DOCTRINA JURÍDICA
REVISTA SEMESTRAL DE DOCTRINA, JURISPRUDENCIA Y LEGISLACIÓN
Año XVI - Número 36 – FEBRERO 2025 – e-ISSN: 2618-4133 / 1853-0338

SECCIÓN DISERTACIONES

TRANSFORMACIÓN DIGITAL EN LA LUCHA CONTRA EL CRIMEN ORGANIZADO

Estrategias éticas para la prevención y humanización de las innovaciones tecnológicas

Pablo Rafael Banchio[1]

"Ciclo de Conferencias sobre la Seguridad Humana y la Seguridad Multidimensional"
Universidad del Museo Social Argentino (Buenos Aires), 30 de octubre de 2024

Resumen: La presente conferencia investiga el impacto de las nuevas tecnologías en la lucha contra el crimen organizado, analizando su potencial, riesgos y las implicaciones éticas que surgen en este contexto. A través de cuatro apartados, se examinan las aplicaciones de la tecnología *blockchain* en la prevención de delitos como el tráfico de personas y el lavado de dinero; el uso de *big data* para la detección y desmantelamiento de redes criminales, con un enfoque en los riesgos de perfilado racial; y las amenazas cibernéticas que las organizaciones criminales emplean en el ámbito digital. Asimismo, se revisan los convenios internacionales existentes y su eficacia en el contexto tecnológico contemporáneo. La disertación concluye que, aunque las tecnologías emergentes pueden ofrecer herramientas valiosas para combatir el crimen organizado, es fundamental establecer un marco ético y regulatorio que garantice la protección de los derechos humanos y minimice los riesgos de uso indebido.

Palabras clave: tecnología, crimen organizado, *blockchain*, tráfico de personas, lavado de dinero, *big data*, perfilado racial, ciberseguridad, amenazas cibernéticas, derechos humanos, regulación internacional, Ética.

[1] Profesor de Ética Digital en el Master «Digitalización y Derechos Humanos» de la Universidad Euro-Mediterránea y Director del Post-Doctorado en «Derechos Humanos e Inteligencia Artificial» de la Università degli Studi Virtuale Innovativa (https://www.universitavirtuale.eu).Ciencias de Buenos Aires. Director del Centro di Studi Giuridici e di Ricerca Internazionale (CSGRI).

Digital transformation in the fight against organized crime

Ethical strategies for the prevention and humanization of technological innovations

Abstarct: This paper investigates the impact of new technologies on the fight against organized crime, analyzing their potential, risks, and the ethical implications that arise in this context. Through four chapters, it examines the applications of blockchain technology in preventing crimes such as human trafficking and money laundering; the use of big data for detecting and dismantling criminal networks, focusing on the risks of racial profiling; and the cyber threats that criminal organizations employ in the digital realm. Additionally, it reviews existing international conventions and their effectiveness in the contemporary technological context. The research concludes that while emerging technologies can offer valuable tools to combat organized crime, it is essential to establish an ethical and regulatory framework that ensures the protection of human rights and minimizes the risks of misuse.

Keywords: technology, organized crime, blockchain, human trafficking, money laundering, big data, racial profiling, cybersecurity, cyber threats, human rights, international regulation, Ethics.

1. Introducción

El crimen organizado es un fenómeno global que ha evolucionado en complejidad y alcance debido, en gran medida, a los avances tecnológicos de las últimas décadas. Hoy en día, organizaciones criminales transnacionales no solo operan en espacios físicos, sino también en el vasto entorno digital, utilizando herramientas avanzadas y recursos tecnológicos que les permiten expandir y diversificar sus actividades. En respuesta, el sistema legal internacional y las autoridades de seguridad pública han comenzado a incorporar nuevas tecnologías para detectar, rastrear y desmantelar estas redes criminales. Sin embargo, esta integración de tecnología en la lucha contra el crimen plantea tanto desafíos éticos como legales, lo cual exige una revisión constante y adaptativa de las normas y marcos regulatorios.

La presente investigación examina este panorama mediante un enfoque interdisciplinario que abarca tanto el potencial de las nuevas tecnologías para combatir el crimen organizado como los dilemas éticos y las limitaciones

regulatorias que estas tecnologías presentan. A través de cuatro apartados, se exploran distintas tecnologías emergentes y su impacto en la lucha contra el crimen organizado, destacando el papel de la cooperación internacional y la necesidad de un marco ético sólido que guíe su implementación.

En el primer apartado, se analiza el uso de la tecnología blockchain en la prevención de delitos como el tráfico de personas y el lavado de dinero. Esta tecnología ofrece una trazabilidad única y la capacidad de proteger datos sensibles, pero también plantea riesgos de "anonimización" y descentralización que pueden facilitar actividades ilícitas. La exploración de estos aspectos ilustra la necesidad de una regulación específica que maximice los beneficios de *blockchain* en la lucha contra el crimen organizado, sin desatender los riesgos éticos y legales.

El segundo apartado se centra en el análisis de *big data* y su aplicación en la seguridad pública. Se investiga cómo los datos masivos permiten predecir y detectar patrones delictivos, lo que representa un recurso significativo para identificar redes de crimen organizado. No obstante, el uso de *big data* en seguridad plantea el riesgo de perfilado racial y otros sesgos discriminatorios, los cuales afectan la equidad y justicia en las prácticas policiales. Este apartado ofrece una revisión de casos reales y propone lineamientos éticos para minimizar los riesgos asociados a esta tecnología.

En el tercer apartado, se aborda el ámbito de la ciberseguridad y su relación con el crimen organizado. Las amenazas cibernéticas, como el *hacking* y el *ransomware*, se han convertido en herramientas comunes de las organizaciones criminales en el entorno digital. Además de describir estas amenazas, este apartado profundiza en la importancia de construir infraestructuras de ciberseguridad basadas en principios éticos, que protejan tanto los datos personales como la integridad de las redes y sistemas. Se analiza, asimismo, el papel de la ética en la toma de decisiones en ciberseguridad y en el desarrollo de estrategias efectivas de prevención del crimen.

Finalmente, el cuarto apartado examina el marco regulatorio internacional y los convenios existentes en la lucha contra el crimen organizado, con especial énfasis en la Convención de Palermo y la Convención de las Naciones Unidas contra la Corrupción. Este apartado evalúa la efectividad de estos acuerdos en el contexto de las nuevas tecnologías, resaltando los retos de su implementación y la necesidad de actualizarlos para abordar las amenazas digitales. Además, se proponen recomendaciones para mejorar la colaboración entre países y adaptar las normas internacionales a las dinámicas del crimen organizado en la era digital.

En conjunto, los cuatro apartados de esta investigación presentan un análisis integral sobre cómo las tecnologías emergentes pueden utilizarse para combatir el crimen organizado y los retos éticos y legales que implica su uso. La investigación concluye con una reflexión sobre la importancia de equilibrar los avances tecnológicos con una perspectiva ética y regulatoria sólida, destacando la cooperación internacional como una herramienta esencial para enfrentar las amenazas del crimen organizado en un mundo cada vez más digitalizado.

2. *Blockchain* y crimen organizado

En este primer apartado pretendemos establecer las bases para comprender cómo *blockchain* puede ser una herramienta poderosa en la lucha contra el crimen organizado, a la vez que enfatizaremos los dilemas éticos y los riesgos que requieren una supervisión y regulación cuidadosa para el uso de la cadena de bloques en este tipo de delitos sin comprometer derechos fundamentales.

2.1 Aplicaciones de *blockchain* en la lucha contra el crimen

La tecnología *blockchain* ha ganado reconocimiento en los últimos años no solo como el soporte técnico para criptomonedas como Bitcoin, sino también por su potencial en sectores como la cadena de suministro, la salud y la seguridad digital[2]. En el contexto de la lucha contra el crimen organizado, blockchain se presenta como una herramienta que puede optimizar y asegurar la trazabilidad de transacciones, especialmente en los casos de tráfico de personas y lavado de dinero.

2.1.1 Tráfico de personas

El tráfico de personas es una de las industrias criminales más lucrativas y difíciles de rastrear debido a la complejidad de las redes transnacionales involucradas y al secretismo de las transacciones. *Blockchain* ofrece un sistema de registro descentralizado que podría documentar de manera transparente las transferencias financieras asociadas a estas redes.

Cada transacción registrada en una cadena de bloques es prácticamente inalterable, lo cual facilita la creación de pruebas para el procesamiento judicial y aumenta las posibilidades de rastrear los flujos de dinero hacia sus verdaderos

[2] Banchio, P. (2022). *Nuevas Tecnologías y Derecho*. Perspectivas Jurídicas. Buenos Aires, 2022.

destinatarios. Además, el uso de contratos inteligentes (*smart contracts*) - programas que se ejecutan automáticamente en el *blockchain* cuando se cumplen ciertas condiciones- permite automatizar procesos que verifican la autenticidad y el destino final de los fondos, bloqueando transacciones sospechosas[3].

2.1.2 Lavado de dinero

El lavado de dinero es un desafío significativo para los sistemas financieros mundiales y una actividad clave para el crimen organizado. *Blockchain* puede ofrecer una infraestructura resistente y transparente en la que cada transacción queda registrada de forma inmutable. Esta tecnología no solo garantiza la transparencia, sino que también permite una trazabilidad eficaz de fondos, lo que facilita la identificación de patrones anómalos que pueden indicar actividades ilícitas.

Mediante la combinación de *blockchain* con técnicas de análisis de datos, las instituciones financieras y las autoridades pueden detectar y detener transacciones ilegales de manera más eficaz. Sin embargo, su implementación plantea ciertos dilemas éticos y técnicos, como se discutirá en las siguientes secciones.

2.2 Evaluación ética del uso de *blockchain*

La aplicación de *blockchain* en la lucha contra el crimen, si bien presenta ventajas, también genera interrogantes éticos que deben abordarse para prevenir abusos y proteger derechos fundamentales.

