

**TRABAJO FINAL DE GRADUACIÓN**

**UNIVERSIDAD SIGLO 21**



**ESPECIALIZACIÓN EN CIBERCRIMEN**

**MATERIA SELECCIONADA: “G” CUESTIONES PROCESALES EN CIBERCRIMEN**

**TEMA: 04 - LA FIGURA DEL AGENTE ENCUBIERTO Y EL AGENTE  
REVELADOR**

**TÍTULO: LA FIGURA DEL AGENTE ENCUBIERTO DIGITAL EN EL  
PROCESO PENAL DE CÓRDOBA**

**Alumno: BUSTOS, Julio Mariano**

**DNI: 34.069.685**

**Córdoba, Argentina**

**29 abril de 2024**

## Resumen

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 novedosas maniobras delictivas perpetradas por sujetos sin rostro, ocultos detrás de un ordenador. 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 agente encubierto digital. El presente trabajo tiene como objetivo principal analizar en profundidad la figura del agente encubierto digital en el marco del proceso penal de la provincia de Córdoba, y su relación con el delito conocido como “suplantación de identidad digital”. Finalmente, se concluye con una propuesta de codificación de esta figura 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.

**Palabras clave:** delitos informáticos, suplantación de identidad digital, privacidad, penal, proceso penal, seguridad informática, identidad digital, agente encubierto digital, agente revelador, ciberpatrullaje

### **Abstract**

In these fast-paced times, the advancement of technology and the proliferation of new computer-based communication and digital interaction media among individuals have brought about the emergence of novel criminal maneuvers perpetrated by faceless individuals hidden behind a computer screen. Alongside this, the concept of digital identity has emerged as a distinctive element of users in the virtual realm. Faced with this new global landscape, justice is faced with the challenge of adapting and finding effective mechanisms to protect its citizens, while at the same time investigating these crimes, clarifying the truth, preventing their effects from spreading, and bringing the perpetrators to justice. One of the tools that is emerging to combat this form of crime is the undercover digital agent. The main objective of this paper is to analyze in depth the figure of the undercover digital agent within the framework of the criminal process in the province of Córdoba, and its relationship with the crime known as "digital identity impersonation". Finally, it concludes with a proposal for the codification of this figure and outlines possible solutions to address the conflict situations that may arise within the framework of a criminal investigation in which the intervention of an undercover digital agent is authorized.

**Key words:** Computer crimes, Digital identity impersonation, Privacy, Criminal, Criminal procedure, Information security, Digital identity, Undercover digital agent, Undercover agent, Cyberpatrol

**I. Índice**

I. Índice.....4

II. Introducción.....6

    2.1 Presentación del Tema.....6

    2.2 Planteo del Problema.....9

    2.3 Objetivo General y Específicos .....9

    2.4 Justificación del Problema.....10

    2.5 Importancia y Viabilidad de la Investigación .....12

III. Marco Teórico.....13

    3.1 Discusión Jurídica en torno al agente encubierto digital .....13

    3.2 Delimitación y descripción del delito de suplantación de identidad digital .....16

    3.3 Comparación del agente encubierto digital con el Ciberpatrullaje.....19

    3.4 Comparación del agente encubierto digital con el agente provocador. ....20

    3.5 Análisis del proceso penal en Córdoba y su regulación del agente encubierto digital.....22

IV. Marco Metodológico.....25

    4.1 Hipótesis.....25

    4.2 Principio de Irresponsabilidad Penal .....26

V. Marco Normativo.....30

    5.1 Convenios Internacionales.....30

5.2 Unión Europea.....	30
5.3 España.....	31
5.4 Brasil.....	33
5.5 Uruguay.....	34
5.6 Legislación Argentina.....	35
5.7 Proyecto de Ley nacional relacionado al Agente Encubierto Digital .....	37
5.8 El ejemplo de la Provincia de Mendoza.....	39
VI. Resultados / Diagnóstico.....	42
VII. Plan de Implementación .....	45
VIII. Conclusión .....	47
IX. Referencias.....	48
X. Bibliografía.....	50

## II. Introducción

### 2.1 Presentación del Tema

El agente encubierto es definido como el funcionario de las fuerzas de seguridad que oculta su identidad y se infiltra en organizaciones criminales para investigar delitos complejos, mientras que el agente revelador, es aquel que simula interés en la compra de bienes, personas, servicios, armas o estupefacientes para investigar estos mismos tipos de delitos. Una definición más precisa, nos brinda el eximio procesalista, José Cafferata Nores quien manifiesta que *“el agente encubierto es un funcionario público que, fingiendo no serlo (simulando ser delincuente) se infiltra en una organización delictiva con el propósito de proporcionar desde el seno de ésta, información que permita el enjuiciamiento de sus integrantes, y a través de ello, el desbaratamiento de esa asociación delictiva”*.<sup>1</sup>

En efecto, ahora cabe proponer una definición del agente encubierto digital/informático y para ellos utilizaremos la propiciada por el abogado especialista en derecho informático, Marcelo Temperini, quien nos dice que: *“Esta medida consiste en la utilización, a través de medios electrónicos, de una identidad supuesta para poder entrar en el ámbito de confianza del sujeto investigado, y desde la cual se busca obtener información de interés para una causa previamente determinada. La justificación de este tipo de medidas, en muchos casos, se relaciona con el nivel de resguardos técnicos que tiene el ciberdelincuente para ocultar su identidad y ubicación, por lo que esta figura puede volverse de importancia para conseguir información de utilidad referente a su identificación, o bien que permita acreditar la comisión de uno o más delitos por el sujeto investigado. Más allá de los aspectos técnicos sobre el*

---

<sup>1</sup> CAFFERATA NORES, José I. y otros. Año 2012. *Manuel de Derecho Procesal Penal*. Pág. 344. Ed. Ciencia, Derecho y Sociedad.

*ocultamiento de la identidad, el agente encargado de dicha tarea generalmente utiliza técnicas de “ingeniería social” para lograr engañar a la persona investigada y obtener así la información que se necesita para la investigación.”<sup>2</sup>*

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 -. 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.

Otra de las actividades que pueden desplegar los agentes encubiertos/reveladores en la investigación de delitos y bandas criminales, es el acceso a ciertos recintos privados, domicilios, con la anuencia de algún miembro de la organización, que le permite el ingreso a esa dependencia privada, en la cual, el agente recolecta información/datos que posteriormente pueden ser incorporados como prueba en el proceso penal.

Ingresando ahora en lo que compete a la materia de ciberdelincuencia, actualmente se encuentra en una candente discusión jurídica en nuestro país, del por qué aún no ha recibido

---

<sup>2</sup> TEMPERINI, Marcelo (2018, 219-254). Delitos informáticos y cibercrimen: Técnicas y tendencias de investigación penal y su afectación a los derechos constitucionales. *Dupuy y otros (2018) Cibercrimen II*. Ed. B. d F.

acogida en el Código Penal Argentino (como sí sucede en otras jurisdicciones foráneas), el delito de suplantación/ usurpación de identidad digital, esto es, la “*utilización del nombre y apellido (en el caso de las personas humanas), o el nombre comercial o de fantasía (para las personas jurídicas), y la imagen (personas humanas) o la imagen de marca (logotipo o isologotipo para las personas jurídicas) para crear un perfil en alguna red social o plataformas de Internet, con el objeto de simular que se trata verdaderamente de la persona nominada y cuya imagen se muestra. Se trata, en definitiva, de hacerse pasar por otro en determinadas plataformas de Internet.*”<sup>3</sup>

Asimismo, es muy utilizado para las investigaciones en entornos digitales, la aplicación de OSINT (Open Source INTelligence), traducido como Inteligencia de Fuentes Abiertas, “*...hace referencia al conjunto de técnicas y herramientas para recopilar información pública, analizar los datos y correlacionarlos convirtiéndolos en conocimiento útil (...) la cual es usada “...para conseguir la información disponible en cualquier fuente pública sobre una empresa, persona física o cualquier otra cosa sobre la que queremos hacer una investigación, y haciendo que todo el cúmulo de datos se convierta en inteligencia que nos sirva para ser más eficaces a la hora de obtener un resultado.*”<sup>4</sup> Ahora bien, esta técnica de investigación en fuentes abiertas, cómo pueden ser los perfiles públicos de Instagram/Facebook, no comprenden aquellos casos en los que el agente encubierto le envía una solicitud de amistad a un perfil privado en un red social para obtener información que no pueda ser vista por todos, cómo así tampoco cuando el agente judicial/policial, ingresa a un grupo privado de Whatsapp o de Telegram para acceder a las conversaciones que mantienen entre sí los miembros de una organización criminal, y que

---

<sup>3</sup> PILNIK, Franco. Año 2021. *Comentarios sobre la suplantación de identidad digital* -[www.saij.gob.ar/IdSAIJ: DACF210223](http://www.saij.gob.ar/IdSAIJ/DACF210223).

