



UNIVERSIDAD CATÓLICA DE CÓRDOBA  
FACULTAD DE DERECHO Y CIENCIAS SOCIALES

**Seminario Optativo II: “Blockchain e IA”**

Trabajo de Investigación:

**“INVESTIGACIÓN PENAL EN ENTORNOS DIGITALES. EL AGENTE  
ENCUBIERTO Y EL USO DE LA INTELIGENCIA ARTIFICIAL EN EL PROCESO  
PENAL DE CÓRDOBA.”**

**Autores:**

*BRUSA, Mateo*

*CAMELINO, Delfina*

*GÓMEZ DEMMEL, María José*

**Profesor:**

*VILLALBA, Jorge Fabián*

Córdoba, Noviembre de 2025.

**“INVESTIGACIÓN PENAL EN ENTORNOS DIGITALES. EL AGENTE**

# ENCUBIERTO Y EL USO DE LA INTELIGENCIA ARTIFICIAL EN EL PROCESO PENAL DE CÓRDOBA”

## RESUMEN

Este trabajo de investigación, realizado por estudiantes de la Universidad Católica de Córdoba en el Seminario Optativo "Blockchain e IA", aborda la impostergable necesidad de adaptar la justicia penal cordobesa a la era digital.

En un contexto de delitos crecientes y "delincuentes sin rostro" que operan en entornos virtuales, cometiendo crímenes graves como el "Grooming" y la distribución de material de abuso sexual infantil, el proyecto se alza como una herramienta innovadora y disruptiva. Su objetivo principal es analizar la aplicación de la Inteligencia Artificial (IA) para crear perfiles digitales robustos que asistan a los agentes encubiertos digitales, permitiéndoles infiltrarse de manera verosímil y segura en organizaciones criminales virtuales.

El proyecto subraya un vacío legal crítico: la Provincia de Córdoba carece de un marco normativo que regule esta figura y el uso de la IA, lo que limita la eficacia investigativa y plantea un riesgo de nulidad procesal. Para subsanar esta tensión, se concluye con una propuesta de codificación integral, que busca dotar al Ministerio Público Fiscal de las herramientas de última generación, como la IA y la tecnología blockchain (para garantizar la integridad y trazabilidad de la evidencia), mientras asegura un estricto control judicial y el respeto de las garantías constitucionales.

Este proyecto es una hoja de ruta para cerrar la brecha entre el delito digital y la capacidad de respuesta legal, posicionando a Córdoba como referente nacional y garantizando que el Estado pueda proteger a las víctimas y fortalecer la acción de la justicia en el siglo XXI.

## PALABRAS CLAVE

**Agente Encubierto Digital:** funcionario autorizado por el Ministerio Público Fiscal que interviene en entornos virtuales bajo identidad digital simulada, con el objetivo de prevenir, investigar o reunir pruebas sobre delitos informáticos complejos.

**Identidad Digital Simulada:** representación virtual de un individuo creada con fines de investigación, que permite al agente encubierto interactuar de manera verosímil en plataformas digitales sin revelar su identidad real.

**Ministerio Público Fiscal (MPF):** es el organismo autónomo del Estado encargado de la investigación y persecución de delitos, la protección de los intereses de la sociedad y la defensa del orden legal. Actúa en el ámbito penal dirigiendo investigaciones, presentando acusaciones ante los tribunales y asegurando que se respeten los derechos de las víctimas y de la sociedad en general.

**Inteligencia Artificial (IA):** conjunto de herramientas y sistemas digitales que permiten automatizar procesos, analizar datos y simular conductas humanas. En este contexto, la IA se emplea para generar perfiles digitales verosímiles que facilitan la actuación de agentes encubiertos en investigaciones penales.

**Blockchain / Cadena de Custodia Digital:** tecnología descentralizada que asegura la integridad, trazabilidad e inalterabilidad de los registros digitales. En el proyecto, se plantea como mecanismo para preservar la evidencia y garantizar la confiabilidad de las actuaciones de los agentes encubiertos digitales.

**Delitos Informáticos / Cibercrimen:** actividades ilícitas cometidas mediante el uso de tecnologías digitales, como grooming, distribución de material de abuso sexual infantil, fraude digital o tráfico de estupefacientes online.

**Marco Normativo:** conjunto de leyes, normas y procedimientos que autorizan y delimitan la actuación de los agentes encubiertos digitales y el uso de IA en investigaciones penales.

**Garantías Procesales:** principios jurídicos que protegen los derechos de todas las partes en el proceso penal.

**Investigación Penal Preparatoria:** etapa inicial del proceso penal destinada a la recopilación de pruebas y esclarecimiento de los hechos delictivos, bajo la dirección del Ministerio Público Fiscal y con control judicial.

**Proyecto de Ley:** propuesta normativa que busca formalizar la actuación del agente encubierto digital, regular el uso de IA en investigaciones penales y establecer mecanismos de supervisión, trazabilidad y control judicial en Córdoba.

## **ABSTRACT**

This research paper, conducted by students of the Universidad Católica de Córdoba within the elective seminar “Blockchain and Artificial Intelligence,” addresses the urgent necessity of adapting the criminal justice system of the Province of Córdoba to the demands of the digital era.

Within a context of increasing criminal activity and the emergence of “faceless offenders” operating in virtual environments—perpetrating serious crimes such as grooming and the distribution of child sexual

abuse material—this project arises as an innovative and disruptive initiative. Its primary objective is to examine the application of Artificial Intelligence (AI) in developing robust digital profiles to support digital undercover agents, thereby enabling credible and secure infiltration into virtual criminal organizations.