2.2.1 Privacidad y transparencia

Una de las cuestiones éticas centrales de *blockchain* es el equilibrio entre privacidad y transparencia. En un sistema de cadena de bloques, los registros de transacciones son públicos y accesibles, lo que puede facilitar la trazabilidad y el control en contextos de crimen organizado.

No obstante, la transparencia total puede amenazar la privacidad individual, especialmente cuando se trata de datos financieros o de identificación personal. Un enfoque ético en el uso de *blockchain* debe considerar el derecho a la

[3] Idem

privacidad de los usuarios y establecer controles sobre qué tipo de información puede hacerse pública y cuál debe estar protegida.

2.2.2 Riesgos de uso indebido

Aunque el objetivo es utilizar *blockchain* como herramienta en la lucha contra el crimen, su descentralización y falta de intermediarios también podrían facilitar su uso por redes criminales que desean eludir el control estatal.

Los mismos principios de transparencia y privacidad que protegen a los ciudadanos también pueden ser explotados para evitar el rastreo de actividades ilegales. Es necesario, por lo tanto, evaluar los riesgos de un sistema que podría, paradójicamente, facilitar los delitos que busca erradicar y analizar cómo mitigar estos riesgos a través de regulaciones y limitaciones éticas.

2.3 Riesgos asociados al uso de *blockchain*

Pese a sus beneficios, el uso de *blockchain* en la lucha contra el crimen organizado presenta riesgos específicos que podrían, en algunos casos, contradecir sus fines de justicia y seguridad.

2.3.1 Posibilidad de encubrimiento de actividades ilegales

Aunque la cadena de bloques permite el seguimiento de transacciones, algunos diseños *blockchain* incluyen funcionalidades de "anonimización" y cifrado que pueden facilitar el encubrimiento de actividades delictivas. Tecnologías como los *mixers* o "tumbadores" de criptomonedas dificultan la identificación de la procedencia de los fondos, lo que podría ser aprovechado por organizaciones criminales para camuflar transacciones.

A medida que las redes criminales se familiarizan con la tecnología, se desarrollan métodos cada vez más sofisticados para explotar estas funcionalidades, lo que representa un obstáculo en el combate contra el crimen.

2.3.2 Dificultad de regular y supervisar la tecnología

La naturaleza descentralizada de *blockchain*, diseñada para evitar la intervención de intermediarios, presenta un desafío en términos de regulación y supervisión. No existe una autoridad central que controle todas las operaciones en una cadena de bloques pública, lo que limita la capacidad de los gobiernos y

organismos internacionales para intervenir. Este es un riesgo particularmente relevante cuando se trata de crímenes que trascienden fronteras nacionales, ya que la falta de regulaciones uniformes facilita que los criminales aprovechen la fragmentación normativa para operar en diferentes jurisdicciones.

2.3.3 Desafíos técnicos y éticos de "anonimización"

La privacidad en *blockchain* puede convertirse en una barrera para la investigación criminal. Por ejemplo, en sistemas que utilizan criptomonedas con altas garantías de anonimato, como "Monero" o "Zcash", resulta más complejo identificar la cadena de transacciones y a sus propietarios.

Estos desafíos no solo son técnicos, sino también éticos, ya que los derechos a la privacidad y a la seguridad pública deben ser equilibrados con sumo cuidado. El desarrollo de regulaciones claras y éticamente sólidas para controlar y monitorizar estos sistemas resulta esencial para aprovechar *blockchain* en la lucha contra el crimen organizado sin comprometer derechos individuales.

2.4 Análisis de casos

Como siempre manifestamos, fieles a la concepción del Tetraedro de Derecho[4], la ciencia jurídica integra la realidad del "ser" en la dimensión sociológica, con la dimensión normológica a través de prescripciones legales que "deben ser", para la realización de la justicia en la dimensión dikelógica, hacia un mundo mejor que "puede ser" en el por-venir de la dimensión témporo-espacial.

En consonancia con ello, expondremos, como siempre casos reales (ser) de aplicación normativa (deber ser) en busca de la justicia, precisamente para los desafíos de un futuro global mejor (poder ser).

Los tres casos analizados a continuación destacan los éxitos y los problemas asociados a la tecnología de una cadena de bloques en la lucha contra el tráfico de personas y el lavado de dinero, mostrando tanto su potencial como sus limitaciones.

Ellos ilustran la doble función de *blockchain* en el contexto del crimen organizado: como herramienta que puede facilitar el encubrimiento de delitos y, simultáneamente, como un medio para rastrear y desmantelar redes criminales.

[4] Banchio, P. (2018). *El Tetraedro del Derecho. Aportes para una Teoría General del Derecho Privado*. Buenos Aires, 20 de marzo de 2018. CERN European Organization for Nuclear Research - Zenodo. https://doi.org/10.5281/zenodo.5513094.

Consideramos que cada caso aporta lecciones sobre la necesidad de regulación, ética y políticas de colaboración entre instituciones. Los retos en privacidad, transparencia y regulación deben ser considerados y abordados para maximizar los beneficios de *blockchain* en la lucha contra el crimen organizado sin comprometer derechos fundamentales.

Caso 1. "Traffik Analysis Hub". *Blockchain* contra el tráfico de personas

a) Descripción del caso: El *Traffik Analysis Hub* es una iniciativa de colaboración entre IBM, "Stop the Traffik" (una organización no gubernamental que combate el tráfico de personas) y otros actores. Este proyecto utiliza la tecnología *blockchain* para rastrear y compartir datos sobre redes de tráfico humano, con el objetivo de identificar patrones y ayudar a las fuerzas del orden a desmantelar dichas redes.

Mediante la plataforma *IBM Blockchain*, esta iniciativa almacena información y permite que varias organizaciones, desde ONGs hasta cuerpos policiales, compartan y consulten datos de manera segura y anónima. Al emplear *blockchain*, los datos se vuelven accesibles y auditables, permitiendo mayor transparencia y mejor coordinación en la lucha contra el tráfico de personas.

b) Funcionamiento técnico: b.1) Procesamiento del lenguaje natural (PLN): *TA Hub* utiliza algoritmos de PLN para analizar grandes cantidades de texto, como publicaciones en redes sociales, noticias y documentos legales, y extraer información relevante sobre la trata de personas.

b.2) Aprendizaje automático: a través del aprendizaje automático, *TA Hub* identifica patrones y relaciones en los datos que pueden indicar la presencia de actividades relacionadas con la trata. Por ejemplo, puede detectar palabras clave, frases y combinaciones de datos que son características de este delito.

b.3) Visualización de datos: la plataforma utiliza herramientas de visualización para presentar los datos de manera clara y concisa, lo que facilita la identificación de tendencias y la toma de decisiones.

c) Tipos de datos: *TA Hub* puede analizar una amplia variedad de datos, incluyendo:

c.1) Datos en línea: publicaciones en redes sociales, anuncios clasificados, sitios web de citas, foros y otros espacios digitales donde los traficantes pueden reclutar víctimas o promocionar sus servicios.

c.2) Datos financieros: transacciones bancarias, transferencias de dinero y registros de pagos que pueden revelar movimientos de fondos ilícitos.

c.3) Datos de viajes: registros de vuelos, hoteles y alquiler de vehículos que pueden ayudar a rastrear los movimientos de las víctimas y los traficantes.

c.4) Datos demográficos: información sobre edad, género, nacionalidad y otras características de las víctimas y los perpetradores.

c.5) Informes policiales: denuncias, investigaciones y sentencias relacionadas con la trata de personas.

d) Impacto y desafíos éticos: Este caso muestra el potencial de *blockchain* para generar una base de datos descentralizada que facilite el intercambio de información sensible, especialmente en delitos que afectan múltiples jurisdicciones.

Sin embargo, uno de los desafíos éticos es garantizar que la privacidad de las víctimas de tráfico no sea comprometida, dado que la cadena de bloques es inmutable y, si la información es incorrectamente registrada o utilizada, podría afectar a individuos y organizaciones.

Además, la interoperabilidad entre diversas agencias y el nivel de acceso de cada actor presentan dilemas éticos sobre quién puede ver y gestionar estos datos, y cómo se asegura la transparencia sin comprometer la seguridad.

e) Fuentes de información:

-Clarín: "Blockchain y la lucha contra la trata de personas" https://www.clarin.com/tecnologia/blockchain-lucha-trata-personas_0_NiqiEJPgX.html

-El Español: "Traffik Analysis Hub, una plataforma que lucha contra la trata de personas con tecnología de IA" https://www.elespanol.com/invertia/empresas/tecnologia/20191122/traffik-analysis-hub-plataforma-personas-tecnologia-ia/446126665_0.html

-Mundo Cloud: "Pasos Libres y la lucha contra la trata de personas mediante la tecnología blockchain" https://mundo.cloud/ibm/pasos-libres-y-la-lucha-contra-la-trata-de-personas-mediante-la-tecnologia-blockchain

Caso 2. "Bitfinex" y el lavado de dinero en criptomonedas

a) Descripción del caso: Bitfinex, una plataforma de intercambio de criptomonedas, fue víctima de un hackeo en 2016, cuando los delincuentes sustrajeron aproximadamente 119.756 bitcoins.

La mayoría de estos bitcoins fueron movidos a través de diversas billeteras en un intento por lavar el dinero, aprovechando la "seudonimidad" que ofrece *blockchain*. Sin embargo, gracias a la naturaleza pública de las transacciones en

la cadena de bloques de Bitcoin, las autoridades pudieron rastrear las direcciones y movimientos de estas criptomonedas.