<sup>4</sup> FONTE, Pablo. Año 2021 - *OSINT, ¿Qué es? ¿Para qué sirve? ¿Qué es Osint? Una introducción a como generar inteligencia a partir de datos obtenidos en fuentes abiertas* - <https://derechodelared.com/osint/>

indefectiblemente, ya sea para enviar la solicitud de amistad o para ingresar a un grupo privado, deberá ingresar utilizando un nombre supuesto/ usurpado o una imagen que no se condice con la de su persona.

## **2. 2 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 teniendo en cuenta la posible receptación y acogida en el Código Penal Argentino de este nuevo delito denominado suplantación/ usurpación de identidad digital, y que el mismo se tipificaría como una figura penal independiente, se plantea entonces la cuestión acerca de ¿cuáles serían los límites legales y posibilidades operativas que podría tener el investigador digital en la provincia de Córdoba para desarrollar su actividad si finalmente se sanciona como delito autónomo la suplantación de identidad digital?

## **2.3 Objetivo General y Específicos**

### ***Objetivo General***

Dilucidar los límites legales y posibilidades de actuación que tiene un agente encubierto digital dentro del proceso penal de la Provincia de Córdoba.

### ***Objetivos Específicos***

1. Identificar normas supletorias en los códigos procesales locales y foráneos que se utilicen para los agentes encubiertos (no digitales) que actúan en el mundo real para infiltrarse en organizaciones criminales.
2. Buscar en el derecho comparado si existe alguna legislación que haya establecido el marco de actuación del agente encubierto digital en su ordenamiento procesal.

3. Analizar las posibles nulidades en las que podría incurrir, o en los posibles ilícitos que se le podrían adjudicar a un agente encubierto que utilice el nombre/foto de una persona del mundo real.
4. Identificar y enumerar los perjuicios que podría sufrir un agente encubierto digital que utilice su nombre verdadero para infiltrarse en organizaciones criminales.
5. Buscar normas del derecho que le permitan/autoricen/justifiquen al agente encubierto digital a cometer infracciones/delitos sin que los mismos sean punibles por la justicia.

## **2.4 Justificación del Problema**

Los delitos cometidos en entornos digitales han ido aumentando exponencialmente con el paso del tiempo, y probablemente sean el mayor flagelo para la sociedad en materia de delincuencia en la actualidad y en los próximos años. Asimismo, los espacios digitales constituyen un ámbito propenso para llevar a cabo actividades de toda índole vinculadas a la delincuencia organizada, como por ejemplo, el tráfico de estupefacientes, la distribución de material de abuso sexual infantil, amenazas y extorsiones, estafas informáticas, entre tantas otras, bajo el velo del anonimato de sus intervinientes, quienes muchas veces ingresan o forman parte de grandes organizaciones dedicadas a delinquir, a cuyos integrantes se los suele ser denominar como los “*delincuentes sin rostro*”, ya que operan detrás de la pantalla de cualquier dispositivo y la posibilidad que sean identificados es prácticamente nula, por ello, la importancia de prevenir estos delitos o de investigarlos si finalmente fueron cometidos.

Las nuevas tecnologías de la información y de la comunicación, han dado lugar al nacimiento de nuevos instrumentos de ataque a través de estos medios que nos invitan a buscar nuevas formas de combatirlos. Una de las figuras que surge en la actualidad, como una herramienta para la Justicia para contrarrestar los efectos de estos delitos, sortear los obstáculos que nos presentan y ayudar en la investigación penal, es la del agente encubierto digital.

Adentrándonos en la función específica de un agente encubierto digital, la misma consiste en la utilización, a través de medios electrónicos, de una identidad supuesta para poder entrar en el ámbito de confianza del sujeto investigado, y desde la cual se busca obtener información de interés para una causa previamente determinada (Temperini – Macedo, 2017).

En el derecho comparado, ya se ha instaurado en varios ordenamientos jurídicos, el ya mencionado delito de “*suplantación de identidad digital*”. En nuestro país, si bien aún no se encuentra legislado, el 15 de septiembre del año 2022, el diputado nacional Jorge Raúl Rizzoti, presentó un proyecto de ley, para incorporar el art 139 ter en el Código Penal Argentino, y así añadir esta figura delictiva, como delito autónomo, el cual, si hubiera sido aprobado, habría quedado redactado de la siguiente forma:

*“Art. 139 ter. - Será reprimido con prisión de seis 6 meses a 2 años el que suplante o se apodere de la identidad digital de una persona humana sin su consentimiento, a través del uso de su nombre, apellido, foto o imagen, o cualquier otra característica que en forma ostensible la identifique como tal, utilizando para tal fin las Tecnologías de la Información y la Comunicación, con la intención de causar un perjuicio a la persona cuya identidad se suplanta o a terceros.*

*La pena será de prisión de 1 a 4 años, siempre y cuando no configure un delito más severamente penado, en los siguientes casos:*

- a) Si se realizara con la intención de cometer un delito;*
- b) Si se ejecutara de forma sostenida en el tiempo o de modo tal que obligue a la víctima a alterar su proyecto de vida;*
- c) Si la identidad creada, apropiada o utilizada fuera de un menor de 18 años.<sup>5</sup>“*

---

<sup>5</sup> Honorable Cámara de Diputados de la Nación Argentina (2022).

<https://www4.hcdn.gob.ar/dependencias/dsecretaria/Periodo2022/PDF2022/TP2022/4868-D-2022.pdf>

Frente a la posible sanción de este nuevo tipo delictivo, como una figura penal independiente en el Código Penal Argentino, denominado suplantación/ usurpación de identidad digital, y teniendo en cuenta el incremento exponencial en la comisión de hechos delictivos en plataformas digitales y consecuentemente, con la necesidad de tener una justicia que avance en la búsqueda de pruebas en la web, aplicaciones y perfiles de redes sociales, muchas veces con la utilización de agentes encubiertos que utilizan perfiles con nombres supuestos -los cuales son de máxima utilidad para obtener estas pruebas y no frustrar la investigación ni perjudicar al funcionario que realice la búsqueda- y no existiendo todavía una regulación en específico, existe un riesgo latente que algunas pruebas obtenidas por estos agentes puedan ser consideradas nulas a futuro o lo que es peor, que su actividad sea tildada de antijurídica, además del bien jurídico que se vería afectado de la persona a la cual el agente encubierto le usurpe su identidad digital.

## **2.5 Importancia y Viabilidad de la Investigación**

El desarrollo de esta investigación reviste gran importancia, atento a que busca arropar jurídicamente la figura del agente encubierto digital, con el fin de que, los operadores jurídicos que se desenvuelven en este rol, en el proceso penal cordobés, lo hagan con absoluto respaldo, dentro de un marco legal que establezca con claridad, los permisos y límites que su actividad entraña.

Asimismo, los funcionarios judiciales y los abogados particulares que accedan a las evidencias recolectadas por estos agentes encubiertos, con el devenir del proceso penal, podrán analizar si las mismas fueron obtenidas de forma legal, o, por lo contrario, si éstas merecen ser tachadas de nulidad y excluidas por ello, de ser analizadas por el juez.

Además, estableciendo los límites que deban tener los agentes encubiertos digitales, estaremos protegiendo en cierta medida, a las personas cuyas identidades digitales puedan ser

vulneradas, como así también, dotaremos de una figura jurídica clave para la pesquisa en este tipo de investigaciones.

La viabilidad de esta investigación – empero del análisis del derecho comparado y la casuística que se va a ir recolectando y reseñando- se va a centrar en la utilización de normas supletorias del derecho penal de fondo, para brindar una solución jurídica a la ausencia de una regulación del agente encubierto digital en el Código Procesal Penal de la Provincia de Córdoba.

### **III. Marco Teórico**

#### **3.1 Discusión Jurídica en torno al agente encubierto digital**

La figura del agente encubierto, siempre fue discutida desde el punto de vista legal y jurídico, no solo en la Argentina, sino también a nivel mundial. Al igual que otras formas de investigación utilizadas en el sistema anglosajón, como por ejemplo el agente encubierto, resultan discutibles desde el punto de vista constitucional (Delbono, 2018, 109). Quizás debido a este fuerte rechazo, es que es una figura – el agente encubierto digital - que ha sido, como bien indica su propia terminología, un ente marcado por la opacidad, el ocultismo y con pocas referencias legales, doctrinales y jurisprudenciales. (Bueno de Mata, 2012)

Partiendo del supuesto que el agente encubierto informático implica una intervención de un agente de seguridad en los ámbitos privados de las personas, o incluso llegado el caso, implica también la utilización del nombre o de la fotografía de otra persona, resulta necesario entonces analizar si este concepto resulta compatible -o no- con nuestro marco legal.