The study underscores a critical legal gap: the Province of Córdoba currently lacks a normative framework regulating both this figure and the use of AI, which constrains investigative effectiveness and generates a risk of procedural nullity. To address this deficiency, the paper concludes with a proposal for comprehensive codification, aimed at equipping the Public Prosecutor's Office with state-of-the-art technological tools—such as AI and blockchain technology—to ensure the integrity and traceability of digital evidence, while simultaneously guaranteeing strict judicial oversight and full respect for constitutional rights and procedural safeguards.

This project thus constitutes a roadmap for bridging the gap between digital crime and the legal system's capacity for response, positioning Córdoba as a national benchmark and ensuring that the State can effectively protect victims and strengthen the administration of justice in the twenty-first century.

## KEY WORDS

**Digital Undercover Agent:** public official authorized by the Public Prosecutor's Office to operate in virtual environments under a simulated digital identity, with the purpose of preventing, investigating, or gathering evidence on complex cybercrimes.

**Simulated Digital Identity:** virtual representation of an individual created for investigative purposes, allowing the undercover agent to interact credibly within digital platforms without disclosing their real identity.

**Public Prosecutor's Office:** is the autonomous state body responsible for investigating and prosecuting crimes, protecting society's interests, and defending the legal order. It operates in the criminal justice system by directing investigations, presenting charges in court, and ensuring that the rights of victims and society are upheld.

**Artificial Intelligence (AI):** a set of digital tools and systems designed to automate processes, analyze data, and simulate human behavior. In this context, AI is employed to generate credible digital profiles that facilitate the performance of undercover agents in criminal investigations.

**Blockchain / Digital Chain of Custody:** decentralized technology that ensures the integrity, traceability, and immutability of digital records. Within this project, it is proposed as a mechanism to

preserve evidence and guarantee the reliability of digital undercover operations.

**Cybercrime / Computer-Related Offenses:** illicit activities committed through the use of digital technologies, such as grooming, distribution of child sexual abuse material, digital fraud, or online drug trafficking.

**Normative Framework:** the body of laws, regulations, and procedures that authorize and delimit the operation of digital undercover agents and the use of AI in criminal investigations.

**Procedural Safeguards:** legal principles that protect the rights of all parties involved in criminal proceedings.

**Preliminary Criminal Investigation:** the initial stage of the criminal process aimed at gathering evidence and clarifying criminal acts, under the direction of the Public Prosecutor's Office and subject to judicial oversight.

**Draft Bill:** legislative proposal seeking to formalize the operation of the digital undercover agent, regulate the use of AI in criminal investigations, and establish mechanisms for supervision, traceability, and judicial control in the Province of Córdoba.



Artículo publicado bajo Licencia Creative Commons Atribución-No Comercial-Sin Derivar.

© Universidad Católica de Córdoba

DOI: [https://doi.org/10.22529/rbia.2026\(8\)06](https://doi.org/10.22529/rbia.2026(8)06)

## INTRODUCCIÓN

En estos tiempos frenéticos, el avance de la tecnología y la proliferación de nuevos medios informáticos de comunicación e interacción digital entre individuos, trajeron aparejado el surgimiento de delincuentes sin rostro, ocultos detrás de un ordenador, que cometen novedosas maniobras delictivas entre las que podemos mencionar al “Grooming”, y/o los delitos relacionados con la tenencia, distribución y producción de imágenes de material con contenido de abuso sexual infantil.

Paralelamente, ha emergido el concepto de identidad digital como elemento distintivo de los usuarios en el ámbito virtual. Ante este novedoso panorama global, la justicia se enfrenta al desafío de

adaptarse y encontrar mecanismos efectivos para proteger a sus ciudadanos, al mismo tiempo que debe investigar estos delitos, esclarecer la verdad, impedir que sus efectos se propaguen y llevar a los perpetradores ante los tribunales. Una de las herramientas que se erige para combatir esta forma de delincuencia, es el uso de la inteligencia artificial para la creación de perfiles y usuarios que puedan ser utilizados por los denominados agentes encubiertos digitales y los operadores jurídicos que desarrollan este rol.

El presente trabajo, realizado de manera original por estudiantes de 3° año de Abogacía de la Universidad Católica de Córdoba en el marco del Seminario Optativo n° 2 (“Blockchain e Inteligencia Artificial”), tiene como objetivo principal, analizar el uso de la inteligencia artificial para la figura del agente encubierto digital dentro del proceso penal de la provincia de Córdoba, su reglamentación y la importancia de esta herramienta para la investigación de delitos informáticos.

Finalmente, se concluye con una propuesta de codificación de esta figura en conjunto con la herramienta de inteligencia artificial y se esbozan posibles soluciones para abordar las situaciones conflictivas que pudieran surgir en el seno de una investigación penal en la que se autorice la intervención de un agente encubierto digital.

A partir de lo expuesto, vemos *a prima facie* que el proyecto se encuentra íntimamente vinculado con la Unidad 3 del programa de la materia que da a luz el presente trabajo: “Inteligencia Artificial”, particularmente con los puntos “Irrupción de la I.A. en el trabajo” y “Equilibrio entre legislación e innovación tecnológica”, en tanto aborda el impacto de la tecnología en la función de los operadores jurídicos y la necesidad de armonizar su utilización con los desafíos que plantea el siglo XXI.

### **I. Elección del Tema: Exposición de Motivos**

La elección de trabajar sobre la figura de los agentes encubiertos en relación con la Inteligencia Artificial nace de la convicción de que es indispensable brindarles herramientas que hagan su labor más eficiente, precisa y segura; y además, responde a la profunda relevancia que este tema tiene para el futuro de la investigación judicial. En un escenario en el que los delitos migran cada vez más a entornos digitales, como grupos de mensajería privada, redes sociales o foros clandestinos, los agentes encubiertos necesitan mecanismos que les permitan investigar de forma ágil y efectiva (INTERPOL, 2021).