En 2022, el FBI arrestó a dos personas en Nueva York relacionadas con el hackeo y recuperó aproximadamente 3.6 mil millones de dólares en bitcoins, lo que representa uno de los mayores decomisos de criptomonedas en la historia.

b) Impacto y desafíos éticos: Este caso demuestra tanto la fortaleza de *blockchain* en términos de rastreo como la complejidad de manejar datos anónimos. Aunque los bitcoins pueden ser rastreados en términos de sus movimientos, identificar a los propietarios detrás de cada billetera suele ser un desafío.

Este caso ejemplifica cómo *blockchain* puede ser una herramienta útil para las fuerzas del orden en el rastreo de fondos, pero también plantea cuestiones éticas sobre el papel de los *exchanges* (plataformas de intercambio) en la prevención del lavado de dinero. ¿Deben los *exchanges* obligatoriamente de monitorizar transacciones sospechosas? ¿Cómo se balancea la necesidad de seguridad pública con el derecho a la privacidad en el uso de criptomonedas?

c) Fuentes de información:

-Cointelegraph: Información sobre la recuperación de fondos y el hackeo de Bitfinex en 2016
https://es.cointelegraph.com/news/us-recovers-bitfinex-hack-funds

-El Diario El Salvador: Artículo sobre Tether y su uso en actividades ilícitas, en relación con Bitfinex
https://www.elsalvador.com/noticias/finanzas/tether-fondos-ilicitos-bitfinex/1014901/2023/

-Cointelegraph: Debate sobre la compensación a los titulares de tokens LEO tras la recuperación de los fondos
https://es.cointelegraph.com/news/bitfinex-fund-recovery-implications

Caso 3. "Silk Road" y el crimen organizado en la *Dark Web*

a) Descripción del caso: Silk Road, una plataforma de mercado negro en la dark web que utilizaba Bitcoin como moneda principal, fue un claro ejemplo de cómo blockchain puede ser aprovechada por organizaciones criminales para facilitar transacciones ilegales.

Creada en 2011, Silk Road permitió la compra de drogas, armas y otros bienes ilegales hasta su cierre en 2013. El FBI utilizó el rastreo de las transacciones en Bitcoin para localizar y capturar a Ross Ulbricht, el fundador de Silk Road. Las transacciones, aunque se realizaban de forma anónima, dejaron rastros en la

blockchain, lo que facilitó a las autoridades seguir el flujo de bitcoins entre compradores y vendedores.

b) Impacto y desafíos éticos: El caso Silk Road revela cómo *blockchain* puede tanto facilitar actividades ilícitas como ofrecer pistas clave para los investigadores. La *dark web* y el uso de criptomonedas anónimas desafían los modelos tradicionales de rastreo financiero.

Asimismo, plantea interrogantes éticos sobre la responsabilidad de quienes desarrollan y mantienen estas tecnologías. Por ejemplo, ¿quién debería ser responsable de monitorear y reportar actividades ilegales cuando la tecnología permite la "seudonimidad"? También abre el debate sobre la intervención gubernamental y hasta qué punto debería regularse el uso de criptomonedas para proteger la seguridad pública sin restringir el derecho a la privacidad.

3. Análisis de *big data* y seguridad pública

El uso de *big data* en la seguridad pública ofrece beneficios innegables en la detección y desmantelamiento de redes criminales, pero también plantea desafíos éticos y sociales significativos. La implementación de estas tecnologías debe considerar los riesgos de perfilado racial y discriminación, y priorizar la creación de mecanismos que aseguren justicia y respeto a los derechos humanos.

Los casos que analizaremos a continuación destacan la necesidad de regulaciones claras, así como de una supervisión ética de los algoritmos y sistemas de análisis, para que el uso de *big data* en la seguridad pública no comprometa los principios de equidad y dignidad humana.

3.1 Uso de *big data* en la detección y desmantelamiento de redes criminales

El uso de *big data* en la seguridad pública ha revolucionado la manera en que las autoridades detectan y desmantelan redes criminales. La recopilación masiva de datos provenientes de diversas fuentes -como redes sociales, registros financieros, cámaras de vigilancia y dispositivos móviles- permite identificar patrones que pueden señalar actividades delictivas y prever eventos criminales.

3.1.1 Predicción de actividades delictivas

El análisis de *big data* facilita la predicción de ciertos comportamientos basados en datos históricos y en el monitoreo de actividades actuales. A través

de algoritmos de aprendizaje automático (*machine learning*), los sistemas de grandes volúmenes de datos pueden identificar patrones que normalmente pasarían desapercibidos para los investigadores humanos, permitiendo a las fuerzas del orden anticiparse a delitos o identificar potenciales focos de criminalidad.

Estos sistemas, al basarse en técnicas de minería de datos y análisis predictivo, pueden proporcionar alertas tempranas que apoyen las investigaciones y permitan una mejor asignación de recursos.

3.1.2 Identificación de redes criminales

Uno de los mayores logros del uso de *big data* en la seguridad pública ha sido la capacidad de identificar redes de crimen organizado a partir de conexiones y patrones en los datos.

Al analizar interacciones entre individuos, transferencias financieras y ubicaciones, los algoritmos pueden generar mapas de relaciones que revelen vínculos entre personas y organizaciones involucradas en actividades ilícitas. Esta capacidad es especialmente valiosa en la lucha contra el tráfico de drogas, el terrorismo y el crimen cibernético, ya que permite rastrear flujos de dinero, movimientos de personas y comunicaciones a escala global.

3.2 Riesgos de perfilado racial y discriminación

El uso de *big data* en la seguridad pública también plantea desafíos éticos significativos, en particular en relación con el perfilado racial y otros tipos de sesgo discriminatorio. Los algoritmos utilizados para identificar patrones de actividad delictiva se basan en datos históricos, que pueden reflejar prejuicios raciales, económicos o de otro tipo. Esto lleva a que el perfilado basado en *big data* pueda intensificar injusticias y crear riesgos de violación de derechos humanos.

3.2.1 Sesgos en los datos

La precisión de los sistemas de *big data* depende de la calidad y objetividad de los datos utilizados. Sin embargo, si estos datos están sesgados debido a prácticas policiales históricas o estereotipos sociales, los resultados pueden ser injustamente perjudiciales para ciertas poblaciones.

Por ejemplo, si un algoritmo de predicción delictiva utiliza registros históricos de arrestos en barrios de minorías, es probable que los resultados refuercen la vigilancia en estas comunidades, independientemente de la tasa real de criminalidad. Este sesgo en los datos puede llevar a la estigmatización y vigilancia excesiva de ciertas comunidades, afectando su confianza en las instituciones públicas y limitando sus libertades.

3.2.2 Desafíos éticos en la protección de derechos humanos

El perfilado racial y la discriminación en el uso de *big data* también representan desafíos éticos profundos. El uso de algoritmos para identificar y clasificar personas con base en sus características demográficas, como raza, etnia o nivel socioeconómico, contradice los principios de igualdad y justicia.

Además, el perfilado racial puede conducir a decisiones automatizadas que resultan en detenciones injustificadas, vigilancia innecesaria y violación de derechos humanos. En el contexto de los derechos humanos, es esencial garantizar que el uso de *big data* no comprometa la dignidad ni las libertades fundamentales de las personas.

3.3 Casos de estudio y prácticas policiales

Para ilustrar los desafíos y efectos del uso de *big data* en la seguridad pública, es relevante analizar algunos casos de estudio donde estas tecnologías han sido implementadas y observar tanto los éxitos como las controversias que han surgido.

3.3.1 El Programa “PredPol” en los Estados Unidos

El programa PredPol, utilizado en varias ciudades de Estados Unidos, es un *software* de predicción de delitos que analiza datos históricos para prever lugares y momentos de posible actividad delictiva.

PredPol utiliza un algoritmo de aprendizaje automático que analiza datos históricos de delitos, como ubicación, tipo de delito y hora del día. A partir de este análisis, el programa genera "zonas de calor" o "*hotspots*" que identifican las áreas donde es más probable que, según patrones previos, ocurran futuros delitos. Estas zonas son luego utilizadas por las fuerzas del orden para concentrar sus patrullajes y recursos.

Si bien el *software* ha mostrado efectividad en la asignación de patrullas, ha sido criticado por su tendencia a reforzar el perfilado racial y focalizar la vigilancia en áreas de bajos ingresos, donde la actividad policial es históricamente más intensa.

a) Impacto en la seguridad pública y la justicia social: El uso de PredPol ha reducido la ocurrencia de ciertos delitos menores en las áreas monitoreadas, pero el enfoque en zonas específicas ha generado desconfianza y preocupación en comunidades marginadas.

Las críticas al programa destacan que el análisis se basa en datos históricos que pueden reflejar prácticas policiales sesgadas, lo que puede llevar a un ciclo de criminalización de las mismas comunidades, incluso si no existe un aumento real de actividad delictiva. Este caso subraya la necesidad de desarrollar algoritmos que no solo optimicen la seguridad pública, sino que también respeten los principios de equidad y justicia social.

3.3.2 Proyecto Nacional de Seguridad en China

En China, el gobierno ha implementado un sistema de *big data* para monitorear y evaluar la actividad de sus ciudadanos con el fin de identificar potenciales amenazas para la seguridad nacional. Este sistema analiza enormes volúmenes de datos provenientes de cámaras de vigilancia, redes sociales y sistemas financieros para rastrear a personas de interés y predecir actividades consideradas riesgosas. Aunque ha permitido al gobierno chino identificar redes criminales y prevenir ciertos delitos, el sistema es objeto de críticas por su falta de transparencia y por su efecto sobre la libertad individual.

a) Impacto en derechos humanos: Este enfoque de seguridad basado en *big data* ha sido duramente criticado por su impacto en los derechos humanos, particularmente en relación con la privacidad y la libertad de expresión. Las técnicas de monitoreo masivo y la recopilación de datos personales sin consentimiento plantean un dilema ético importante y han sido denunciadas por organizaciones de derechos humanos como una forma de vigilancia estatal opresiva. Este caso resalta la importancia de establecer límites éticos y legales claros en el uso de *big data* para la seguridad pública, asegurando que las tecnologías no se conviertan en herramientas de control que restrinjan derechos fundamentales.