Para el jurista español, Bueno de Mata (2012), el tema de la identidad falsa no debe resultar polémico, ya que entiende que para asegurar el éxito de la investigación, resulta imprescindible mantener en secreto su identidad, ello a fin de que no sea descubierto por los

integrantes de la organización delictiva en la cual se infiltra y garantice el éxito de la investigación. En estos casos la colisión con el derecho fundamental a la intimidad del investigado queda justificada con la autorización judicial y con la ponderación de los intereses en juego.

Siguiendo el pensamiento de este doctrinario *“La justificación del engaño usado por el agente encubierto radica en una cuestión de política criminal, que llega a justificar las consecuencias disvaliosas que su utilización implica. La solución viene dada por una ponderación de valores, en el que se acaba por dar preponderancia al valor “eficacia”, en el sentido que, si se quiere luchar eficazmente contra este delito tan oculto, la mejor manera y la opción idónea es infiltrar a la persona de esta manera para llegar a una situación más favorable para la sociedad. Estamos eligiendo así una solución que reporta más seguridad y bienestar al conjunto de la sociedad y que logra la justicia, objetivo capital en un Estado de Derecho (Bueno de Mata, 2012).*

Ahora bien, este beneficio para la sociedad, en nuestro ordenamiento nacional y provincial, debería estar legislado y no estar sujeto a la potestad del funcionario judicial de turno que decida discrecional, o lo que es peor, arbitrariamente por su cuenta cuál es el mejor beneficio para la sociedad, dado que es una facultad que debe estar estrictamente regulada y quedar en manos del poder legislativo.

Justamente, en la vereda opuesta a la legalidad de la actuación del agente encubierto, encontramos la posición de Zaffaroni (1998) quien sostiene que *“El legislador no puede eximir de pena a sus funcionarios, en razón de equiparar arbitrariamente bienes jurídicos de diferente valor, como sucede al valorar del mismo modo el éxito de una investigación criminal y la propiedad, la intimidad, la autoridad legítima del mismo estado o el riesgo previsible para la vida de una persona. Si se entiende que el legislador puede operar de esta manera, no quedaría derecho alguno tutelado ni garantizado, pues su garantía dependería del valor que quisiera asignarle cada estado, subordinándolo a la eficacia de sus agencias policiales, que operarían como valor supremo.”*

Pero a pesar de esta postura esgrimida por el Dr. Zaffaroni y la de otros juristas que ponen en tela de juicio la legalidad de estas actuaciones y la validez de las pruebas recabadas por estos medios, y a pesar también de tener en cuenta que en el proceso penal de Córdoba la figura no se encuentra reglamentada, ello no resulta óbice u obstáculo alguno, para su adecuada aplicación en nuestros procedimientos. En efecto, primeramente cabe mencionar que la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional del año 2000, receptó implícitamente esta figura a los fines de combatir este tipo de delitos, pues el artículo 20 de la norma consigna que “(...) *cada Estado Parte adoptará, dentro de sus posibilidades y en las condiciones prescritas por su derecho interno, las medidas que sean necesarias para permitir el adecuado recurso a la entrega vigilada y, cuando lo considere apropiado, la utilización de otras técnicas especiales de investigación, como la vigilancia electrónica o de otra índole y las operaciones encubiertas, por sus autoridades competentes en su territorio con objeto de combatir eficazmente la delincuencia organizada*”.

Gracias a este tipo de normas del derecho internacional y a otras del fuero local, que, si bien no especifican que el agente encubierto digital, tenga permitido suplantar la identidad de otra persona para conseguir sus fines en el marco de una investigación penal, no caben dudas que, en este momento, la figura del agente encubierto digital se alza como la más propensa para combatir el crimen en los entornos digitales. Para Delbono, (2018), por ejemplo, haciendo alusión a la *Deep web* afirmó que “no habría, en principio, otra alternativa de detectar delincuentes en *tor*”.

Es claro que, Internet constituye un nuevo espacio en el que se desarrolla la actividad delictiva más diversa, y la figura del agente encubierto se muestra como un medio eficaz para el descubrimiento y la persecución de quienes se aprovechan de la red para sus propósitos. (Rodríguez Caro, 2016).

Indagar elementos delictivos en una red tor (o en la *deep web*) no es una labor sencilla. Aunque el sitio en cuestión cuenta con innumerables contenidos que podrían ser potencialmente susceptibles de incurrir en delito, su verificación no resulta fácil, especialmente cuando se debe identificar al individuo detrás del teclado. Llevar a cabo una labor de inteligencia en esta red requiere indefectiblemente de la intervención del agente encubierto, una figura que como hemos visto, no siempre ha sido bien recibida en el ámbito judicial.

Aun así, coincidiendo con la gran mayoría de los juristas, el agente encubierto digital resulta la mejor alternativa posible para investigar los delitos de esta nueva era digital. Ahora, solo resta enmarcar su actuación dentro de un marco legal que justifique sus actos, entre ellos, los de suplantar una identidad digital.

### **3.2 Delimitación y descripción del delito de suplantación de identidad digital**

Como primer punto en este tópico, brindaremos algunas definiciones que nos acerca el licenciado en sistemas y experto en la temática, Cristian Borghello, quien manifiesta que:

*“la identidad se puede definir como el carácter distintivo, aquel conjunto de atributos y características que permiten individualizar a la persona en sociedad, pertenecientes a un individuo determinado, o compartidas por todos los miembros de una determinada categoría o grupo social. (...) Por consiguiente, el concepto acuñado como identidad digital representa esas mismas características y actividades, pero llevadas a cabo en internet, como consecuencia del crecimiento de las comunicaciones digitales. (...) La identidad digital, entendida como el conjunto de rasgos y características particulares que una persona expresa a través de internet,*

*forma parte inescindible de la identidad personal de cada sujeto, en su faz dinámica, y más precisamente en su aspecto psicológico, social y moral.”*<sup>6</sup>

Teniendo en cuenta esta definición, se podría decir entonces que el delito de suplantación de identidad digital se llevaría a cabo con la utilización no autorizada de la identidad, ya sea por su nombre o fotografía, marca, de una persona física o jurídica en el ámbito de internet.

Ahora bien, hay que señalar que no toda conducta que uno realice en internet o en las redes sociales tendientes a ocultar un perfil y/o utilizar fotos que no se coincidan con nuestra imagen, o nombres supuestos que no nos pertenecen, concluyen necesariamente en una conducta reprochable jurídicamente.

Con esta postura coinciden los juristas, Temperini- Macedo cuando afirmaron que debían: *“... comenzar sosteniendo que, en principio, la mera creación y utilización de un perfil falso no contradice ninguna normativa vigente, sino que, por el contrario, podría ser considerado como una manifestación de la libertad de expresión y a modo general, representando una de las libertades más importantes que hacen (...) a Internet. Sin embargo, como siempre sucede desde el Derecho, existen límites a respetar a partir de los cuáles se podría estar incurriendo en un delito penal. Uno de estos casos es donde ese perfil falso, se haga usurpando la identidad de una persona real, configurándose así un caso de usurpación o suplantación de identidad.”*<sup>7</sup>

Se ha dicho previamente, que en la Argentina no está legislado aún el delito de suplantación de identidad digital, pero son varios los proyectos que se han ido presentando para

---

<sup>6</sup> BORGHELLO, Cristian y otro. Año 2012. Suplantación de Identidad Digital como delito informático en Argentina. Pág. 79-93. Simposio de Informática y Derecho. Jornadas Argentinas de Informática N° 41 - 2012. ISSN 1850-2814

<sup>7</sup> TEMPERINI, Marcelo – MACEDO, Maximiliano (2015). *La problemática de los perfiles falsos en Facebook y su relación con el Cibercrimen*. Simposio Argentino de Informática y Derecho.

su introducción en el Código Penal Argentino y que delimitarían el marco en el cual, esas conductas merezcan una sanción jurídica.