Aplicar Inteligencia Artificial en este ámbito abre la posibilidad de que estos agentes puedan infiltrarse digitalmente, identificar patrones de comportamiento, detectar riesgos en tiempo real y recopilar información valiosa de manera automatizada (Europol, 2023). Esto no sólo acelera las investigaciones, sino que también reduce la exposición directa de los agentes en contextos de riesgo y mejora la calidad de la

evidencia recolectada.

Este proyecto nace inspirado en nuestra motivación de fortalecer la capacidad del Estado para prevenir y combatir delitos graves como el grooming, la explotación infantil, el tráfico de estupefacientes o el fraude digital y, al mismo tiempo, proteger a los sectores más vulnerables de la sociedad (Ministerio Público Fiscal de la Nación, 2022). De este modo, no sólo se optimiza la labor de los investigadores, sino que se contribuye a generar un entorno digital más seguro para todos.

Elegimos este tema porque creemos que es innovador, disruptivo y necesario: apunta a mejorar el trabajo de quienes están en la primera línea de la lucha contra el delito, dándoles herramientas tecnológicas de última generación para que puedan cumplir su tarea de manera más simple, rápida y efectiva.

## **II. Descripción del Trabajo y Fundamentación**

En el Código Procesal Penal de la Provincia de Córdoba, las figuras del agente encubierto/revelador no se encuentran reguladas (menos aún la del agente encubierto digital), por lo cual no existe un marco jurídico específico que regule su actividad, sino que deben ser contempladas dentro de las normas generales de derecho constitucional, penal y procesal penal o bien, bajo el amparo de la Ley 27.319 en materia nacional -la que sin embargo no hace alusión alguna a la figura del agente encubierto digital-.

Esta situación ha sido señalada por organismos especializados, que advierten que “la normativa argentina no contempla de forma expresa la figura del agente encubierto digital, lo que genera vacíos legales frente a la creciente sofisticación de la criminalidad informática” (Ministerio Público Fiscal de la Nación [MPF], 2021).

Ahora bien, es importante destacar que, por cuestiones relacionadas con el éxito de la investigación, como para la seguridad personal del agente encubierto/revelador y de su familia, el ocultamiento de su identidad resulta imprescindible para el desarrollo de su actividad dentro de una investigación judicial, y es así como se realiza cotidianamente en la pesquisa de los delitos que no han sido cometidos en plataformas digitales. Necesariamente el agente encubierto no utilizará su nombre verdadero, llegando incluso a modificar algunos leves detalles de su aspecto físico. En este sentido, “el ocultamiento de identidad constituye una herramienta excepcional pero necesaria para garantizar la eficacia de la investigación y la seguridad del agente” (Ferrajoli, 2018, p. 245).

Otra de las actividades que pueden desplegar los agentes encubiertos/reveladores digitales en la investigación de delitos y bandas criminales, es el acceso a ciertos grupos privados de Whatsapp, Telegram,

etc., con la anuencia de algún miembro de la organización, que le permite el ingreso a ese grupo privado, en el cual, el agente recolecta información/datos que posteriormente pueden ser incorporados como prueba en el proceso penal.

Para ingresar a estos grupos privados y recolectar pruebas, es importante que el agente encubierto digital no revele su verdadera identidad, para protegerse a sí mismo y sus allegados, y que a la vez, no suplante digitalmente la identidad de otra persona, y aquí, es dónde emerge la inteligencia artificial para crear perfiles digitales con robustez que les permitan acceder al interior de estas bandas criminales y sean capaces de interactuar de manera verosímil en entornos virtuales delictivos.

### **III. Planteo del Problema**

No existiendo un marco normativo que regule en el Código Procesal Penal de la Provincia de Córdoba la figura del agente encubierto digital y el uso de la inteligencia artificial para las investigaciones penales, y teniendo en cuenta que para ingresar a ciertos grupos de organizaciones criminales y/o contactarse con delincuentes digitales sea necesaria la creación de perfiles con el apoyo de la Inteligencia Artificial, se plantea entonces la cuestión acerca de ¿cuáles serían los límites legales y posibilidades operativas que podría tener el investigador digital en el Poder Judicial de la provincia de Córdoba para desarrollar su actividad sin contar un marco normativo que lo respalde? (MPF, 2021).

Un aspecto que merece especial atención en el abordaje, es la manera en que se recaban, conservan y presentan las pruebas digitales. En este contexto, surge como interrogante la posible aplicación de la tecnología blockchain en los procesos de obtención de evidencia: ¿puede esta herramienta garantizar la integridad, trazabilidad e inalterabilidad de las pruebas desde su origen hasta su presentación ante la justicia? En efecto, “el uso de blockchain en el ámbito judicial puede fortalecer la cadena de custodia digital, garantizando la autenticidad y trazabilidad de la evidencia, aunque su adopción requiere adaptación normativa y validación técnica” (Organización de las Naciones Unidas [ONU], 2021).

La descentralización y la estructura criptográfica de blockchain ofrecen un potencial innovador para reforzar la cadena de custodia digital, pero también plantean desafíos en cuanto a su validación jurídica y aceptación dentro del marco procesal penal. Este trabajo se propone explorar estas cuestiones, considerando tanto las oportunidades como las limitaciones que implica incorporar esta tecnología al ámbito probatorio en investigaciones vinculadas a delitos informáticos.

### **IV. Revisión de Antecedentes: “Estado del Arte”**

#### **IV. 1. Proyecto de Ley Nacional sobre el Agente Encubierto Digital**

En el año 2017, bajo el número 2714-D-2017, y luego reproducido en 2019, la diputada María Gabriela Burgos presentó un proyecto de ley tendiente a incorporar formalmente la figura del agente encubierto informático en la Ley N.º 27.319 de Delitos Complejos. El objetivo principal de la propuesta era adaptar el marco legal argentino a los desafíos emergentes de la criminalidad digital, estableciendo una herramienta eficaz de investigación penal (Burgos, 2017).