3.4 Análisis de casos reales

Como ya manifestamos, para comprender los beneficios y desafíos del uso de *big data* en la seguridad pública, se presentan a continuación algunos casos reales en los que esta tecnología ha sido aplicada. Estos ejemplos muestran el impacto en la reducción de delitos y el desmantelamiento de redes criminales, al mismo tiempo que evidencian riesgos éticos, como el perfilado racial y la discriminación.

En ellos queremos evidenciar que, aunque el *big data* tiene un gran potencial para mejorar la seguridad pública y optimizar los recursos en la lucha contra el crimen, también puede contribuir a la discriminación y la vigilancia desigual.

Como ya expresamos en numerosos trabajos anteriores[5], los algoritmos y sistemas de análisis predictivo utilizados en seguridad pública deben diseñarse y supervisarse cuidadosamente, con el fin de evitar sesgos y proteger los derechos humanos. Estos casos ponen de relieve la necesidad de una regulación clara, auditorías éticas y transparencia en el uso de big data, asegurando que su implementación sea equitativa y respetuosa de la dignidad humana.

Caso 1. "Palantir" y el Departamento de Policía de Los Ángeles (LAPD)

a) Descripción del caso: la empresa de *software* Palantir ha colaborado con el Departamento de Policía de Los Ángeles (*LAPD*) en el uso de *big data* para prevenir y resolver crímenes. Palantir utiliza su *software* de análisis para integrar datos de distintas fuentes, como registros policiales, redes sociales, y antecedentes penales.

Estos datos son procesados para identificar relaciones y patrones que puedan ayudar a anticipar delitos y monitorizar a personas consideradas de interés para el departamento. El *software* permite a los investigadores obtener información detallada sobre patrones de actividad delictiva, lo cual ayuda en la toma de decisiones y la focalización de recursos.

b) Impacto y desafíos éticos: aunque la colaboración ha mostrado resultados positivos en la prevención de ciertos delitos, ha generado preocupación en cuanto al perfilado racial y la privacidad. Se ha denunciado que

[5] Banchio, P. (2024). *Algorética*. Zenodo. https://doi.org/10.5281/zenodo.12806322.
Banchio, P. (2024) Existencialismo y tecnología. Desafíos éticos de la autonomía y la autenticidad en la era digital. *Doctrina Jurídica,* XV(35), noviembre de 2024.
Banchio, P. (2024). *Humanismo algorítmico y transparencia digital: un enfoque centrado en los valores humanos*. Zenodo. https://doi.org/10.5281/zenodo.12790268.
Banchio, P. (2024). *La Ética en la inteligencia artificial y los algoritmos a través del análisis de ocho casos jurisprudenciales*. Zenodo. https://doi.org/10.5281/zenodo.12803079.

el *software* tiende a concentrar la vigilancia en comunidades de minorías y en áreas de bajos recursos, perpetuando estereotipos y marginando a determinados grupos. Este caso expone un dilema ético fundamental en el uso de *big data*: la posible discriminación estructural que surge de algoritmos que refuerzan patrones preexistentes, lo cual cuestiona la justicia y equidad del sistema.

Caso 2. Proyecto "*Operation LASER*" en el Departamento de Policía de Chicago

a) Descripción del caso: el Departamento de Policía de Chicago implementó un programa denominado "*Operation LASER*" (*Los Angeles Strategic Extraction and Restoration*), que utiliza *big data* para crear un "índice de riesgo" de criminalidad. Mediante un algoritmo, se clasificaba a las personas en función de la probabilidad de participar en actos delictivos, basándose en factores como sus antecedentes penales, relaciones sociales, y datos geográficos. Este índice fue utilizado para orientar la vigilancia policial y priorizar intervenciones en áreas de alta criminalidad.

b) Impacto y desafíos éticos: el programa fue criticado por la forma en que etiquetaba a personas como "de alto riesgo" sin evidencia específica de que estuvieran involucradas en actividades ilegales. Este perfilado ha sido visto como una forma de discriminación que estigmatiza a ciertos individuos y comunidades.

Además, *Operation LASER* fue señalado por su falta de transparencia y por basarse en datos sesgados, lo que afectaba desproporcionadamente a minorías étnicas y residentes de vecindarios de bajos ingresos. En 2019, el programa fue cancelado, en gran parte debido a las críticas sobre su enfoque discriminatorio y la percepción de violación de derechos civiles.

Caso 3. Sistema de vigilancia predictiva en Reino Unido

a) Descripción del caso: en el Reino Unido, algunas fuerzas policiales implementaron un sistema de vigilancia predictiva mediante *big data* para analizar y prever la ocurrencia de delitos en ciertas áreas.

El sistema utiliza datos históricos, incluyendo registros de arrestos y reportes de crímenes, junto con información de redes sociales, para identificar, como PredPol "zonas calientes" de actividad delictiva. La policía incrementa la presencia en estas áreas en base a la predicción de que podrían ocurrir delitos, con el fin de prevenir eventos delictivos.

b) Impacto y desafíos éticos: si bien este enfoque ha permitido a la policía reducir la incidencia de algunos delitos, ha sido criticado por el perfilado racial y por reforzar la vigilancia en áreas específicas, muchas veces ocupadas por minorías y grupos socioeconómicamente desfavorecidos.

Este caso también nos muestra cómo el uso de *big data*, aunque eficaz para reducir el delito en ciertos contextos, puede contribuir a una vigilancia desigual y a la percepción de criminalización de comunidades específicas. Por lo demás, la recopilación y uso de datos personales de redes sociales plantea interrogantes sobre el derecho a la privacidad y el consentimiento de las personas cuyos datos son analizados.

Caso 4. Sistema de Crimen Predictivo de IBM en la Policía de Nueva York (*NYPD*)

a) Descripción del caso: el Departamento de Policía de Nueva York (NYPD) ha utilizado un sistema de análisis predictivo desarrollado por IBM para identificar patrones delictivos y focalizar recursos en zonas de mayor riesgo.

Este sistema analiza una amplia gama de datos, desde informes policiales hasta información meteorológica, con el objetivo de predecir dónde y cuándo es más probable que ocurran delitos. Esta iniciativa ha sido parte de un esfuerzo mayor para optimizar la asignación de recursos policiales y mejorar la seguridad pública.

b) Impacto y desafíos éticos: aunque el sistema ha ayudado a reducir la incidencia de algunos delitos en las áreas estudiadas, los críticos señalan que el enfoque puede llevar a una vigilancia excesiva y discriminatoria.

Dado que la mayoría de los datos históricos provienen de comunidades específicas, el sistema tiende a enviar más vigilancia a esos mismos lugares, perpetuando un ciclo de perfilado racial y aumentando la percepción de hostigamiento en ciertas áreas. Este caso subraya la importancia de desarrollar y auditar algoritmos que consideren la justicia social y la equidad, para evitar que los sistemas de big data refuercen desigualdades estructurales en la seguridad pública.

Caso 5. "COMPAS" y el sistema de Justicia Penal en Estados Unidos

a) Descripción del caso: el sistema de evaluación de riesgo conocido por su siglas "COMPAS" (*Correctional Offender Management Profiling for Alternative Sanctions)* es una herramienta de inteligencia artificial y análisis predictivo

ampliamente utilizada en el sistema de justicia penal de Estados Unidos. Diseñado para asistir a jueces y agentes de libertad condicional en la toma de decisiones sobre la libertad bajo fianza, sentencias y la supervisión de los individuos en el sistema, *COMPAS* emplea algoritmos que analizan diversos factores de riesgo para predecir la probabilidad de reincidencia de un acusado.

Este sistema evalúa una amplia gama de variables, desde antecedentes criminales hasta detalles personales, como empleo, educación y relaciones sociales. Estas variables se utilizan para calcular una "puntuación de riesgo" que refleja la probabilidad de que un individuo reincida en la conducta delictiva. Sin embargo, a pesar de su implementación generalizada, *COMPAS* ha sido objeto de numerosas críticas y controversias debido a cuestiones de sesgo racial y falta de transparencia. Estudios han señalado que el sistema tiende a dar puntuaciones de riesgo más altas a personas de raza negra en comparación con personas blancas en situaciones similares, lo cual ha generado preocupaciones sobre la equidad y la discriminación en el uso de estos sistemas automatizados en la justicia.

Otro problema es que el algoritmo de *COMPAS* no es transparente, lo cual significa que los usuarios finales (jueces y agentes de libertad condicional) no conocen los detalles de cómo se ponderan los factores en la generación de la puntuación de riesgo. Esto se conoce como "caja negra algorítmica" (*black box*) ya que el sistema realiza evaluaciones sin que se comprenda completamente su proceso de decisión. Esta falta de transparencia plantea serios problemas éticos y legales, ya que las personas afectadas por estas evaluaciones no pueden impugnar ni comprender cómo se han determinado sus puntuaciones de riesgo.

La eficacia y la equidad del sistema *COMPAS* han suscitado un debate amplio sobre el uso de algoritmos en el sistema de justicia penal, destacando la necesidad de un enfoque ético en el diseño y uso de estas herramientas. La preocupación por la precisión, la transparencia y el sesgo algorítmico es fundamental para evitar que se perpetúen o amplifiquen injusticias en las decisiones judiciales y en las políticas de libertad condicional.

b) Jurisprudencia al respecto:[6]

b.1) State v. Loomis (2016). El sistema de evaluación de riesgo *COMPAS (Correctional Offender Management Profiling for Alternative Sanctions)* se utiliza en varios estados de Estados Unidos para predecir la probabilidad de reincidencia de los delincuentes. Sin embargo, su uso ha generado un intenso debate sobre

[6] Banchio, P. (2024). *La Ética en la inteligencia artificial y los algoritmos a través del análisis de ocho casos jurisprudenciales*. Zenodo. https://doi.org/10.5281/zenodo.12803079.

las implicaciones éticas de basar decisiones judiciales en algoritmos complejos y opacos.