Primeramente, podemos mencionar la presentación en el año 2021 que realizó la senadora María Graciela Ocaña, quien buscaba incorporar como Artículo 139 ter al Código Penal Argentino, el siguiente delito:

*“Será reprimido con prisión de seis (6) meses a dos (2) años y multa de pesos cincuenta mil (\$50.000) a doscientos cincuenta mil (\$250.000) al que a través de internet, redes sociales, cualquier sistema informático o medio de comunicación, creare, transfiriere, suplantase, se apropiare o utilizare sin su consentimiento la identidad de una persona humana o jurídica que no le pertenezca, con la intención de cometer un delito o causar un perjuicio a la persona cuya identidad se suplanta o a terceros. Se aplicará prisión de uno (1) a tres (3) años y el doble de la pena de multa establecida en el párrafo anterior si concurriere alguna de las siguientes circunstancias: 1) La víctima fuera menor de dieciocho (18) años, mayor de setenta (70) años, o una persona con discapacidad; 2) El hecho fuere cometido por el/la cónyuge, ex cónyuge, o por la persona que esté o haya estado unida a la víctima por unión convivencial o similar relación de afectividad, aun sin convivencia; 3) El hecho fuere cometido por un familiar hasta el cuarto grado de consanguinidad o segundo grado de afinidad”*

El último proyecto presentado con relación a la suplantación de identidad digital fue el del diputado, Alberto Nassef quien buscaba incorporar este delito en el mismo número de artículo, pero con una diferente terminación jurídica. Así expresaba:

*“Será reprimido con prisión de un año a tres años el que adoptare, creare, apropiare suplantare, apoderare o utilizare, a través de internet, y/o cualquier sistema informático, y/o medio de comunicación y/o sistemas pertinentes para ello, la identidad digital de una persona humana o jurídica, sin su consentimiento, a través del uso de su nombre, apellido, foto y/o imagen, y/o cualquier otra característica que indefectiblemente la identifique como tal, con la*

*intención de cometer un delito y/o causar un perjuicio a la persona cuya identidad se suplanta o a terceros. La pena será de prisión de cuatro a seis años, siempre y cuando no configure un delito más severamente penado, en los siguientes casos: a) Si se realizare de forma continuada en el tiempo; b) Si obligare a la víctima a alterar su proyecto de vida; c) Si la identidad creada, apropiada o utilizada fuere de un menor de 18 años.”*

Como se ve, en un breve período de tiempo, fueron dos los proyectos presentados para sancionar con fuerza de ley este delito que afecta a tantas personas en estos tiempos modernos.

### **3.3 Comparación del agente encubierto digital con el Ciberpatrullaje**

En este momento, es preciso hacer una salvedad para entender mejor el marco en el cual se circunscribe la tarea del agente encubierto, aquellos casos en los cuales se va a requerir su participación, y en qué casos no sería pertinente.

Para ello primero hay que mencionar una tarea cotidiana que realizan las fuerzas y agentes de investigación en los procesos penales, que es la denominada actividad de Ciberpatrullaje.

En palabras del especialista en cibercrimen, Marcelo Temperni el ciberpatrullaje es la *“...medida de investigación consiste en el acceso, análisis y procesamiento masivo de información pública disponible en internet, buscando detectar comportamientos criminales en línea que, en caso de reunirse algunos indicios o elementos, podrían dar lugar al inicio de una investigación penal concreta. De todas las medidas listadas, esta es la única que no refiere a la investigación de un delito concreto, sino que es una actividad de prevención que suele ser cada vez más realizada por distintas fuerzas alrededor del mundo”*. (Temperini, 2018)

La diferencia entre el ciberpatrullaje y el agente encubierto digital (otras de las medidas listadas) es que en este último la fuerza de seguridad que oculta su identidad lo hace con un

objetivo concreto –la obtención de información útil para una investigación ya en curso–. En cambio, en el ciberpatrullaje resulta una etapa previa, donde ni siquiera es necesario ocultar la identidad del agente de seguridad, toda vez que estamos ante casos cuya exposición pública (sin límites de privacidad) permite un acceso irrestricto a la información por cualquier usuario. (Temperini, 2018)

Se diferencia también de la inteligencia sobre fuentes abiertas, en las que allí también suele utilizarse para casos ya en curso (si bien puede ser etapa preliminar) donde ya existió una noticia criminis sobre el hecho que se está intentando averiguar. (Temperini, 2018)

Se ve cómo estas actividades de búsqueda en la web, pueden ser realizadas por un agente judicial (no necesariamente encubierto) tienen como finalidad, inmiscuirse en foros o comunidades abiertas para ver qué ocurre o para ver si descubre algún delito. Para estas tareas, en principio, NO se requieren forzosamente de una autorización judicial previa, y pueden encuadrarse sin mayores dificultades en lo que en nuestro medio se identifica como tareas de investigación o inteligencia en fuentes abiertas.

### **3.4 Comparación del agente encubierto digital con el agente provocador.**

El análisis de estas dos figuras no es menor, atento a que su actividad tiene consecuencias disímiles en el proceso penal, ya que una cosa es recabar pruebas, información y otra totalmente distinta desde el punto de vista ético y legal, es la de participar o provocar en un tercero la comisión de un hecho ilícito.

Esa distinción entre lo permitido y lo prohibido surge claramente al comparar la figura del agente encubierto digital con la del "agente provocador", con el fin de comprender en qué circunstancias la actuación del funcionario de las fuerzas de seguridad se ajusta a derecho y en cuáles no.

En primer lugar, es importante señalar que la figura del agente provocador es aquella persona que -generalmente con fines probatorios- incita a otra a cometer un delito, sin que previamente existan circunstancias que indiquen su disposición a hacerlo.

El agente provocador actúa como un inductor del delito, que de otra manera no se habría cometido, aunque no busca la consumación de este y toma medidas de precaución para facilitar el procesamiento de los involucrados en el hecho delictivo. El agente provocador solo busca iniciar la actividad del provocado para que sea atrapado "con las manos en la masa". En relación con el agente provocador, es importante destacar que esta práctica es inviable en un Estado de Derecho, ya que resulta incoherente e inaceptable que el poder público, a través de sus fuerzas de seguridad, fomente y actúe de manera favorable a la comisión de un delito que no fue manifestado previamente, para luego reprimirlo penalmente.

Para el abogado Lucas Bello en su obra *“las diferencias que presenta la figura del agente encubierto informático con la del agente provocador son sutiles, aunque sustanciales para distinguirlas. En esa distinción radica la legitimidad de la mencionada en primer término y la ilegitimidad de aquella que se vincula al agente provocador. En el caso del agente encubierto informático, su accionar no se dirige a idear o fomentar la ejecución de conductas ilícitas, en la medida en que la organización o grupo criminal debe existir de modo previo a su designación. En efecto, la figura no pretende poner en marcha una actividad asociativa, sino que persigue inmiscuirse en una organización previamente establecida con el objeto de desbaratar sus planes y recolectar pruebas que permitan individualizar a sus responsables”*.<sup>8</sup>

---

<sup>8</sup> BELLO, Lucas (2022). *Agente Encubierto Informático. Aspectos operativos y constitucionales*. Ed. Temas de Derecho Penal y Procesal Penal

En esa línea, y diferenciándolo del agente provocador, el agente encubierto informático debe ser designado judicialmente en tal carácter antes de comenzar su labor. Esta designación anticipada, con control judicial constante durante su tarea y su intervención con el fin de recolectar información sobre sucesos ocurridos o en curso, evita equiparar la figura del agente encubierto informático con la del agente provocador.

En Argentina, tanto la Ley N° 23.319 como el nuevo Código Procesal Penal de la Nación, hacen una distinción entre las figuras del Agente Encubierto y del Agente Revelador. En este sentido, establecen que, en el primer caso, se trata de un miembro de las fuerzas de seguridad que, ocultando su identidad, se infiltra o introduce en las organizaciones criminales, con el objetivo de identificar a los responsables, evitar la comisión de un delito o recolectar información y pruebas (Art. 3 de la Ley N° 27.319 - 175 ter y quater CPPN). Por otro lado, en relación con el Agente Revelador, se define como aquel integrante de las fuerzas de seguridad designado para simular interés o llevar a cabo actividades como el transporte, compra o consumo de personas, servicios, armas, estupefacientes u otras acciones de un grupo delictivo, con el propósito de identificar a los involucrados en un delito, arrestarlos, confiscar bienes, liberar a las víctimas o recolectar pruebas que contribuyan a esclarecer los actos ilícitos (Art. 5 de la Ley N° 27.319 - 175 quinquies y sexies CPPN).

### **3.5 Análisis del proceso penal en Córdoba y su regulación del agente encubierto digital.**

Hasta la actualidad, el ordenamiento procesal cordobés, no recepta en ninguno de sus artículos la figura del agente encubierto, consecuentemente, resulta ineficaz hacer referencia a esa figura digital, lo que no significa que esta institución se encuentre prohibida, si tenemos en cuenta

el principio de libertad probatoria consagrado en el Art.217 del Código Procesal Penal de la Provincia de Córdoba.

En las fiscalías de Instrucción de Lucha Contra el Narcotráfico que existen en la provincia, utilizan como guía la ya mencionada Ley Nacional N° 27319 de *“Investigación, Prevención y Lucha de los delitos complejos”*. Por ello, las utilizaciones del agente encubierto en las investigaciones por narcotráfico en Córdoba se ven enmarcadas dependiendo de la regulación nacional y utilizan para sus investigaciones oficiales de la policía de la Provincia de Córdoba.

