.ai/app/uploads/2022/01/Mexico_Agenda_Nacional_Mexicana_de_IA_2030.pdf

Europol (2025), *European Union Serious and Organised Crime Threat Assessment – The changing DNA of serious and organised crime*, Publications Office of the European Union, Luxembourg. ISBN 978-92-9414-000-5. Doi: 10.2813/0758057

Europol (2025), Internet Organised Crime Threat Assessment – IOCTA: *Steal, deal and repeat – How cybercriminals trade and exploit your data*. European Union Agency for Law Enforcement Cooperation (EUROPOL). ISBN 978-92-9414-027-2. Doi: 10.2813/4926508

EUROPOL (2023), *Una de las lavanderías criptomonedas más grandes de la cubierta sexista lavada*, 15 de marzo 2023. https://www.europol.europa.eu/media-press/newsroom/news/one-of-darkwebs-largest-cryptocurrency-laundromats-washed-out

International Center for Not-for-Profit Law (2024), *Informe Final sobre Derechos Digitales en Centroamérica: Enfoque en Honduras, Guatemala, El Salvador y Nicaragua*. ICNL. Disponible en: https://www.icnl.org/wp-content/uploads/Informe-Final-sobre-Derechos-Digitales-en-Honduras-Guatemala-El-Salvador-y-Nicaragua.pdf

Heather Chen and Kathleen Magramo (2024), Finance worker pays out $25 million after video call with deepfake 'chief financial officer'. CNN

Hintze, A. (2016) *Understanding the Four Types of AI, from Reactive Robots to Self-Aware Beings*. The Conversation. https://theconversation.com/understanding-the-four-types-of-ai-from-reactive-robots-to-self-aware-beings-67616

Gutiérrez, J.D. (2024), *Documento de consulta pública: Directrices de la UNESCO para el uso de sistemas de inteligencia artificial en juzgados y tribunales*. UNESCO. Disponible en: https://unesdoc.unesco.org/ark:/48223/pf0000390781_spa

Guzmán Valladares, M. E. (2024), *Ciberdelitos y los delitos informáticos*. Escuela Judicial de Honduras.

IBM X-Force (2025), *Índice de Inteligencia sobre Amenazas de 2025: transformando ciberdefensa en ciberresiliencia*. IBM Institute for Business Value. Disponible en: https://www.ibm.com/thought-leadership/institute-business-value/report/2025-threat-intelligence-index

Jeff Sims (2023), *Introducing EyeSpy: A Cognitive Threat Agent*. Hayas. Disponible en: https://www.hyas.com/blog/eyespy-proof-of-concept

Juan Manuel Aguilar Antonio (2025), *Redes Criminales de Alto Riesgo que utilizan la Inteligencia Artificial para la Comisión de Delitos*. EL PACCTO 2.0.

M. Luz Domínguez (2025), *Slopsquatting: una nueva ciberamenaza para empresas que automatizan el desarrollo con IA*. Bit Life Media. Disponible en: https://bitlifemedia.com/2025/04/slopsquatting-una-nueva-ciberamenaza-para-empresas-que-automatizan-el-desarrollo-con-ia/

Naciones Unidas (2025), *Junta Internacional de Fiscalización de Estupefacientes*, Informe 2024. ISBN 978-92-1-107118-4. Disponible en: https://www.incb.org/documents/Publications/AnnualReports/AR2024/Annual_Report/E-INCB-2024-1-SPA.pdf

P.F Nettel, E. Hankins, R. Stirling, G. Cirri, G. Grau. S. Rahim y E. Crampton, (2024) *Government AI Readiness Index 2024*, Oxford insights. Disponible en: https://oxfordinsights.com/wp-content/uploads/2025/06/2024-Government-AI-Readiness-Index.pdf

Pascual Estapé, J.A. (2025), Interceptan el primer narcosubmarino autónomo que usa los satélites Starlink para orientarse. 20 minutos – Computer Hoy. Disponible en: https://computerhoy.20minutos.es/tecnologia/primer-narcosubmarino-autonomo-usa-satelites-starlink-orientarse-1471183

Práxedes Martínez-Moreno, Andrea Valsecchi, Pablo Mesejo, Óscar Ibañez, Sergio Damas (2024). *Evidence evaluation in craniofacial superimposition using likelihood ratios*. Information Fusion. Disponible en: https://doi.org/10.1016/j.inffus.2024.102489

Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial. Anexo III: Sistemas de IA de alto riesgo, Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32024R1689

Sentencia T-323 de 2024, *Uso de herramientas de inteligencia artificial generativas en procesos judiciales de tutela*, Corte Constitucional de la República de Colombia, Sala Segunda de Revisión. Disponible en: https://www.diarioconstitucional.cl/wp-content/uploads/2024/08/Vea-sentencia-Corte-Constitucional-de-Colombia-T-323-24.pdf

Stankovich, M., Feldfeber, I., Quiroga, Y., Ciolfi Felice, M., y Marivate, V. (2023), *Kit de herramientas global sobre IA y el estado de derecho para el poder judicial*. UNESCO. Disponible en: https://unesdoc.unesco.org/ark:/48223/pf0000387331_spa

Stuart J. Russel y Peter Norvig (1995, edición actualizada 2020), *Inteligencia Artificial: un enfoque moderno*. Prentice Hall.

Zack, Whittacker (2025), *How the ransomware attack at Change Healthcare went down: A Timeline*, Techcrunch, January 27, 2025. Disponible en: https://techcrunch.com/2025/01/27/how-the-ransomware-attack-at-change-healthcare-went-down-a-timeline/

Ziemer, H. (2025), *Illicit Innovation: Latin America Is Not Prepared to Fight Criminal Drones*. Center for Strategic and International Studies. Disponible en: https://www.csis.org/analysis/illicit-innovation-latin-america-not-prepared-fight-criminal-drones

EL PACCTO 2.0

EU-LAC Partnership on justice and security