El caso "State v. Loomis" ilustra este debate. La Corte Suprema de Wisconsin analizó la utilización de *COMPAS* en la sentencia de Eric Loomis, quien argumentaba que esta herramienta violaba su derecho al debido proceso. Loomis sostenía que la naturaleza opaca del algoritmo le impedía cuestionar su exactitud o validez, vulnerando sus derechos fundamentales.

La Corte, en una decisión compleja, determinó que el uso de *COMPAS* era constitucional. Sin embargo, enfatizó la necesidad de transparencia en el funcionamiento del algoritmo y recomendó que las evaluaciones de riesgo no sean el único factor determinante en las decisiones judiciales.

Este caso pone de relieve la importancia de la explicabilidad y la supervisión humana en el uso de algoritmos en el sistema de justicia penal. Si bien los algoritmos pueden ser útiles para procesar grandes cantidades de datos y predecir ciertos patrones, no deben sustituir el juicio humano y la comprensión contextual de cada caso.

La decisión en "State v. Loomis" marca un precedente importante en la discusión sobre la ética en el uso de la inteligencia artificial en el ámbito legal. Es crucial establecer mecanismos que garanticen la transparencia, la rendición de cuentas y la protección de los derechos individuales en la implementación de estas tecnologías.

b.2) "EE.UU. v. Hudson" (2016). Los algoritmos, herramientas que automatizan procesos y toman decisiones en base a datos, como *COMPAS* no son inmunes a los sesgos. Estos sesgos pueden generar cierto tipo de discriminación contra determinados grupos de personas, con graves consecuencias en ámbitos como el sistema judicial.

El caso **"**Estados Unidos contra Hudson" ilustra este problema de manera preocupante. En este caso, un tribunal federal de los Estados Unidos dictaminó que el uso de un algoritmo de riesgo *COMPAS* para evaluar a los delincuentes reincidentes era discriminatorio. El algoritmo, utilizado para predecir la probabilidad de reincidencia, tenía más probabilidades de clasificar erróneamente a los acusados negros como de alto riesgo.

¿Cómo se llegó a esta situación? El tribunal determinó que el algoritmo se basaba en datos históricos sesgados. Estos datos, que reflejaban las desigualdades existentes en el sistema penal, llevaron al algoritmo a perpetuar esas mismas desigualdades. Como resultado, los acusados negros eran más propensos a ser erróneamente clasificados como de alto riesgo, lo que se traducía en penas más severas.

Este caso pone de relieve la necesidad de una profunda revisión de los algoritmos utilizados en el sistema judicial. Es crucial implementar medidas que garanticen la imparcialidad y la equidad en su desarrollo y aplicación. No podemos permitir que herramientas que deberían servir para la justicia se conviertan en instrumentos de discriminación.

c) Fuentes de información:

-El País: Discusión sobre el uso de inteligencia artificial en la justicia y los sesgos éticos asociados, incluyendo el caso de COMPAS.
https://elpais.com/tecnologia/2019/11/15/actualidad/1573806116_925631.html

-Redalyc: Análisis sobre COMPAS y otros algoritmos de justicia, explorando variables y consideraciones de derechos humanos.
https://www.redalyc.org/articulo.oa?id=320329114002

-AcademiaLab: Descripción técnica y críticas al algoritmo de COMPAS, incluyendo su impacto en decisiones judiciales.
https://academia-lab.com/articulo/COMPAS

4. Ciberseguridad y crimen organizado

La ciberseguridad se ha convertido en un pilar fundamental en la lucha contra el crimen organizado en la era digital. Con el aumento de la dependencia de las tecnologías digitales, los criminales han adoptado técnicas cibernéticas avanzadas para llevar a cabo delitos que van desde el robo de información hasta el uso de *ransomware* y el *hacking* a gran escala.

En este apartado exploraremos las principales amenazas cibernéticas, la necesidad de infraestructuras seguras y el papel de la ética en la implementación de estrategias de ciberseguridad que prevengan y combatan el crimen organizado.

4.1 Amenazas cibernéticas y crimen organizado

En el ámbito del crimen organizado, las amenazas cibernéticas han adquirido una gran relevancia debido a la facilidad con la que pueden ejecutarse en comparación con métodos tradicionales, y a la capacidad de estas para atravesar fronteras sin la necesidad de una presencia física. Las principales amenazas utilizadas en el ámbito digital por organizaciones criminales incluyen el *hacking*, el *ransomware*, el *phishing*, y los ataques de denegación de servicio distribuido (*DDoS*), entre otros.

4.1.1 *Hacking* y robo de información

El *hacking* consiste en el acceso no autorizado a sistemas o redes con el fin de robar, modificar o destruir información. Esta técnica es utilizada frecuentemente por redes de crimen organizado para robar datos personales, financieros y de propiedad intelectual, y venderlos en el mercado negro.

Los ataques de *hacking* han afectado tanto a individuos como a instituciones gubernamentales y empresas privadas, exponiéndolos a enormes pérdidas financieras y riesgos de reputación. El robo de información confidencial facilita otros crímenes como el fraude financiero y la extorsión, y permite a los delincuentes establecer redes de contactos y clientes dentro de sus propias operaciones delictivas.

4.1.2 *Ransomware* y extorsión digital

El *ransomware* es una forma de *malware* que cifra los datos de la víctima y exige un pago, generalmente en criptomonedas, para desbloquearlos. El *ransomware* ha sido ampliamente utilizado por organizaciones criminales debido a su efectividad y al anonimato que proporcionan los pagos en criptomonedas.

Este tipo de ataque ha paralizado sistemas críticos en hospitales, empresas y servicios gubernamentales, demostrando su capacidad de crear caos y forzar a las víctimas a pagar grandes sumas de dinero. La extorsión digital es particularmente preocupante en infraestructuras críticas, donde las operaciones detenidas pueden poner en riesgo vidas humanas, como es el caso de hospitales o sistemas de transporte.

4.1.3 *Phishing* y estafas online

El *phishing* es una técnica de ingeniería social que engaña a las personas para que proporcionen información personal, como contraseñas y detalles bancarios. Esta técnica es comúnmente utilizada para robar identidades y realizar fraudes financieros, ya que permite a los criminales suplantar la identidad de sus víctimas y acceder a sus cuentas bancarias o realizar compras no autorizadas.

Las redes criminales a menudo utilizan el *phishing* como puerta de entrada para ataques más complejos, como el *hacking* o el *ransomware*, y es especialmente efectivo debido a la falta de educación y conciencia sobre la ciberseguridad en el público general.

4.1.4 Ataques *DDoS* (Denegación de Servicio Distribuido)

Los ataques de denegación de servicio distribuido (*DDoS*) consisten en abrumar un sistema o red con una cantidad masiva de solicitudes para que los servidores no puedan responder, lo cual lleva al colapso del sistema. Estos ataques pueden tener un impacto significativo en la infraestructura digital de una organización, interrumpiendo sus operaciones e impidiendo que los usuarios legítimos accedan a los servicios.

Las organizaciones criminales utilizan los ataques *DDoS* para extorsionar a empresas, amenazando con detener sus operaciones a menos que se les pague una "cuota de protección".

4.2 Construcción de infraestructuras seguras con perspectiva ética

Para enfrentar las amenazas cibernéticas y proteger a las organizaciones y personas de los ataques del crimen organizado, es esencial construir infraestructuras cibernéticas seguras. Sin embargo, esta construcción debe tener en cuenta no solo la seguridad técnica, sino también principios éticos que garanticen un respeto profundo a la privacidad y los derechos de los usuarios.

4.2.1 Principios éticos para la ciberseguridad

La construcción de infraestructuras de ciberseguridad seguras implica una serie de principios éticos esenciales que buscan proteger los derechos y libertades de los individuos y evitar que estas medidas de seguridad se conviertan en herramientas de vigilancia y control. Como hemos expuesto en trabajos anteriores, entre estos principios se incluyen:

a) Privacidad: las infraestructuras de ciberseguridad deben respetar la privacidad de los usuarios, limitando la recopilación y el almacenamiento de datos personales al mínimo necesario y garantizando la confidencialidad de la información.

b) Transparencia: las organizaciones deben ser transparentes en sus prácticas de seguridad y dejar claro cómo protegen los datos y la privacidad de sus usuarios. Esta transparencia genera confianza y permite a los usuarios conocer las medidas de seguridad que protegen su información.

c) Responsabilidad: los desarrolladores y administradores de infraestructuras cibernéticas deben asumir la responsabilidad de prevenir y mitigar los riesgos de

seguridad, así como de realizar auditorías y evaluaciones regulares para identificar posibles vulnerabilidades.

d) Justicia y Equidad: las políticas y procedimientos de ciberseguridad deben

diseñarse de manera que no discriminen ni afecten desproporcionadamente a grupos específicos, garantizando que todos los usuarios tengan acceso a una protección equitativa sin comprometer sus derechos.

4.3 Rol de la Ética en la ciberseguridad

La ética desempeña un papel fundamental en la ciberseguridad, guiando la toma de decisiones en cada etapa, desde el diseño hasta la implementación de políticas y medidas de seguridad. La consideración ética en la ciberseguridad ayuda a equilibrar la necesidad de proteger la infraestructura y los datos con la obligación de respetar los derechos y libertades individuales.

4.3.1 Ética en el diseño de estrategias de ciberseguridad

Las decisiones éticas deben estar presentes desde la etapa de diseño de una infraestructura de ciberseguridad.