Es preciso recordar en este momento, el escándalo que supuso allá por el año 2013 en la provincia de Córdoba, las noticias y causas que surgieron en la Justicia Federal en torno a la utilización en la división de Drogas Peligrosas de la Policía de Córdoba, de un agente encubierto que no pertenecía a las fuerzas policiales. Se trataba de un particular que se hizo altamente conocido en aquel entonces, apodado *“El francés”* Viarnes <sup>9</sup>. La incorrecta utilización de este individuo derivó en numerosas investigaciones y procesos en la justicia federal, en la cual condenaron el accionar de la policía de la provincia de Córdoba manifestando que en abierta violación al art.31 bis de la Ley Nacional 23.737 introdujeron (a quien a posteriori resultaría imputado y detenido) Juan Francisco Viarnes en tareas policiales de inteligencia e investigación, como agente encubierto o agente provocador, particularmente respecto a hechos relacionados con el tráfico de estupefacientes, lo cual generó nulidades en el proceso penal, con grave perjuicio por haber actuado ilegalmente, y que eso supuso incluso, que fueran irregularmente detenidas personas por sus informaciones y tareas ilegales y que pese a estar involucradas en la peligrosa actividad del narcotráfico, a la postre terminarían liberadas y absueltas por estas irregularidades

---

<sup>9</sup> SIMO, Juan (9 de septiembre de 2013). *“El “Francés”: informante arrepentido ¿o agente encubierto digital?”*. <https://www.lavoz.com.ar/sucesos/el-frances-informante-arrepentido-o-agente-encubierto-ilegal/>

cometidas, al utilizar a una persona que no oficial de policía en la investigaciones, contrariando lo expresamente regulado en la normativa nacional.

A pesar de la reseña anterior, no todo es negativo en esta provincia. En el año 2018 la Legislatura Provincial sancionó la Ley N° 10.593 y con eso le dio creación y vida a la primera Fiscalía de Instrucción de Cibercrimen a nivel nacional, dedicada pura y exclusivamente a la investigación de los delitos relacionados con la alta tecnología informática. La misma comenzó a funcionar en el mes de agosto del año 2019, y su competencia (de excepción) rige materialmente para aquellos hechos que impliquen aprovechamiento de las vulnerabilidades de sistemas informáticos, atentados contra la integridad, confidencialidad o disponibilidad de datos o sistemas informáticos, así como todo otro evento que se sirva de la tecnología informática como medio o fin para la comisión de un delito, siempre y cuando aquella fuera determinante en la actividad delictiva, generando una especial complejidad técnica en la investigación.

Asimismo, en la Provincia de Córdoba se cuenta con la Dirección de Policía Judicial dependiente del Ministerio Público Fiscal que entre sus filas tiene a la División de Investigaciones Operativas (DIO), la cual coopera en la investigación penal preparatoria en los casos que le sean requeridos por los Fiscales, magistrados u otros funcionarios del Poder Judicial. En esta dirección, trabajan personas, en su gran mayoría abogados, a las cuales se les asigna el rol de “detectives” y en ella se investigan los hechos que, por su complejidad, dificultad investigativa, conmoción social y trascendencia pública, requieran el despliegue operativo mediante la aplicación de técnicas, métodos, procedimientos y conocimientos especializados. Dentro de esta dependencia pública, hay un grupo de detectives exclusivamente destinados a la investigación de los delitos cometidos en entornos digitales y son quienes muchas veces se los requieren para diversas pesquisas judiciales. Estos operadores judiciales, son lo que muchas veces son utilizados por la fiscalía de Cibercrimen para realizar las “*tareas de campo*” en las investigaciones judiciales

(entre ellas el ciberpatrullaje), siendo su labor complementada por otros equipos de Policía Judicial, las Áreas de Informática y Tecnología Forense.

## IV. Marco Metodológico

### 4. 1 Hipótesis

*Si bien la figura del agente encubierto digital no se encuentra regulada en el Código Procesal Penal de Córdoba, se puede justificar plenamente su aplicación recurriendo a otras normas supletorias del derecho.*

Para sostener y desarrollar esta hipótesis se va a hacer una intervención profesional para resolver el problema de este vacío legal jurídico que tiene el sistema procesal de Córdoba, realizando una investigación de tipo descriptiva/explicativa, a través de la bibliografía, jurisprudencia y doctrina recabada, tomando un enfoque cualitativo.

Esta intervención si bien estará limitada al proceso penal cordobés, se va a nutrir de las experiencias, leyes, y jurisprudencia de otras provincias y países para así poder obtener los resultados deseados.

Así de este modo, se va a buscar encontrar la solución para justificar el/los posible/s ilícitos que pueda cometer el agente encubierto digital al desarrollar su tarea investigativa, ya sea cuando utilice nombres/fotografías que les pertenezcan a otras personas del mundo real, o ingresando sin orden judicial previa a perfiles o grupos privados digitales.

Por ello, ante el interrogante de qué responsabilidad penal le cabe al agente encubierto cuando, infiltrado dentro de la organización delictiva, se ve compelido, a cometer un delito, algunos responden que, en principio, debe ser eximido de sanción penal, ya sea porque actuó en cumplimiento de un deber, o en ejercicio de una orden legítima de autoridad competente, o en el legítimo ejercicio de un cargo o por un estado de necesidad. (Arciniegas Martínez, 2007)

Compartiendo el pensamiento de este autor colombiano, entiendo que a nivel nacional y específicamente en la provincia de Córdoba que no se encuentra delimitada jurídicamente su labor, los posibles delitos que cometan los agentes encubiertos digitales en este momento, estarían amparados y no serían punibles, si se aplican para esos actos, las causas de justificación del artículo 34 del Código Penal Argentino, más específicamente las del inciso 4 esto es la que dice: *“El que obrare en cumplimiento de un deber o en el legítimo ejercicio de su derecho, autoridad o cargo.”*

En orden de justificar esta postura se buscarán citas de autores locales, jurisprudencia y doctrina que avala la hipótesis y solución planteada al problema existente, para que, con la aparición de la figura penal del delito de suplantación de identidad digital, los agentes encubiertos puedan trabajar e incorporar pruebas al proceso sin que las mismas sean tachadas de nulas o inconstitucionales.

#### **4.2 Principio de Irresponsabilidad Penal**

En primer punto hay que destacar que el Código Penal Argentino, prevé en su artículo N° 34 las denominadas “causas de justificación”, las que establecen que para ciertas conductas que a prima facie pudieran adjudicarse delitos penales, pero que, realizadas dentro de los enunciados allí esbozados, conducen a su NO punibilidad. De acuerdo con el Tribunal Superior de Justicia de la Provincia Córdoba, el legítimo ejercicio de un cargo en función del artículo 34 inc. 4 del Código Penal Argentino *“...implica el ejercicio del propio poder de decisión o ejecución correspondiente a un cargo público, y debe ser legítimo. La legitimidad supone la legalidad del título en cuya virtud el autor desempeña el cargo y la legalidad de su ejercicio en el caso concreto. Lo primero requiere que la autoridad no haya sido usurpada (C.P.246). El ejercicio es*

*legal si el autor obra en materia de su competencia y no lo hace con abuso de autoridad (CP 248 y 251), ni con exceso en la acción, sea en el modo o en la medida de su ejercicio”.*<sup>10</sup>

Durante el desarrollo de operaciones encubiertas informáticas, los funcionarios involucrados pueden verse obligados o incluso autorizados a cometer un delito. En este contexto de llevar a cabo una operación ilegal, o al desempeñarse como miembro de una organización criminal, la comisión de un delito a menudo se presenta como la manera de establecer vínculos de confianza con los demás integrantes, demostrar lealtad e incluso facilitar la realización de la operación encubierta por medios digitales. Quien asume ese rol en una organización criminal, cuyo objetivo principal es cometer delitos, orientará sus acciones hacia la comisión de tales ilícitos y la promoción de la actividad delictiva, ya que ese es el método mediante el cual puede infiltrarse y, en consecuencia, obtener información privilegiada de la organización.

En ese contexto, el funcionario judicial y doctrinario Lucas Bello manifiesta que: *“existe un principio de irresponsabilidad penal que recae sobre la actuación del agente encubierto informático. Expresamente, las normas que regulan su actuación establecen que no será punible el agente encubierto que, como consecuencia necesaria del desarrollo de la actuación encomendada, se hubiese visto compelido a incurrir en un delito, siempre que este 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.”* (Bello, 2022)

Sin embargo, en ausencia de una disposición específica en el código procesal penal de Córdoba que regule la figura del agente encubierto informático, su autorización, funciones y límites, la eventual comisión de un delito en el marco de su actividad podría encuadrarse en el Artículo 34 inciso 4 del Código Penal Argentino. En caso de que efectivamente, exista una

---

<sup>10</sup> Tribunal Superior de Justicia de Córdoba - Sala Penal, Sentencia n° 184, 06/08/2010, “AGUIRRE, Gustavo Celestino p.s.a abuso de arma agravado reiterado – Recurso de casación”

imputación formal en un proceso penal en curso, el mencionado Artículo 34 del Código Penal Argentino se aplicaría en consonancia con lo dispuesto en el Artículo 350 inciso tercero del Código Procesal Penal de Córdoba, lo que significa: “*Artículo 350.- Procedencia. El sobreseimiento procederá cuando: (...) 3) Sea evidente que medie una causa de justificación, inimputabilidad, inculpabilidad o una excusa absolutoria.*”

En relación a este punto, hay también una discusión jurídica. Algunos autores como Cafferata Nores y Tarditti que hablan del “*Injusto penal*”, conciben la tipicidad y la antijuricidad como dos caras de una misma moneda y entienden que estas causales enunciadas en el art. 34.4 del CP no son propiamente de justificación, como sí lo son las de la legítima defensa o la del estado de necesidad. Así entienden, que al operar una circunstancia que se desarrolla dentro del marco del ejercicio legítimo de un derecho u autoridad, o en el cumplimiento de un deber, se ratifica la falta de tipicidad de esa acción ante la falta de ilicitud penal, por lo que, en este caso en particular, siguiendo esas posturas doctrinarias, puede formularse el sobreseimiento también por la misma causal prevista en el artículo 350 inc. 2 del CPP.