El proyecto proponía modificar el artículo 3º de la mencionada ley, agregando el siguiente párrafo:

“Será considerado agente encubierto informático todo aquel funcionario de las fuerzas de seguridad autorizado, altamente calificado, que presta su consentimiento y, ocultando su identidad, interactúe, se relacione o participe, a través de una identidad supuesta, en grupos de internet, redes sociales y plataformas de intercomunicación online, con el fin de identificar o detener a los autores, partícipes o encubridores; de impedir la consumación de un delito; o para reunir información y elementos de prueba necesarios para la investigación, con autorización judicial.” (Proyecto de Ley 2714-D-2017, art. 3, Argentina) Además, el proyecto procuraba anticipar y regular un aspecto clave: la creación y utilización de identidades digitales simuladas. Para ello, proponía agregar un nuevo párrafo al artículo 4º de la misma ley, el cual dispondría:

“El perfil de identidad supuesta será regulado por el Ministerio de Seguridad, quedando legítimamente habilitados para actuar en todo lo relacionado con la investigación concreta en la causa para la que fue creado.” (Proyecto de Ley 2714-D-2017, art. 4, Argentina)

En lo relativo a la eximición de responsabilidad penal, la iniciativa se limitaba a incorporar al agente encubierto informático dentro del artículo 9º de la Ley 27.319, sin desarrollar mayores precisiones sobre los alcances o límites de su actuación. La redacción propuesta quedaba de la siguiente forma:

“Artículo 9º — No será punible el agente encubierto, el agente encubierto informático o el agente revelador que, como consecuencia necesaria del desarrollo de la actuación encomendada, se hubiese visto compelido a incurrir en un delito, siempre que éste no implique poner en peligro cierto la vida o la integridad psíquica o física de una persona o la imposición de un grave sufrimiento físico o moral a otro.” (Proyecto de Ley 2714-D-2017, art. 9, Argentina)

Pese a la relevancia de esta propuesta en el contexto del avance del delito informático, el proyecto no

prosperó ni fue sancionado a nivel nacional, quedando como un antecedente relevante en el debate sobre la necesidad de adaptar el marco jurídico a los desafíos del cibercrimen (Burgos, 2017).

## IV.2. El Caso de la Provincia de Mendoza

A diferencia del estancamiento legislativo a nivel nacional, la Provincia de Mendoza avanzó decididamente en la incorporación del agente encubierto digital dentro de su ordenamiento procesal penal. Luego de un extenso debate legislativo local con sucesivos intercambios entre las Cámaras de Diputados y Senadores, se aprobó una reforma al Código Procesal Penal que incluye el nuevo artículo 29 bis, el cual entró en vigencia el 4 de marzo de 2024 (Ley N.º 9.556, 2023).

La normativa mendocina establece que:

“En los casos de investigación de delitos en que resulte necesaria la intervención del agente en entornos o plataformas digitales, el Fiscal podrá requerir fundadamente ante el Juez Penal Colegiado la actuación encubierta de un agente...” (Código Procesal Penal de Mendoza, art. 29 bis, incorporado por Ley N.º 9.556, 2023)

Esta autorización judicial sólo podrá otorgarse cuando concurran dos condiciones fundamentales:

1. Que la investigación esté seriamente dificultada sin este recurso, y
2. Que se trate de delitos cometidos a través de medios informáticos que impidan otras formas de investigación (Ley N.º 9.556, 2023, art. 29 bis).

Entre los aspectos más relevantes de esta legislación se destacan:

- La actuación encubierta no podrá superar los 180 días desde la notificación de la autorización judicial al fiscal.
- Los perfiles digitales no podrán representar personas reales bajo ningún concepto y serán creados por personal técnico idóneo del Ministerio Público Fiscal.
- El fiscal deberá resguardar, en condiciones de seguridad, toda la información vinculada al perfil digital (denominación, características, plataformas utilizadas, claves de acceso y actividades autorizadas).
- El agente encubierto digital podrá, con autorización específica, intercambiar archivos ilícitos en el marco de la investigación.
- Estará exento de responsabilidad penal por aquellas conductas que sean consecuencia necesaria de su

actuación, siempre que estas sean proporcionales al objetivo de la investigación y no constituyan provocación al delito (Ley N.º 9.556, 2023, art. 29 bis).

Mendoza, históricamente reconocida como referente en materia de reformas procesales penales, se convierte así en la primera provincia del país en regular expresamente la figura del agente encubierto digital, alineando su normativa con estándares internacionales como los establecidos en la Convención de Budapest sobre Ciberdelincuencia (Consejo de Europa, 2001).

### **IV.3. Situación de la Provincia de Córdoba**

A la fecha, la Provincia de Córdoba no cuenta con un marco normativo específico en su Código Procesal Penal que regule la figura del agente encubierto digital ni el uso de herramientas de inteligencia artificial (IA) en el marco de investigaciones penales (Código Procesal Penal de la Provincia de Córdoba, Ley N.º 8.123, 1991). Esta ausencia normativa se vuelve especialmente relevante frente a la creciente sofisticación de las organizaciones criminales que operan en entornos digitales (Organización de Estados Americanos [OEA], 2023).

En muchos casos, para lograr el acceso a comunidades cerradas, grupos delictivos virtuales o redes criminales en la dark web, resulta indispensable crear perfiles simulados, posiblemente generados con el apoyo de tecnologías de IA que permitan construir identidades verosímiles. Sin una regulación clara, estas prácticas quedan en un limbo jurídico que podría afectar tanto la validez probatoria de las actuaciones como la seguridad jurídica de los operadores que las llevan a cabo (INTERPOL, 2022).