Los desarrolladores y arquitectos de seguridad deben considerar el impacto de sus decisiones en los derechos de los usuarios, diseñando soluciones que garanticen la protección de la privacidad y minimicen la posibilidad de uso indebido de los datos. Este enfoque ético puede incluir prácticas como la "anonimización: de datos, la minimización de recopilación de información personal y la implementación de políticas claras de gestión de acceso.

4.3.2 Ética en la implementación y el monitoreo

La implementación de estrategias de ciberseguridad también debe estar guiada por principios éticos, especialmente en cuanto a la transparencia y la justicia. Las organizaciones deben comunicar a sus usuarios cómo están protegiendo sus datos y proporcionar acceso a mecanismos de resolución de conflictos en caso de vulneraciones de seguridad.

Además, el monitoreo de la actividad en redes e infraestructuras debe realizarse respetando la privacidad de los usuarios y evitando prácticas de vigilancia excesiva.

4.3.3 Prevención del crimen organizado con perspectiva ética

Al aplicar medidas de ciberseguridad para prevenir el crimen organizado, es esencial encontrar un equilibrio entre la necesidad de detener actividades ilícitas y la protección de los derechos humanos. Las estrategias de ciberseguridad no deben caer en la tentación de priorizar la seguridad a expensas de los derechos individuales. En este contexto, la ética actúa como un marco regulador que ayuda a los profesionales de la ciberseguridad a tomar decisiones informadas y equilibradas.

4.4 Análisis de casos reales

La aplicación de estrategias de ciberseguridad en la lucha contra el crimen organizado ha mostrado diversos resultados en Europa y América Latina, debido a las diferencias en recursos tecnológicos, normativas, y niveles de cooperación internacional en cada región. A continuación, se presentan varios casos reales que ilustran tanto el éxito como los desafíos de la ciberseguridad en la contención de actividades delictivas organizadas.

Caso 1. "EncroChat" y la Red de Comunicación Criminal

a) Descripción del caso: en Europa, uno de los casos de ciberseguridad más

significativos fue la operación de infiltración en la red de comunicación encriptada EncroChat, que desveló la magnitud de la infraestructura digital utilizada por organizaciones criminales. EncroChat era una plataforma de comunicación cifrada ampliamente utilizada por grupos criminales para coordinar actividades ilícitas, como el tráfico de drogas, el lavado de dinero y los asesinatos por encargo. La red de EncroChat contaba con decenas de miles de usuarios, de los cuales un alto porcentaje estaba vinculado a actividades ilegales.

En 2020, las autoridades francesas y neerlandesas lograron acceder a la red de EncroChat tras varios meses de investigaciones y decodificación de las comunicaciones cifradas. Este acceso permitió a las autoridades monitorear miles de conversaciones en tiempo real, obteniendo evidencia crucial para desmantelar operaciones criminales en varios países europeos, incluyendo Reino Unido, Francia, Países Bajos y España.

b) Resultados y desafíos éticos: la infiltración en EncroChat fue un logro importante en la lucha contra el crimen organizado; sin embargo, planteó varios

dilemas éticos. Por un lado, las autoridades lograron prevenir crímenes y recopilar información invaluable sobre las redes delictivas. Por otro lado, la intervención también generó preocupaciones sobre el derecho a la privacidad y la legitimidad del monitoreo generalizado de las comunicaciones cifradas. Además, la operación se topó con el reto de presentar pruebas que fueran admisibles en los sistemas judiciales de diferentes países, ya que el origen de las pruebas obtenidas mediante la infiltración presentaba desafíos legales en términos de derecho a un juicio justo y a la privacidad de los individuos monitoreados.

c) Fuentes de información:

-ElDiario.es: Europa logra interceptar la red de comunicaciones EncroChat, usada principalmente en actividades criminales.
https://www.eldiario.es/tecnologia/europa-rompe-cifrado-encrochat_1_6109656.html

-Público: Descripción de la intervención de EncroChat y su impacto en redes criminales.
https://www.publico.es/internacional/operacion-policial-red-encrochat-criminales.html

-Confilegal: La Audiencia Nacional de España ratifica la validez de pruebas de EncroChat, destacando la cooperación judicial en la Unión Europea para casos de crimen organizado.
https://confilegal.com/20230615-audiencia-nacional-legalidad-pruebas-encrochat

-Confilegal: Opinión de la abogada general del TJUE sobre el uso de órdenes europeas de investigación y el rol de la fiscalía en casos de EncroChat.
https://confilegal.com/20231010-fiscalia-orden-europea-investigacion-encrochat

Caso 2. "Lava Jato" y el uso de ciberseguridad en la investigación de lavado de dinero

a) Descripción del caso: el caso del Lava Jato en Brasil representa una de las investigaciones de corrupción y lavado de dinero más grandes en América Latina, implicando tanto a funcionarios gubernamentales como a grandes corporaciones.

La investigación reveló un esquema de corrupción en el que varias empresas de construcción sobornaron a políticos y ejecutivos de la empresa petrolera estatal Petrobras para asegurar contratos lucrativos.

Para enfrentar la sofisticación de las actividades delictivas y el volumen de información, las autoridades utilizaron avanzadas técnicas de ciberseguridad y análisis de *big data*, permitiéndoles descifrar registros financieros, monitorear transferencias de dinero sospechosas y vincular digitalmente a los involucrados.

b) Resultados y dilemas éticos: el Lava Jato tuvo un impacto profundo en la política y la economía de Brasil, y sus efectos se extendieron a otros países de América Latina donde los mismos actores habían realizado actividades corruptas.

Sin embargo, el uso intensivo de tecnologías de ciberseguridad también generó controversias, especialmente en torno a la recopilación masiva de datos de comunicaciones privadas, lo que provocó cuestionamientos sobre el equilibrio entre la protección de los derechos individuales y la eficacia de las medidas anticorrupción. Además, el proceso de judicialización de la información digitalizada se enfrentó a obstáculos legales relacionados con la integridad de las pruebas digitales y su recolección en diversas jurisdicciones.

Caso 3. Redes de tráfico humano en la Unión Europea

Otro ejemplo importante en el ámbito europeo es la investigación de redes de tráfico humano, particularmente aquellas que operan entre Europa del Este y Europa Occidental.

Utilizando técnicas avanzadas de ciberseguridad y análisis de big data, las fuerzas policiales han logrado identificar redes de tráfico humano que utilizan redes sociales y aplicaciones de mensajería encriptada para captar víctimas y coordinar su transporte a distintos países de Europa Occidental.

Un caso reciente en Alemania reveló cómo una red criminal organizada utilizaba sitios *web* y aplicaciones encriptadas para captar y trasladar a mujeres jóvenes desde Rumanía y Hungría hacia el oeste, explotándolas en redes de prostitución forzada.

a) Resultados y desafíos éticos: la infiltración en estas redes de tráfico humano demostró la eficacia de la ciberseguridad y el análisis digital para identificar patrones de actividad sospechosa y desmantelar redes de captación. Sin embargo, el proceso también enfrenta desafíos éticos, como el riesgo de vigilancia masiva y la posibilidad de interceptar comunicaciones de personas no involucradas en actividades delictivas.

Además, las operaciones transnacionales exigen la cooperación entre varios países, lo cual implica la armonización de normativas de protección de datos, privacidad y procedimientos legales, un desafío aún no resuelto en su totalidad.

Caso 4. Narcotráfico en América Latina y el uso de criptomonedas

En América Latina, el uso de criptomonedas se ha popularizado en los últimos años entre las organizaciones criminales, especialmente en el narcotráfico. Los carteles han adoptado criptomonedas como el Bitcoin para realizar transacciones internacionales, aprovechando el anonimato que ofrecen estas monedas para lavar dinero y financiar sus operaciones.

Un caso destacado en México mostró cómo una red de narcotraficantes utilizaba una combinación de criptomonedas y plataformas digitales de intercambio para blanquear dinero a través de intermediarios en Asia y Europa.

a) Resultados y desafíos éticos: este caso resaltó la dificultad de rastrear las transacciones en criptomonedas y el reto de establecer regulaciones internacionales efectivas en el manejo de estas. Además, la lucha contra el uso del Bitcoin y otras criptomonedas en actividades ilícitas ha planteado dilemas éticos significativos, como el conflicto entre el derecho a la privacidad financiera y la necesidad de transparencia en transacciones de grandes sumas de dinero.

Las autoridades deben encontrar formas de controlar y supervisar las criptomonedas sin vulnerar el derecho a la privacidad de los usuarios, especialmente aquellos que utilizan estas tecnologías de forma legal y ética.

4.5 Reflexiones finales del apartado

El papel de la ciberseguridad en la lucha contra el crimen organizado es fundamental para proteger a las personas, las empresas y los gobiernos de las amenazas digitales. Sin embargo, para que estas estrategias sean verdaderamente efectivas y justas, es necesario integrar una perspectiva ética en cada fase de su diseño y aplicación.

Las infraestructuras de seguridad deben construirse con principios éticos claros que garanticen la privacidad y equidad, y deben supervisarse de forma continua para evitar cualquier desviación hacia prácticas discriminatorias o invasivas. Con un enfoque ético y responsable, la ciberseguridad puede ser una herramienta poderosa para combatir el crimen organizado y proteger los derechos fundamentales de los individuos en la era digital.

Los casos reales que hemos desarrollado nos muestran que, aunque la ciberseguridad y las tecnologías digitales ofrecen herramientas poderosas para combatir el crimen organizado, también conllevan riesgos éticos y legales que deben ser abordados. En particular, los casos de “EncroChat” y “Lava Jato” subrayan la necesidad de un equilibrio entre la efectividad de las investigaciones

y la protección de los derechos individuales, mientras que las redes de tráfico humano y el uso de criptomonedas en el narcotráfico destacan los desafíos específicos en la vigilancia y supervisión de actividades transnacionales.

Estos ejemplos evidencian que los esfuerzos de ciberseguridad en la lucha contra el crimen organizado deben estar acompañados por una sólida perspectiva ética que guíe la recopilación y uso de información y garantice que las prácticas de ciberseguridad respeten los derechos fundamentales de los individuos.