Esta posibilidad la plantean los nombrados cuando expresan que: “*Quien piense que estos casos -v.gr. cumplimiento de un deber- no son casos de justificación, sino de antinormatividad, y, por tanto, de ausencia del tipo, encuadrará el sobreseimiento en el inc. 2º y no en el 3º*”.<sup>11</sup>

Todo esto debe tener un fundamento, de porqué el mismo no será punible y para ello nuevamente se debe considerar la postura del ya mencionando al jurista Lucas Bello cuando afirma que “*...el fundamento de ese principio de irresponsabilidad penal descansa en que el*

---

<sup>11</sup> Cafferata Nores – Tarditti, “*Código Procesal Penal de la Provincia de Córdoba Comentado*”, Tomo 2 Pág. 89. Ed. Mediterránea 2003

*agente no tiene la voluntad de favorecer la lesión de un bien jurídico a partir de la comisión de un delito, sino que su accionar es justamente a los fines de preservar el orden y la tutela de bienes jurídicos de suma importancia. Ese principio no es ilimitado. De hecho, el delito cometido siempre tiene que ser una consecuencia del desarrollo de la actividad encomendada por la autoridad judicial y aquel no puede atentar contra la vida o la integridad física o psíquica de terceros; de lo contrario, en caso de que el delito no tenga que ver con la operación encubierta o aquel afecte bienes jurídicos individuales contra la vida y la integridad de otras personas, el hecho será punible” (Bello, 2022).*

Considerando esta posición, se está en condiciones de sostener que si bien no está legislado el agente encubierto digital, si a un funcionario público de la justicia o de la policía de Córdoba se le encomienda una tarea como agente encubierto digital dentro del marco de una investigación penal preparatoria, y el mismo utiliza una identidad digital supuesta con imágenes que le pertenecen a un ciudadano real, al menos desde el punto de vista penal, y al no verse afectado el bien jurídico vida o integridad de este otro individuo, este accionar del operador se vería amparado por este principio de irresponsabilidad penal, quedando al margen el perjuicio civil que se le pudiere haber ocasionado a un tercero. No obstante ello, las consecuencias de utilizar las imágenes o nombres de un tercero podrían a posteriori incluso derivar en ataques de los delincuentes que han sido investigados, por ello, es que, si bien la suplantación de una identidad digital podría verse justificada en miras de salvaguardar bienes jurídicos de mayor importancia, se recomienda enfáticamente su no utilización y propiciar en todo caso, la utilización de identidades ficticias o no reales como acertadamente dispone el Código Procesal de la Provincia de Mendoza.

## **V. Marco Normativo**

### **5.1 Convenios Internacionales**

La Convención Internacional contra la delincuencia organizada transnacional, celebrada en Palermo en diciembre del año 2000, hace expresa alusión a Técnicas especiales de investigación, en el primer apartado de su Art. 20. Entre ellas incluye a las operaciones encubiertas, por autoridades competentes, a los fines de combatir eficazmente la delincuencia organizada.

En el mismo sentido, la Convención de las Naciones Unidas contra la Corrupción, adoptada en Nueva York, el 31 de octubre de 2003, prevé diversas técnicas especiales de investigación, a fin de combatir eficazmente la corrupción, las que deberán ajustarse a los principios fundamentales del ordenamiento jurídico interno de cada Estado, tales como a la entrega vigilada; la vigilancia electrónica o de otra índole y las operaciones encubiertas, así como para permitir la admisibilidad de las pruebas derivadas de esas técnicas en sus tribunales (Art. 50 de la Convención).

El Convenio de Budapest no aborda directamente las técnicas específicas de investigación, como el uso de agentes encubiertos en el ciberespacio. Sin embargo, los Estados parte pueden emplear diversas técnicas de investigación, dentro del marco legal de cada país, para combatir la ciberdelincuencia, siempre respetando los derechos fundamentales y las normas internacionales de derechos humanos.

### **5.2 Unión Europea**

En la Unión Europea se encuentran referencias a las investigaciones encubiertas en el Convenio de asistencia judicial en materia penal de 29 de mayo del año 2000. El Convenio citado, viene a definir las investigaciones encubiertas como aquellas indagaciones de actividades

delictivas realizadas por agentes que trabajan de forma infiltrada, en definitiva, bajo una falsa identidad. Estas investigaciones deben llevarse a cabo con absoluto respeto a los códigos y leyes de los países miembros donde se lleven a cabo las investigaciones. Este Convenio, advierte que los agentes que lleven a cabo investigaciones encubiertas precisan adquirir la preparación y formación adecuada, de modo que puedan ser requeridos para infiltrarse en una asociación ilícita criminal, con unos objetivos claros que son: acceder a información, así como poder identificar y detener a los miembros de esa asociación criminal.

### **5.3 España**

España, por ejemplo ya avanzó en esta temática y en su nueva regulación de la Ley de Enjuiciamiento Criminal, en el artículo 282 bis, contempla la figura del agente encubierto informático para investigaciones que afecten a actividades propias de la delincuencia organizada, donde el juez de instrucción competente y el ministerio fiscal, podrán autorizar a funcionarios de la policía judicial, y teniendo en cuenta su necesidad a los fines de la investigación, a actuar bajo identidad supuesta y a adquirir y transportar los objetos, efectos e instrumentos del delito y diferir la incautación de los mismos.

La Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, fue una modificación para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. Esta modificación realiza implementa una adecuación de la normativa procesal a los avances tecnológicos, incorporando diligencias de investigación tecnológicas: captación de comunicaciones a distancia; registro de conversaciones orales a través de medios electrónicos; utilización de mecanismos técnicos de rastreo, ubicación y obtención de imágenes; inspección y examen de dispositivos de almacenamiento de datos voluminosos y los historiales de actividad en equipos informáticos.

La figura del agente encubierto informático, pese a tener un ámbito de actuación tecnológico, no se encuentra recogido en este Título VIII, sino en el art. 282 bis, en los apartados 6 y 7.

El Anteproyecto de la Ley de Enjuiciamiento Criminal fue aprobado en 2020 tiene novedades interesantes sobre la figura del agente encubierto informático.

El art. 288 bis 6 de la mencionada normativa, permite para el agente encubierto informático, actuar bajo una identidad falsa, para poder entrar en foros, conversaciones, en definitiva, comunicaciones que se lleven a cabo en las redes. Al mencionarse canales cerrados, hay que reducir el concepto y por tanto la necesidad de autorización judicial a ese tipo de canales, ya que la navegación en internet por foros y comunicaciones abiertas por parte de la Policía Judicial no implica injerencia en derecho fundamental alguno, no precisa autorización, ni identificación expresa.

La autorización judicial de agente encubierto informático, en el párrafo 6 del art. 282 bis permite tres actividades:

- a)** entrar en canales cerrados con una identidad falsa;
- b)** Distribuir o remitir de forma autónoma ficheros ilícitos por la naturaleza de su contenido;
- c)** analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos;
- d)** captación de imagen y audio, así como su grabación en comunicaciones dentro de esos canales cerrados.

#### 5.4 Brasil

En Brasil, no existe una ley específica que regule la figura del agente encubierto digital. Sin embargo, su uso se encuentra amparado por diversos preceptos legales y jurisprudenciales, principalmente en el ámbito del derecho procesal penal. El Código Penal Brasileiro (Ley 2.848/1940) no establece una definición explícita del agente encubierto, pero sí permite la utilización de "*métodos especiales de investigación*" que podrían incluir esta figura. La Ley 7.960/1984 (Ley de Intervención Telefónica): regula la interceptación de comunicaciones telefónicas y telemáticas, una herramienta comúnmente utilizada por agentes encubiertos digitales. El Código de Proceso Penal (Decreto-Lei 3.689/1941) establece las normas generales del proceso penal brasileño, incluyendo la posibilidad de utilizar "diligencias investigativas especiales" que podrían incluir el uso de agentes encubiertos. (Art. 240).