Esta situación evidencia la urgente necesidad de actualizar el marco procesal penal cordobés, incorporando herramientas legales adecuadas para el abordaje de delitos informáticos, en línea con los avances ya implementados en otras jurisdicciones como Mendoza (Ley N.º 9.556, 2023), y en consonancia con las recomendaciones internacionales sobre ciberdelincuencia (Consejo de Europa, 2001; OEA, 2023).

## **V. Desarrollo del Proyecto: “Puesta en Escena”**

Habiendo ya analizado cuál es el punto de partida de la cuestión, en esta sección nos abocaremos a exponer en qué consistió nuestro proyecto, las dificultades con las que nos encontramos durante su desarrollo y las propuestas de mejora que finalmente elaboramos, con el propósito de aportar un trabajo de valor tanto para la comunidad científica como para el Ministerio Público Fiscal de la Provincia de Córdoba.

Como se adelantó anteriormente, nuestro equipo se propuso explorar la posible aplicación de

herramientas de inteligencia artificial (IA) al ámbito de la investigación penal, específicamente en relación con la figura del agente encubierto digital.

Desde el inicio, trabajamos bajo la orientación de un tutor especializado en cibercrimen y delitos digitales. Su intervención fue esencial debido a que nos ayudó a comprender las dinámicas y desafíos concretos que enfrentan las investigaciones penales vinculadas a delitos informáticos. A partir de las reuniones iniciales, identificamos rápidamente la problemática central que advertimos cuando nos referimos al “estado del arte”: en Córdoba, la figura del agente encubierto digital no se encuentra regulada, lo que imposibilita su utilización formal dentro de una causa judicial y condiciona el alcance de cualquier desarrollo práctico.

Ante este escenario, decidimos enfocar nuestro proyecto en el diseño y simulación de posibles aplicaciones de inteligencia artificial en el ámbito fiscal, particularmente orientadas a la generación de perfiles digitales verosímiles que podrían ser utilizados, en un futuro marco legal adecuado, por un agente encubierto digital.

Para cumplir con nuestro cometido, analizamos de qué manera estas herramientas podrían integrarse en las etapas iniciales de una investigación penal, respetando siempre los principios de legalidad, proporcionalidad y control judicial.

Si bien comprendimos que no resultaba posible aplicar el proyecto en una causa real por la ausencia de regulación específica, elaboramos modelos teóricos y pruebas de laboratorio que nos permitieron visualizar su potencial utilidad práctica y los desafíos que implicaría su implementación dentro de las fiscalías cordobesas.

Para ello, construimos un entorno de prueba controlado en el que simulamos escenarios típicos de interacción digital vinculados a conductas potencialmente delictivas —por ejemplo, ofrecimientos de bienes o servicios fraudulentos y conversaciones en grupos cerrados de mensajería—.

Junto al mentor, analizamos casos reales ya concluidos en una Fiscalía, con el fin de identificar patrones de lenguaje y comportamiento que suelen repetirse en las investigaciones de cibercrimen. A partir de esa observación, generamos un conjunto de datos sintéticos, compuesto por mensajes ficticios, nombres genéricos y metadatos simulados (como horarios de conexión o frecuencia de envío), que sirvió como base para el desarrollo de un modelo de lenguaje de pequeña escala.

El propósito central fue utilizar inteligencia artificial para la creación de perfiles digitales

encubiertos, capaces de imitar de manera coherente la conducta y el estilo comunicacional de un usuario real dentro de una comunidad virtual. A través de esta tecnología, el sistema podía generar biografías, publicaciones y respuestas automáticas que reproducían el tono, la estructura y el ritmo de interacción observados en las conversaciones analizadas. De esta forma, demostramos que la IA podría emplearse como una herramienta auxiliar para asistir al agente encubierto digital en la construcción de una identidad ficticia sólida, evitando errores humanos y reforzando la verosimilitud del personaje creado.

Finalmente, realizamos ensayos internos de validación, en los que distintos integrantes del equipo interactuaron con los perfiles generados para evaluar su grado de credibilidad. Las observaciones fueron registradas en una planilla comparativa, donde se valoraron indicadores como tiempo de respuesta, coherencia temática y capacidad de mantener una narrativa continua. De este modo, logramos establecer una matriz de criterios técnicos que permitiría, cuando exista un marco jurídico apropiado, orientar la creación y supervisión de perfiles digitales destinados a tareas encubiertas.

Es menester aclarar que todo el trabajo se desarrolló en un entorno cerrado, con información ficticia y sin ningún tipo de interacción con usuarios reales, asegurando así el cumplimiento de las pautas éticas y legales vigentes.

De manera complementaria, exploramos también el potencial de la tecnología blockchain como herramienta para reforzar la cadena de custodia digital y la trazabilidad de la evidencia en el curso de las investigaciones. En este sentido, evaluamos cómo su estructura descentralizada e inmutable podría aplicarse al registro de las actuaciones de un eventual agente encubierto digital.

Cada interacción simulada, archivo generado o registro relevante del entorno de prueba se vinculó a un identificador único (*hash*), que funcionaba como una huella digital capaz de garantizar su autenticidad. De este modo, ante una posible auditoría o requerimiento judicial, podría demostrarse que la información no fue alterada desde su obtención, asegurando la confiabilidad del material obtenido y reduciendo el margen de manipulación o pérdida de evidencia.

Asimismo, diseñamos un esquema de registro secuencial para documentar de manera inalterable el proceso de recolección y almacenamiento de evidencia, asegurando que todas las actuaciones —desde la creación del perfil digital hasta la obtención y preservación de datos— queden debidamente autenticadas. Para ello, cada fase quedaba registrada mediante códigos criptográficos verificables dentro de una red de prueba (*testnet*), lo que permitió reproducir el flujo de custodia de forma transparente y auditable.