5. Normativa internacional sobre el crimen organizado

En este apartado resumiremos brevemente las dos principales normas del marco regulatorio en materia internacional que rige la lucha contra el crimen organizado, con un enfoque en cómo los tratados y convenios internacionales abordan las complejidades tecnológicas actuales.

En particular, examinaremos los dos principales acuerdos internacionales vigentes, su impacto y eficacia en un contexto digital en constante evolución, y los desafíos que enfrentan los países para implementar y adaptar estas regulaciones en la era de las nuevas tecnologías.

Finalmente, como es nuestro estilo, propondremos algunas recomendaciones de *lege ferenda* para hacer frente a los desafíos de las nuevas tecnologías frente a esta normativa internacional en vigor.

5.1 Convención de Palermo

En la lucha contra el crimen organizado, los convenios internacionales desempeñan un papel fundamental al establecer un marco jurídico común que permite la cooperación y la coordinación transfronterizas.

Uno de los tratados clave en este ámbito es la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, también conocida como Convención de Palermo (2000), aprobada por Ley 25.632, sancionada y promulgada en agosto de 2002.

Este acuerdo, firmado por más de 190 países, es el primer instrumento global que define el delito de crimen organizado transnacional y sienta las bases jurídicas para la cooperación en varias áreas, tales como el lavado de dinero, la corrupción y el tráfico de personas.

La Convención de Palermo se articula a través de tres protocolos que abordan aspectos específicos del crimen organizado: el "Protocolo contra la Trata de

Personas", el "Protocolo contra el Tráfico Ilícito de Migrantes" y el "Protocolo contra la Fabricación y el Tráfico Ilícito de Armas de Fuego". Estos instrumentos buscan armonizar las definiciones de delitos y fomentar la colaboración entre los Estados para enfrentar problemas complejos en el ámbito transnacional.

5.2 Convención de Naciones Unidas

Además de la Convención de Palermo, la Convención de las Naciones Unidas contra la Corrupción (CNUCC) (2003) es otro acuerdo esencial para combatir el crimen organizado que fue aprobado por Ley 26.097, sancionada en mayo de 2006

Este convenio se centra en erradicar la corrupción en los sectores público y privado, ya que la corrupción suele ser un facilitador crítico para el funcionamiento de redes delictivas. La CNUCC establece medidas para la prevención, criminalización, cooperación internacional y recuperación de activos obtenidos a través de la corrupción, y promueve la transparencia y la rendición de cuentas en los sistemas judiciales y financieros.

5.3 Impacto y eficacia de las normas internacionales en la Era Digital

El avance de las tecnologías digitales ha creado nuevas oportunidades y desafíos para la aplicación de las normas internacionales en la lucha contra el crimen organizado. Si bien la Convención de Palermo y la CNUCC proporcionan una estructura jurídica sólida, en muchos casos resulta insuficiente para abordar los aspectos específicos del entorno digital.

El uso de criptomonedas, redes encriptadas y transacciones digitales transfronterizas por parte de las organizaciones criminales ilustra la necesidad de actualizar y adaptar estos convenios para enfrentar los nuevos métodos utilizados por los delincuentes.

Uno de los impactos positivos de estos convenios es que han facilitado el desarrollo de sistemas de cooperación entre países, permitiendo el intercambio de información y la realización de investigaciones conjuntas en casos de crimen organizado. Las plataformas de Interpol y Europol, así como las unidades de inteligencia financiera (UIF), son ejemplos de cómo los acuerdos internacionales contribuyen a crear redes de cooperación en un contexto digital.

No obstante, la eficacia de las normas internacionales se ve limitada por la falta de armonización en las legislaciones nacionales y las diferencias en los recursos tecnológicos entre los países. En muchos casos, las legislaciones locales

no logran equiparar el nivel de detalle y actualización que requieren los convenios internacionales, lo cual dificulta su aplicación uniforme en los Estados parte. A su vez, la falta de infraestructura tecnológica avanzada y de personal especializado en algunos países limita la capacidad para implementar efectivamente las normas en contextos digitales.

5.4 Desafíos de implementación en nuevas tecnologías

La implementación de los convenios internacionales en la era de las nuevas tecnologías enfrenta diversos desafíos, tales como la velocidad de desarrollo tecnológico,

las diferencias en los marcos regulatorios y la capacidad de supervisión y control.

En primer lugar, la rapidez con la que evolucionan las tecnologías digitales representa un obstáculo, ya que los convenios internacionales suelen estar formulados para contextos menos dinámicos y requieren de períodos largos para ser negociados y aprobados y muchas veces convierte al Derecho en un indicador del pasado. Esto resulta en un retraso regulatorio que organizaciones criminales pueden aprovechar para operar con impunidad.

El modelo normativo concebido como experiencia mutiladora en el positivismo del siglo XIX, siempre viene después, *ex post facto*, y se encuentra por ello, imposibilitado de encontrar respuestas anticipatorias. La norma consagra, afirma y testimonia una realidad anterior -*ex ante*- pero no la produce. Por ello, venimos propugnando, con el modelo del Tetraedro[7], que el Derecho elabore respuestas jurídicas estratégicas anticipatorias y futurizas desde sus despliegues integrales en busca de la justicia en lugar de imaginar un mundo fantástico y escribir normas con la inquietante idea de que podrá hacerse esa ingeniería social ya que el Derecho debe descubrirse y no inventarse.

Un ejemplo claro, de este desafío en la temática que estamos tratando, es la regulación de las criptomonedas en el marco de la Convención de Palermo. Aunque la convención aborda el lavado de dinero y el financiamiento de actividades ilícitas, no incluye disposiciones específicas para las criptomonedas, un medio comúnmente utilizado en el crimen organizado. Este vacío jurídico dificulta la aplicación de las normas y permite que los delincuentes se aprovechen del anonimato y la descentralización que ofrecen estas tecnologías.

[7] Banchio, P. (2018). *El Tetraedro del Derecho. Aportes para una Teoría General del Derecho Privado*. Buenos Aires, 20 de marzo de 2018. CERN European Organization for Nuclear Research - Zenodo. https://doi.org/10.5281/zenodo.5513094, *cit.*

Otro desafío importante es la protección de los derechos humanos en la aplicación de nuevas tecnologías contra el crimen organizado. Las prácticas de vigilancia y recolección de datos masivos pueden entrar en conflicto con el derecho a la privacidad, especialmente cuando las investigaciones transnacionales utilizan datos personales sin el consentimiento explícito de los individuos. La protección de la privacidad y la salvaguarda de los derechos individuales son esenciales para que los esfuerzos internacionales contra el crimen organizado mantengan su legitimidad y ética.

Finalmente, como anticipamos, las diferencias en la capacidad de supervisión y control entre los países constituyen un obstáculo significativo. Mientras que los países más desarrollados cuentan con sistemas avanzados de monitoreo y ciberseguridad, las naciones con menos recursos tecnológicos y económicos enfrentan dificultades para implementar las disposiciones de los convenios internacionales. Esto genera un desequilibrio en la capacidad de aplicación, lo que permite que el crimen organizado se traslade hacia regiones con menor capacidad de supervisión y control.

5.5 Recomendaciones para fortalecer la colaboración internacional

Para superar estos desafíos y mejorar la eficacia de las normas internacionales en la era digital, se proponen las siguientes recomendaciones:

a) Revisión y actualización de los convenios internacionales: Es fundamental que los tratados como la Convención de Palermo y la CNUCC sean revisados periódicamente para incluir disposiciones específicas sobre tecnologías emergentes, tales como criptomonedas, inteligencia artificial y análisis de big data. La inclusión de protocolos específicos para el ámbito digital permitiría a los Estados miembro abordar los nuevos métodos y técnicas utilizadas por el crimen organizado.

b) Fortalecimiento de la cooperación tecnológica entre países: La creación de redes de cooperación en ciberseguridad y la estandarización de herramientas digitales para la detección y monitoreo de actividades ilícitas son esenciales. Programas de asistencia técnica y capacitación en ciberseguridad, especialmente para países en vías de desarrollo, permitirían una implementación más uniforme de los convenios y una mayor equidad en la lucha contra el crimen organizado.

c) Promoción de políticas de respeto a los derechos humanos: La aplicación de tecnologías digitales debe realizarse bajo principios de proporcionalidad y respeto a los derechos fundamentales de las personas. Es crucial que la cooperación internacional incluya salvaguardas de derechos humanos y

mecanismos de rendición de cuentas para prevenir abusos y garantizar que las investigaciones se realicen de manera ética.

d) Creación de un marco regulador específico para criptomonedas en el contexto de crimen organizado: Dada la creciente utilización de criptomonedas por organizaciones criminales, es recomendable que los tratados internacionales incluyan directrices para su monitoreo y regulación. Este marco debería contemplar un enfoque equilibrado entre el control de actividades ilícitas y el respeto a la privacidad financiera.

e) Establecimiento de un observatorio internacional de nuevas tecnologías y crimen organizado: La creación de una entidad internacional que monitoree el uso de tecnologías en el crimen organizado y emita recomendaciones a los Estados miembros permitiría una respuesta más ágil ante los avances tecnológicos. Este observatorio podría colaborar con instituciones académicas y organizaciones no gubernamentales para producir informes y alertas sobre tendencias y riesgos emergentes.

Estas recomendaciones buscan optimizar el impacto de los convenios internacionales en un entorno cada vez más digitalizado y ayudar a los Estados a enfrentar los desafíos de la lucha contra el crimen organizado en la era de la tecnología avanzada.