En materia de jurisprudencia el Supremo Tribunal Federal (STF), ha reconocido la validez del uso de agentes encubiertos digitales en diversas decisiones, siempre que se respeten los principios constitucionales y las garantías procesales y los Tribunales Superiores han seguido la línea jurisprudencial del STF y han establecido criterios específicos para la utilización de esta figura, como la necesidad de autorización judicial y la proporcionalidad de la medida.

Alguna de esta jurisprudencia que se puede mencionar del Supremo Tribunal Federal de Brasil:

1. Recurso Extraordinario (RE) 875.512-RS: En este caso, el STF autorizó el uso de un agente encubierto digital para investigar un esquema de tráfico de drogas que operaba a través de internet. El Tribunal fundamentó su decisión en los siguientes argumentos:

- La gravedad del delito que se investigaba (tráfico de drogas) justificaba la utilización de métodos de investigación especiales como el uso de agentes encubiertos digitales.
- La medida era proporcional a la gravedad del delito y al potencial beneficio probatorio que se podía obtener.

- Se respetaron los derechos y garantías del acusado, ya que la operación fue autorizada por un juez y se respetaron los principios de legalidad, proporcionalidad y necesidad.

2. Habeas Corpus (HC) 126.266-SP: En este caso, el STF rechazó un recurso de Habeas Corpus presentado por un acusado de fraude electrónico que había sido investigado por un agente encubierto digital. El Tribunal sostuvo que la utilización de esta figura era válida y que no había vulnerado los derechos del acusado.

3. Recurso Extraordinario (RE) 1.040.912-RJ: En este caso, el STF estableció algunos criterios específicos para la utilización de agentes encubiertos digitales, como la necesidad de autorización judicial previa, la proporcionalidad de la medida y el respeto a los derechos y garantías del acusado.

## **5.5 Uruguay**

En el Derecho Penal Uruguayo tampoco existe una ley específica que regule la figura del agente encubierto digital. Sin embargo, su uso se encuentra amparado por diversos preceptos legales y jurisprudenciales, principalmente en el ámbito del derecho procesal penal. El Código Penal Uruguayo (Decreto-Ley 14.267/1975): No establece una definición explícita del agente encubierto, pero sí permite la utilización de "métodos especiales de investigación" que podrían incluir esta figura. El Código Procesal Penal (Ley 19.293/2017): Establece las normas generales del proceso penal uruguayo, incluyendo la posibilidad de utilizar "diligencias investigativas especiales" que podrían incluir el uso de agentes encubiertos. La Ley 18.022/2008 (Ley de Delitos Informáticos) regula los delitos informáticos y establece la posibilidad de utilizar "técnicas especiales de investigación" para su investigación, entre las que podría incluirse el uso de agentes encubiertos digitales. (Art. 13)

En materia de jurisprudencia la Suprema Corte de Justicia (SCJ) ha reconocido la validez del uso de agentes encubiertos digitales en diversas decisiones, siempre que se respeten los principios constitucionales y las garantías procesales. Entre ellas, podemos mencionar el Auto de Corte N° 29.295/2018 en el que la SCJ autorizó el uso de un agente encubierto digital para investigar un esquema de pornografía infantil que operaba a través de internet. El Tribunal fundamentó su decisión en los siguientes argumentos:

- La gravedad del delito que se investigaba (pornografía infantil) justificaba la utilización de métodos de investigación especiales como el uso de agentes encubiertos digitales.
- La medida era proporcional a la gravedad del delito y al potencial beneficio probatorio que se podía obtener.
- Se respetaron los derechos y garantías del acusado, ya que la operación fue autorizada por un juez y se respetaron los principios de legalidad, proporcionalidad y necesidad.

## **5.6 Legislación Argentina**

En Argentina contamos con la Ley 27319 denominada “*Investigación, Prevención y Lucha de los delitos complejos. Herramientas. Facultades*”, la cual tiene por objeto brindar a las fuerzas policiales y de seguridad, al Ministerio Público Fiscal y al Poder Judicial las herramientas y facultades necesarias para ser aplicadas a la investigación, prevención y lucha de los delitos complejos, regulando las figuras del agente encubierto, el agente revelador, el informante, etc., no haciendo alusión alguna en esta normativa a la figura del agente encubierto digital.

En la ley se menciona expresamente que su aplicación deberá regirse por principios de necesidad, razonabilidad y proporcionalidad y está dirigida para la investigación de delitos de producción, tráfico, transporte, siembra, almacenamiento y comercialización de estupefacientes,

precursores químicos o materias primas para su producción o fabricación previstos en la ley 23.737 o la que en el futuro la reemplace, y la organización y financiación de dichos delitos; delitos previstos en la sección XII, título I del Código Aduanero, todos los casos en que sea aplicable el artículo 41 quinquies del Código Penal; delitos previstos en los artículos 125, 125 bis, 126, 127 y 128 del Código Penal; Delitos previstos en los artículos 142 bis, 142 ter y 170 del Código Penal; delitos previstos en los artículos 145 bis y ter del Código Penal; delitos cometidos por asociaciones ilícitas en los términos de los artículos 210 y 210 bis del Código Penal; y para los delitos previstos en el libro segundo, título XIII del Código Penal.

En esta ley se define al agente encubierto como todo aquel funcionario de las fuerzas de seguridad autorizado, altamente calificado, que presta su consentimiento y ocultando su identidad, se infiltra o introduce en las organizaciones criminales o asociaciones delictivas, 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.

Además, establece que su intervención debe ser ordenada por el juez, de oficio o a requerimiento del Ministerio Público Fiscal. El nombramiento y la adopción de las medidas necesarias para su salvaguardia serán responsabilidad del Ministerio de Seguridad de la Nación, bajo supervisión judicial. La información recopilada por el agente encubierto y el agente revelador será comunicada de inmediato al juez y al representante del Ministerio Público Fiscal involucrado, de la manera más adecuada para facilitar el desarrollo de su labor y evitar la revelación de su función e identidad.

Yendo al punto central que nos incumbe para el presente trabajo, esta ley nacional expresamente detalla en su **artículo 9** que: “...**no será punible** el agente encubierto 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” (lo remarcado me pertenece).*

Finalmente, establece en su **artículo 10** que: *“cuando el agente encubierto o el agente revelador hubiesen resultado imputados en un proceso, harán saber confidencialmente su carácter al juez interviniente, quien en forma reservada recabará la pertinente información a la autoridad que corresponda. Si el caso correspondiere a las previsiones del artículo anterior, el juez lo resolverá sin develar la verdadera identidad del imputado”*

A nivel nacional, esta es la única normativa con la que se cuenta en relación al agente encubierto, sin ninguna mención al agente encubierto digital, y si bien esta ley introduce la NO punibilidad de ciertos delitos que pueda cometer el agente encubierto, no detalla expresamente cuáles serían los que no están incluidos, no hay un numerus clausus de posibilidades, como así tampoco no se encuentra expresamente detallada la vía procesal para instrumentar un posible sobreseimiento de estos delitos que pueda cometer en su función el agente encubierto digital.

### **5.7 Proyecto de Ley nacional relacionado al Agente Encubierto Digital**

En el año 2017 con el número: 2714-D-2017, y reproducido en el año 2019 la diputada María Gabriela Burgos, presentó un proyecto de ley en el cual solicitaba Incorporar al artículo 3° de la Ley 27.319 de Delitos Complejos, 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, participe, a través una identidad supuesta en grupos de internet, redes sociales y plataformas de intercomunicación on line, 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”.*<sup>12</sup>

En consonancia, esta diputada también buscaba en cierta medida, regular el problema que podría suscitarse en el futuro con la identidad supuesta que pudiera usar el agente encubierto digital, el querer introducir al artículo 4º de la Ley 27.319 de Delitos Complejos, el siguiente párrafo, el cual hubiera quedado redactado de la siguiente manera: *“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”.*

Finalmente, este proyecto de ley, en cuanto a la no punibilidad de las conductas realizadas por el agente encubierto digital, simplemente se limitaba a introducir su figura en la ya mencionada Ley Nacional 27319, sin agregarle ninguna otra circunstancia relevante, dejando el artículo 9, redactado 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.”*

---

<sup>12</sup> Honorable Cámara de Diputados de la Nación Argentina. (24 de mayo de 2017). *Expediente 2714-D-2017* sumario: *Delitos Complejos. Ley 27319 Modificaciones, Sobre incorporación De La Figura De Agente Encubierto Informático.* Publicado En: Trámite Parlamentario N° 55. <https://www2.hcdn.gob.ar/proyectos/proyectoTP.jsp?exp=2714-D-2017>

## 5.8 El ejemplo de la Provincia de Mendoza

Hace exactamente dos meses, y luego de haber sido extensamente debatido por el poder legislativo mendocino, con idas y vueltas entre la cámara de diputados y senadores locales, se aprobó la ley que introduce la figura del agente encubierto digital en el proceso penal de Mendoza. Durante las sesiones parlamentarias, se recalcó la importancia de su incorporación al Código Procesal Penal de dicha provincia, para enmarcarse en el cumplimiento de la Convención de Budapest con el fin de proteger a la sociedad de los delitos informáticos.