Si bien estas pruebas se realizaron únicamente en entornos simulados y sin conexión con

investigaciones reales, nos permitieron comprender el potencial de esta tecnología para fortalecer la validez, transparencia y trazabilidad de las actuaciones encubiertas digitales dentro del Ministerio Público Fiscal, reduciendo el margen de error humano y las controversias sobre la integridad de la prueba digital.

## **VI. Los Desafíos ante la Ausencia de Regulación Normativa**

Como se expuso en las secciones precedentes, la Provincia de Córdoba carece de un marco jurídico específico que habilite la actuación del agente encubierto digital y el uso de herramientas de inteligencia artificial en el proceso penal. Esta omisión genera un vacío normativo que no sólo impide su aplicación práctica en las investigaciones, sino que también plantea serios riesgos procesales: la eventual nulidad de las actuaciones o de la prueba obtenida mediante técnicas no previstas por la legislación vigente.

El reconocimiento de esta limitación fue uno de los principales desafíos de nuestro trabajo. Si bien las simulaciones realizadas junto a nuestro tutor demostraron el potencial de la inteligencia artificial y la tecnología blockchain para asistir al Ministerio Público Fiscal en la investigación de delitos informáticos, la inexistencia de una base legal clara impide trasladar estas herramientas al ámbito real sin vulnerar principios esenciales como el de legalidad, control judicial y debido proceso. En consecuencia, cualquier intento de implementar actuaciones encubiertas digitales en causas reales —sin regulación expresa— podría derivar en la invalidez de la prueba o incluso en responsabilidad funcional para los operadores intervinientes.

Frente a esta situación, consideramos necesario proponer una respuesta institucional que permita canalizar de forma segura, transparente y jurídicamente válida el uso de estas nuevas tecnologías en el ámbito penal provincial. Con ese objetivo, nuestro equipo elaboró un Proyecto de Ley para la incorporación de la figura del agente encubierto digital y la regulación del uso de inteligencia artificial en el proceso penal de la Provincia de Córdoba, destinado a ser presentado ante el Ministerio Público Fiscal y, particularmente, ante uno de los Fiscales Adjuntos, como insumo para una eventual revisión o reforma legislativa.

La iniciativa busca dotar al Ministerio Público Fiscal de un marco normativo que contemple la figura del agente encubierto digital dentro de los límites del debido proceso, garantizando que toda actuación de esta naturaleza cuente con autorización judicial previa, trazabilidad técnica y control institucional.

Asimismo, el proyecto incorpora la creación de una Estructura de Control Técnico-Digital (CSTD) —dependiente de la Fiscalía General— encargada de auditar los sistemas de inteligencia artificial utilizados, mantener registros reservados de agentes habilitados y velar por la observancia de los principios de legalidad, proporcionalidad y minimización de daño.

De este modo, el trabajo no se limita a una propuesta teórica, sino que ofrece un aporte concreto al debate jurídico contemporáneo sobre la incorporación de tecnologías disruptivas al sistema de justicia penal, anticipando los dilemas éticos, técnicos y normativos que deberán abordarse en el futuro inmediato.

## **VI.1. Proyecto de Ley: Incorporación del Agente Encubierto Digital y Regulación del Uso de Inteligencia Artificial en el Proceso Penal de la Provincia de Córdoba**

*LA LEGISLATURA DE LA PROVINCIA DE CÓRDOBA SANCIONA CON FUERZA DE LEY:*

### ***Artículo 1° – Objeto***

*La presente ley tiene por objeto incorporar y regular la figura del agente encubierto digital dentro del proceso penal de la Provincia de Córdoba, así como establecer un marco normativo para la utilización de herramientas de inteligencia artificial (IA) en investigaciones criminales realizadas por el Ministerio Público Fiscal, asegurando el respeto de los principios de legalidad, necesidad, proporcionalidad, control judicial y trazabilidad.*

### ***Artículo 2° – Definición***

*Se considera agente encubierto digital al funcionario autorizado por el Ministerio Público Fiscal para intervenir, bajo identidad digital simulada, en entornos virtuales, plataformas de comunicación o redes sociales, con el fin de prevenir, investigar o reunir pruebas sobre delitos de especial complejidad o aquellos cometidos mediante el uso de tecnologías digitales.*

### ***Artículo 3° – Autorización judicial***

*El uso de esta técnica especial requerirá autorización previa y fundada del juez de control, conforme a lo dispuesto en los artículos 312, 329, 330 y 337 del Código Procesal Penal de la Provincia de Córdoba (Ley 8.123).*

*El requerimiento deberá indicar:*

- a) el delito investigado y su calificación jurídica;*
- b) los motivos que justifican la necesidad de la medida;*
- c) la identidad del agente designado;*
- d) el ámbito y duración máxima de la actuación;*

e) los límites expresos de la intervención.

*La resolución judicial fijará la duración inicial, que no podrá exceder tres (3) meses, prorrogable por igual término mediante fundamentación expresa.*

#### **Artículo 4° – Custodia y registro digital**

*Toda actuación del agente encubierto digital deberá registrarse de manera íntegra y verificable, preservando la cadena de custodia digital y garantizando la autenticidad y la integridad de los datos. La actuación se considerará un acto irreproducible en los términos del artículo 330 del CPP Córdoba.*

*Los registros digitales serán almacenados bajo control del Ministerio Público Fiscal, con acceso exclusivo del juez de control y las partes autorizadas.*

#### **Artículo 5° – Uso de inteligencia artificial**

*Podrá emplearse inteligencia artificial como herramienta auxiliar para la creación o mantenimiento de identidades digitales simuladas, siempre que se garantice:*