6. Conclusión

En el articulo para la disertación que en estas líneas finaliza hemos intentado abordar los complejos desafíos y oportunidades que la tecnología presenta en la lucha contra el crimen organizado, así como el papel fundamental de la cooperación internacional y la regulación en este ámbito. La evolución tecnológica ha dado lugar a herramientas poderosas para detectar y combatir actividades delictivas, tales como la tecnología *blockchain*, el análisis de *big data* y la ciberseguridad. Sin embargo, estas innovaciones también han planteado dilemas éticos y han creado nuevas vulnerabilidades que requieren un enfoque de gobernanza global y colaborativo.

En el primer apartado, bajo el inciso 2, examinamos cómo la tecnología *blockchain* puede apoyar la trazabilidad en las transacciones financieras, lo cual es crucial para combatir el tráfico de personas y el lavado de dinero. Sin embargo, también se exploraron los riesgos asociados, como el anonimato y la descentralización, que pueden ser aprovechados por organizaciones criminales. Este análisis muestra que, si bien *blockchain* tiene un gran potencial en la lucha

contra el crimen organizado, su uso debe ir acompañado de regulaciones específicas y salvaguardas éticas para evitar un uso indebido.

El segundo apartado, en el punto 3, intentamos profundizar en el análisis de *big data* y su aplicación en la seguridad pública. La capacidad de los sistemas de *big data* para detectar patrones delictivos y desmantelar redes de crimen organizado es un recurso poderoso, pero plantea riesgos significativos en términos de perfilado racial y discriminación. A través de la revisión de casos reales, se constató la necesidad de regular el uso de *big data* para minimizar los sesgos y proteger los derechos humanos, asegurando que la justicia y la equidad no se vean comprometidas en la búsqueda de seguridad.

En el tercer apartado (punto 4), la investigación analizó el papel de la ciberseguridad en la protección de las infraestructuras digitales contra las amenazas del crimen organizado. La ciberseguridad emerge no solo como una necesidad técnica, sino también como una responsabilidad ética para prevenir ataques y proteger datos sensibles. Los ejemplos revisados muestran que la construcción de infraestructuras cibernéticas seguras debe incorporar valores éticos fundamentales, promoviendo la protección de la privacidad y la transparencia en la prevención del crimen.

Finalmente, en el cuarto apartado, bajo el inciso 5, revisamos los principales convenios internacionales y se evaluó su eficacia en el contexto digital. La Convención de Palermo y la Convención de las Naciones Unidas contra la Corrupción ofrecen un marco indispensable para la cooperación global, pero también enfrentan retos para adaptarse a las tecnologías emergentes y al entorno digital. Los vacíos en la regulación de criptomonedas y la falta de armonización en las capacidades tecnológicas de los países dificultan una aplicación uniforme de estos acuerdos, lo que subraya la importancia de revisar y actualizar las normas internacionales de manera continua.

En conclusión, la lucha contra el crimen organizado en la era digital requiere una integración armoniosa de tecnología, ética y regulación internacional. Las herramientas tecnológicas pueden fortalecer los esfuerzos para combatir redes criminales transnacionales, pero su uso debe ser guiado por principios éticos que protejan los derechos humanos y por marcos normativos flexibles y actualizables. La cooperación internacional es clave en este proceso; solo mediante un esfuerzo coordinado que incorpore una visión ética y regulatoria en las nuevas tecnologías, será posible enfrentar eficazmente los desafíos del crimen organizado en el siglo XXI.

7. Referencias

7.1 Bibliografía

Banchio, P. (2018). *El Tetraedro del Derecho. Aportes para una Teoría General del Derecho Privado*. Buenos Aires, 20 de marzo de 2018. CERN European Organization for Research - Zenodo. https://doi.org/10.5281/zenodo.5513094.

Banchio, P. (2022). *Nuevas Tecnologías y Derecho*. Perspectivas Jurídicas. Buenos Aires, 2022.

Banchio, P. (2023). *Nueva legislación europea sobre las plataformas digitales: regulación, implicaciones y desafíos de implementación*. Jornada Ítalo-Argentina de Derecho Civil. Academia Nacional de Ciencias de Buenos Aires, Buenos Aires, Argentina. https://doi.org/10.5281/zenodo.11077619

Banchio, P. (2023). *Nuova normativa europea sulle piattaforme digitali: regolamentazione, implicazioni e sfide di attuazione*. Conferenza binazionale di Diritto Civile. Accademia Nazionale delle Scienze di Buenos Aires, Buenos Aires, Argentina. https://doi.org/10.5281/zenodo.11077576

Banchio, P. (2023). *Reflections on a Legal Framework for Artificial Intelligence*. *Artificial Intelligence eJournal*, 6(47). http://dx.doi.org/10.2139/ssrn.4320870

Banchio, P. (2024). *Algorética*. Zenodo. https://doi.org/10.5281/zenodo.12806322

Banchio, P. (2024). *Desafíos legales, éticos y prácticos de la moderación de contenido impulsada por inteligencia artificial*. Zenodo. https://doi.org/10.5281/zenodo.13896337

Banchio, P. (2024). *Discriminación algorítmica: un análisis jurídico de los desafíos y oportunidades en la era digital*. Zenodo. https://doi.org/10.5281/zenodo.12790078

Banchio, P. (2024) Existencialismo y tecnología. Desafíos éticos de la autonomía y la autenticidad en la era digital. *Doctrina Jurídica,* XV(35), noviembre de 2024

Banchio, P. (2024). *Humanismo algorítmico y transparencia digital: un enfoque centrado en los valores humanos*. Zenodo. https://doi.org/10.5281/zenodo.12790268

Banchio, P. (2024). *Impacto ambiental de la Inteligencia Artificial. Análisis, desafíos y estrategias para un desarrollo sostenible*. Zenodo. https://doi.org/10.5281/zenodo.13624181

Banchio, P. (2024). *Inteligencia artificial en la moderación de contenidos online*. Zenodo. https://doi.org/10.5281/zenodo.13901543

Banchio, P. (2024). *La Ética en la inteligencia artificial y los algoritmos a través del análisis de ocho casos jurisprudenciales*.
Zenodo. https://doi.org/10.5281/zenodo.12803079

Banchio, P. (2024). *Legal Framework to Combat Disinformation and Hate Speech on Digital Platforms*. *Law & Society: International & Comparative Law eJournal*, 19(67). http://dx.doi.org/10.2139/ssrn.4879162

Banchio, P. (2024). *Legal Responses to Disinformation and Hate Speech in the Digital Age*. *AI and Human Rights Law Journal*, 2(4).
Zenodo. https://doi.org/10.5281/zenodo.12594869

Banchio, P. (2024). *L'impatto dell'intelligenza artificiale sulle risorse umane*. *AI and Human Rights Law Journal*, 2(6), 21-29.
Zenodo. https://doi.org/10.5281/zenodo.12737782

Banchio, P. (2024). *L'intelligenza artificiale nella moderazione dei contenuti online*. *AI and Human Rights Law Journal*, 4(5), 3-20.
Zenodo. https://doi.org/10.5281/zenodo.12744750

Banchio, P. (2024). *Risposte giuridiche all'intelligenza artificiale: umanesimo algorítmico e trasparenza digitale*.
Zenodo. https://doi.org/10.5281/zenodo.11073624

7.2 Fuentes de información

AcademiaLab: Descripción técnica y críticas al algoritmo de COMPAS, incluyendo su impacto en decisiones judiciales.
https://academia-lab.com/articulo/COMPAS

Clarín: "Blockchain y la lucha contra la trata de personas"
https://www.clarin.com/tecnologia/blockchain-lucha-trata-personas_0_NiqiEJPgX.html

Cointelegraph: Información sobre la recuperación de fondos y el hackeo de Bitfinex en 2016
https://es.cointelegraph.com/news/us-recovers-bitfinex-hack-funds

Cointelegraph: Debate sobre la compensación a los titulares de tokens LEO tras la recuperación de los fondos
https://es.cointelegraph.com/news/bitfinex-fund-recovery-implications

Confilegal: La Audiencia Nacional de España ratifica la validez de pruebas de EncroChat, destacando la cooperación judicial en la Unión Europea para casos

de crimen organizado.
https://confilegal.com/20230615-audiencia-nacional-legalidad-pruebas-encrochat

Confilegal: Opinión de la abogada general del TJUE sobre el uso de órdenes europeas de investigación y el rol de la fiscalía en casos de EncroChat.
https://confilegal.com/20231010-fiscalia-orden-europea-investigacion-encrochat

El Diario El Salvador: Artículo sobre Tether y su uso en actividades ilícitas, en relación con Bitfinex
https://www.elsalvador.com/noticias/finanzas/tether-fondos-ilicitos-bitfinex/1014901/2023/

El Español: "Traffik Analysis Hub, una plataforma que lucha contra la trata de personas con tecnología de IA"
https://www.elespanol.com/invertia/empresas/tecnologia/20191122/traffik-analysis-hub-plataforma-personas-tecnologia-ia/446126665_0.html

El País: Discusión sobre el uso de inteligencia artificial en la justicia y los sesgos éticos asociados, incluyendo el caso de COMPAS.
https://elpais.com/tecnologia/2019/11/15/actualidad/1573806116_925631.html

ElDiario.es: Europa logra interceptar la red de comunicaciones EncroChat, usada principalmente en actividades criminales.
https://www.eldiario.es/tecnologia/europa-rompe-cifrado-encrochat_1_6109656.html

Mundo Cloud: "Pasos Libres y la lucha contra la trata de personas mediante la tecnología blockchain"
https://mundo.cloud/ibm/pasos-libres-y-la-lucha-contra-la-trata-de-personas-mediante-la-tecnologia-blockchain

Público: Descripción de la intervención de EncroChat y su impacto en redes criminales.
https://www.publico.es/internacional/operacion-policial-red-encrochat-criminales.html

Redalyc: Análisis sobre COMPAS y otros algoritmos de justicia, explorando variables y consideraciones de derechos humanos.
https://www.redalyc.org/articulo.oa?id=320329114002.