*a) que no se suplante la identidad de personas reales;*

*b) que el modelo de IA utilizado sea validado por la Estructura de Control Técnico-Digital (CSTD); c) que se registren la versión, parámetros y prompts utilizados, para asegurar trazabilidad y control judicial posterior.*

#### **Artículo 6° – Estructura de Control Técnico-Digital (CSTD)**

*Créase la Estructura de Control Técnico-Digital (CSTD), dependiente de la Fiscalía General del Ministerio Público Fiscal, con funciones de:*

*a) supervisar la designación, formación y actuación de los agentes encubiertos digitales; b)*

*mantener un registro reservado de los agentes habilitados;*

*c) auditar los sistemas de IA empleados;*

*d) garantizar el cumplimiento de los principios de legalidad, proporcionalidad y minimización de daño. La*

*CSTD estará integrada por especialistas en Derecho Penal, Criminología, Ciberseguridad e Inteligencia Artificial designados por la Fiscalía General.*

#### **Artículo 7° – Control externo y auditoría**

*Dispónese una auditoría externa anual a cargo de una entidad académica o técnica independiente, preferentemente una universidad pública con trayectoria en informática jurídica o ética digital. La misma*

*deberá emitir un informe público sobre el cumplimiento de las garantías legales y la eficacia del mecanismo.*

#### ***Artículo 8° – Formación obligatoria***

*Todo funcionario del Ministerio Público Fiscal que intervenga en investigaciones digitales deberá realizar cursos de capacitación específica en ética, derecho procesal y tecnología aplicada a la investigación penal,*

*conforme a los artículos 6 y 7 de la Ley Orgánica del Ministerio Público Fiscal de la Provincia de Córdoba (Ley 7.826).*

#### ***Artículo 9° – Garantías procesales***

*Las actuaciones del agente encubierto digital deberán respetar los derechos y garantías reconocidos en la Constitución Nacional, la Constitución de la Provincia de Córdoba, los tratados internacionales de derechos humanos y los principios generales del debido proceso.*

*Cualquier exceso o violación de estos principios implicará la nulidad de la prueba obtenida y la responsabilidad funcional del agente o funcionario interviniente.*

#### ***Artículo 10° – Reglamentación***

*El Ministerio Público Fiscal reglamentará la presente ley en un plazo no mayor a noventa (90) días desde su promulgación, mediante la aprobación del Protocolo para la Designación y Actuación de Agentes Encubiertos Digitales, el cual deberá ser publicado en el Boletín Oficial.*

#### ***Artículo 11° – Vigencia***

*La presente ley entrará en vigencia a los treinta (30) días de su publicación.*

#### ***Artículo 12° – Comuníquese al Poder Ejecutivo.***

## **VI.2. Fundamentos Complementarios**

### **VI.2.a. Autorización Judicial y Control Jurisdiccional**

La base procesal para la autorización judicial de las actuaciones encubiertas digitales se encuentra en

los artículos 312 (secreto de las actuaciones), 329 (facultades del fiscal de instrucción), 330 (actos irreproducibles) y 337 (duración de la investigación y prórrogas) del Código Procesal Penal de la Provincia de Córdoba (Ley N.º 8.123).

Estas disposiciones permiten articular un mecanismo garantista en el que el fiscal solicite la medida, el juez de control la autorice conforme a derecho y se establezcan límites temporales y materiales de acuerdo con el principio de proporcionalidad. De esta manera, se asegura el control judicial efectivo sobre toda actuación encubierta digital, preservando los derechos y garantías del proceso penal.

### **VI.2.b.Designación, Control Institucional y Custodia Probatoria**

La Ley Orgánica del Ministerio Público Fiscal (Ley N.º 7.826) faculta a la Fiscalía General a organizar y dirigir la Policía Judicial, lo que posibilita la creación de estructuras internas especializadas, como el Registro Confidencial de Agentes Encubiertos Digitales (RCAED) y la Estructura de Control Técnico-Digital (CSTD).

Estas entidades tendrían a su cargo la designación, supervisión y formación de los agentes encubiertos digitales, así como la auditoría de los sistemas de inteligencia artificial utilizados en el desarrollo de sus tareas. Paralelamente, toda actuación digital debería ser considerada un acto irreproducible (art. 330 CPP), resguardando su autenticidad mediante técnicas de preservación y validación pericial —tales como el uso de *hashes*, *timestamps* y firmas digitales— que garanticen la integridad de la evidencia y la trazabilidad de la cadena de custodia.

### **VI.2.c. Importancia Institucional y Social**

La incorporación de la figura del agente encubierto digital representa un avance significativo en la capacidad del Estado para enfrentar la criminalidad informática y los delitos cometidos en entornos virtuales, tales como el *grooming*, la trata de personas con fines digitales, la difusión de material de abuso sexual infantil y otras modalidades delictivas propias de la era tecnológica.

Desde una perspectiva garantista, el proyecto procura que el uso de herramientas tecnológicas en la investigación penal se desarrolle bajo controles judiciales efectivos, procedimientos transparentes, formación técnica especializada y auditorías externas independientes. De este modo, la innovación tecnológica se integra al proceso penal sin vulnerar derechos fundamentales ni principios constitucionales.

Asimismo, la iniciativa busca armonizar el desarrollo del Derecho con las transformaciones del siglo XXI, asegurando que el progreso digital se produzca dentro de los valores del Estado de Derecho. Su eventual implementación por parte del Ministerio Público Fiscal y elevación a la Legislatura Provincial permitiría posicionar a Córdoba como referente nacional en materia de Derecho Penal Digital, al conjugar eficacia investigativa con un respeto irrestricto por las garantías constitucionales y los derechos humanos.

## CONCLUSIÓN

El desarrollo del presente trabajo nos permitió comprender que la tecnología, lejos de ser un fenómeno ajeno al Derecho, constituye hoy un motor de cambio y un desafío central para su evolución. La irrupción de la inteligencia artificial y la expansión del mundo digital han transformado las formas de delinquir, pero también han abierto nuevas posibilidades para la investigación, la prevención y la protección de los derechos de las personas.

En ese contexto, la figura del agente encubierto digital se erige como una herramienta necesaria, pero aún pendiente de regulación en la Provincia de Córdoba. El vacío normativo actual no sólo limita la eficacia de las investigaciones y obstaculiza la utilización de estas herramientas en la práctica, sino que también deja a los operadores judiciales ante un terreno incierto, en el que el deber de investigar se enfrenta al riesgo de vulnerar garantías procesales. Además, pone en riesgo la protección de las personas más vulnerables y de los propios agentes, quienes se encuentran en la primera línea de combate contra el delito y requieren garantías claras para actuar con seguridad y eficiencia.

Nuestro proyecto busca ofrecer una respuesta a esa tensión: cómo compatibilizar la innovación tecnológica con los principios del Estado de Derecho. A través del diseño de modelos de inteligencia artificial capaces de generar identidades digitales verosímiles, y del empleo experimental de blockchain como mecanismo de trazabilidad y preservación probatoria, demostramos que es posible pensar un futuro en el que la tecnología se integre al proceso penal con transparencia, control y respeto por los principios procesales.

Ante los desafíos que plantea la ausencia de legislación específica en la materia, surge con fuerza nuestra propuesta: un Proyecto de Ley para regular la figura del Agente Encubierto Digital y el Uso de Inteligencia Artificial, que representa el paso decisivo de la teoría a la acción institucional. Esta iniciativa no

pretende reemplazar los mecanismos tradicionales de investigación, sino complementarlos, dotando a los operadores judiciales de herramientas adecuadas para enfrentar una criminalidad cada vez más sofisticada y transnacional.

Este proyecto es el candidato ideal para liderar una próxima reforma del Código Procesal Penal de Córdoba, precisamente porque la realidad fáctica ya superó a la ley. Incorporar la figura del Agente Digital Encubierto asistido por IA es un acto de legítima defensa social que alinea la legislación con la tecnología de investigación más avanzada.

La regulación no es solo un permiso, sino también una garantía: al establecer límites claros, la ley protege los derechos constitucionales mientras asegura que la evidencia digital pueda ser incorporada válidamente. Complementar la regulación de la IA con el uso de blockchain permite un procedimiento más eficiente, transparente y auditable, elevando la credibilidad del Poder Judicial de Córdoba en la investigación de ciberdelitos a los más altos estándares.

Creemos firmemente que este proyecto trasciende lo tecnológico: es nuestra forma de contribuir a una sociedad más segura y justa. Sabemos que detrás de cada investigación hay víctimas que esperan respuestas, familias que buscan justicia y profesionales que arriesgan su integridad. Por eso decidimos poner nuestra creatividad y esfuerzo en desarrollar una solución que facilite su labor y les permita actuar con mayor rapidez y precisión. Porque si el delito no descansa, la investigación tampoco puede hacerlo.

Y es allí, donde ve la luz este proyecto, que proporciona una hoja de ruta para cerrar la brecha entre el delito digital y la capacidad de respuesta legal, transformando el actual limbo jurídico en un marco de eficacia operativa y seguridad jurídica para toda la provincia, protegiendo a las víctimas, a los agentes y, en última instancia, fortaleciendo la justicia.

## BIBLIOGRAFÍA

Burgos, M. G. (2017, 24 de mayo). *Proyecto de ley 2714-D-2017: Delitos complejos – Ley 27.319 – Modificaciones, sobre incorporación de la figura de agente encubierto informático* [Proyecto de ley]. Honorable Cámara de Diputados de la Nación. Retrieved from <https://www2.hcdn.gob.ar/proyectos/proyectoTP.jsp?exp=2714-D-2017>

Consejo de Europa. (2001, 23 de noviembre). *Convenio sobre la Ciberdelincuencia (Convención de Budapest)* [Tratado internacional]. Consejo de Europa. <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>

Córdoba. (1991). *Código Procesal Penal de la Provincia de Córdoba (Ley N.º 8.123)* [Ley provincial]. Boletín Oficial de la Provincia de Córdoba. <https://boletinoficial.cba.gov.ar/>

Ferrajoli, L. (2018). *Derecho y razón: Teoría del garantismo penal* (10.ª ed.). Trotta.

INTERPOL. (2022). *Global Crime Trend Report 2022* [Informe]. INTERPOL. <https://www.interpol.int/en/Crimes/Cybercrime/Global-Crime-Trend-Report-2022>

Mendoza. (2023, 4 de marzo). *Ley N.º 9.556: Modifica el Código Procesal Penal e incorpora la figura del agente encubierto digital* [Ley provincial]. Boletín Oficial de la Provincia de Mendoza. <https://www.boletinoficial.mendoza.gov.ar/>

Ministerio Público Fiscal de la Nación. (2021). *Informe sobre desafíos de la investigación penal frente al ciberdelito* [Informe]. MPF Argentina. <https://www.mpf.gob.ar>

Organización de Estados Americanos. (2023). *Amenazas cibernéticas y tendencias del delito digital en América Latina y el Caribe* [Informe]. Secretaría de Seguridad Multidimensional, OEA. <https://www.oas.org>

Organización de las Naciones Unidas. (2021). *Blockchain for Governance and the Rule of Law* [Informe]. United Nations Office on Drugs and Crime. <https://www.unodc.org>

Proyecto de Ley 2714-D-2017. (2017). *Incorporación del Agente Encubierto Informático en la Ley N.º 27.319 de Delitos Complejos*. Honorable Cámara de Diputados de la Nación.