Mendoza siempre pionera en reformas procesales y referente en el país por este motivo, introdujo al Código Procesal el artículo 29 bis, el cual comenzó a regir desde el 04 de marzo de 2024; y que reza lo siguiente:

*"Artículo 29 bis. - Agente encubierto digital. 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 bajo las premisas anteriores y las condiciones aquí previstas. La autorización de este medio de investigación excepcional se emitirá por decreto fundado, en el marco de la investigación de delitos previstos en los artículos 128, 131 del Código Penal, en delitos concretos de especial gravedad o de investigación compleja y siempre que existan motivos suficientes que acrediten:*

- a)** Que el éxito de la investigación esté seriamente dificultado de no recurrirse a este medio.*
- b)** Que se trata de delitos cometidos a través de medios informáticos que no permiten otra forma de investigación.*

*La actuación encubierta no podrá exceder de ciento ochenta (180) días a contar desde que la autorización otorgada por el Juez Penal sea notificada al Fiscal. Los perfiles o identidades digitales, en ningún caso podrán ser imágenes de personas reales, serán creados y*

*administrados por personal técnico idóneo del Ministerio Público Fiscal, funcionarios o auxiliares de la fuerza de seguridad en función judicial con experiencia y desarrollo en la materia, y bajo el control directo del Fiscal a cargo de la investigación, quien hará constar las directivas, reservando en caja de seguridad: la denominación y características del perfil utilizado por el agente encubierto; plataformas digitales donde se actuará; claves de acceso validadas y actividad concreta a desarrollar por el agente. Una vez concluida la intervención del agente encubierto digital, el Fiscal dejará constancias de su existencia en el legajo/expediente.*

*El agente encubierto digital, con autorización específica para ello, podrá intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido. El agente encubierto digital estará exento de responsabilidad criminal por aquellas actuaciones que sean consecuencia necesaria del desarrollo de la investigación, siempre que guarden la debida proporcionalidad con la finalidad de ésta y no constituyan una provocación al delito.*

*A los efectos del presente artículo se considera agente encubierto digital al funcionario de las fuerzas de seguridad o miembro del Ministerio Público Fiscal autorizado, que previo prestar su consentimiento, oculte o utilice un perfil digital encubierto, interactúe y se relacione digitalmente a través de tecnologías de la información y de la comunicación con el objeto de: identificar o detener a los autores, partícipes o encubridores de un delito; impedir la consumación de un delito; o para reunir información o elementos de prueba necesarios para la investigación." .*

Podemos destacar, de la susodicha normativa, como principales datos distintivos para la presente investigación que:

- a)** El fiscal puede requerir fundadamente ante el Juez Penal Colegiado la actuación encubierta de un agente.
  
- b)** Únicamente deben ser delitos cometidos a través de medios informáticos que no permitan otra forma de investigación.
  
- c)** La actuación encubierta está limitada en el tiempo y la misma no podrá exceder los 180 días.
  
- d)** Las cuentas o identidades en línea que empleen los agentes no podrán representar a personas reales en ningún caso. Estas serán creadas y gestionadas por personal técnico especializado del Ministerio Público Fiscal.
  
- e)** El fiscal debe mantener en resguardo la identificación y las especificaciones del perfil empleado por el agente encubierto; las plataformas en línea donde se llevará a cabo la actuación; las contraseñas verificadas y la actividad específica a desarrollar.
  
- f)** Una vez finalizada la intervención del agente encubierto informático, el Fiscal dejará constancia de su existencia en el expediente judicial.
  
- g)** El agente encubierto informático, con autorización específica para ello, podrá intercambiar o transmitir por sí mismo archivos ilegales debido a su contenido.
  
- h)** El agente encubierto informático estará exento de responsabilidad criminal por aquellas actuaciones que sean consecuencia necesaria del desarrollo de la investigación.

## VI. Resultados / Diagnóstico

De lo investigado y mencionado en el presente trabajo, se observa que:

- No son muchas las legislaciones extranjeras como así tampoco en el ámbito local, que regulan específicamente la tarea del agente encubierto informático, siendo la provincia de Mendoza un referente a nivel nacional.
- Se advierte a simple vista el vacío legal existente en la provincia de Córdoba en materia procesal relacionada al agente encubierto digital.
- En lo que naturalmente coinciden muchos juristas y doctrinarios, es que esta figura jurídica del agente encubierto informático resulta una de las herramientas más invasivas de los derechos fundamentales de los individuos, ya que constituye una forma de ponerse en contacto con los delincuentes a través de medios digitales, con el riesgo que esto supone, sumado a ello, con las posibles afectaciones al derecho de defensa de los involucrados.
- Aun así, la figura del agente encubierto informático es constitucional, en la medida en que los derechos y garantías de los imputados encuentren su límite en la afectación de idénticas prerrogativas de terceros o del orden público.
- Los principales cuestionamientos sobre esta figura, y probablemente, los principales problemas o nulidades que pueden surgir en una investigación penal en la que se requiere la presencia de un agente encubierto digital es cuando se lo quiere equiparar con la figura del agente provocador y se lo utiliza de ese modo.
- A raíz de estos temores fundados, la discusión gira entorno a qué limitaciones, obligaciones, condiciones y prerrogativas se les puede asignar en un marco judicial a un agente encubierto informático, teniendo en cuenta esta posibilidad de afectación a

principios y garantías constitucionales, como la privacidad de las comunicaciones, la prohibición de autoincriminación o la afectación a la identidad digital de una persona real.

- Frente a estas circunstancias, los códigos que, si regulan la actividad del agente encubierto digital, buscan limitar su trabajo, y circunscribirlo para cuando sean estrictamente indispensables a los fines de conseguir el objetivo propuesto; lo que implica que la información y los datos que permitirían obtener estas herramientas de investigación, no se podrían obtener por otros medios menos invasivos.
- Para ello, las normas que regulen la actividad del agente encubierto digital que puedan ser introducidas a futuro, en un Código Procesal de la Provincia de Córdoba, deben tener en cuenta los principios de **razonabilidad, proporcionalidad y excepcionalidad**. La investigación penal preparatoria llevada a cabo por un Fiscal de Instrucción, cuando acuda a esta figura debe surgir a raíz de la necesidad particular y compleja que presenta un caso.
- Necesariamente el agente encubierto digital debe tener una designación previa en el expediente y un posterior control judicial permanente en el marco de su actuación.
- Su intervención debe ser a los fines de obtener información sobre hechos sucedidos o que se están llevando a cabo, y no de posibles hechos futuros, lo que impide así, que esta figura sea equiparada con la figura del agente provocador.
- Asimismo, y en pos de resguardar la integridad física y digital del agente encubierto **deberá necesariamente utilizar una identidad supuesta digital, absteniéndose de utilizar imágenes o nombres o usuarios digitales de otras personas reales, atento a que ellos también podrían verse perjudicados o atacados por los ciberdelincuentes que se están investigando**, sumado a la configuración del delito de suplantación de identidad digital que se cometería de no seguir esta directriz.
- El principio de irresponsabilidad penal que recae sobre la actuación del agente encubierto informático no es ilimitado y absoluto; de hecho, en caso de incurrir en la comisión de un

delito, aquel debe ser una consecuencia del desarrollo de la actividad encomendada por la autoridad judicial y no puede atentar contra la vida o la integridad física o psíquica de terceros, pues, en ese supuesto, el hecho sería reprochable penalmente.

- En los casos que exista una investigación en curso y una imputación formal en contra de un agente encubierto digital, la misma pueda ser solucionada con un pedido de sobreseimiento penal, en virtud del artículo 34 inc. 4 del Código Penal Argentino, esto es por el cumplimiento de un deber o cargo, dejando a salvo los posibles reclamos civiles que un damnificado que vio usurpada su identidad digital pueda hacerle al Estado.
- La legislación en la provincia de Córdoba no ha acompañado el desarrollo que ha tenido la delincuencia informática, poniendo en evidencia la falta de técnicas modernas de investigación. Para tener una justicia expeditiva y responder rápidamente a las exigencias de este mundo globalizado, la herramienta del agente encubierto digital se erige como necesaria.

## VII. Plan de Implementación

El plan de implementación para resolver esta problemática y atento al diagnóstico en el cual se encuentra la Provincia de Córdoba, de acuerdo con lo reseñado previamente sería el siguiente:

### 1) **Primero:**

Que en el corto plazo, el Ministerio Público Fiscal de la Provincia de Córdoba, a través de la facultad que le otorga al Fiscal General la Ley Orgánica -Ley Provincial N° 7826, imparta a través de instrucciones generales (disposiciones que se imparten a los inferiores jerárquicos en cuestiones relativas al servicio y al ejercicio de sus funciones que en principio, son de cumplimiento obligatorio para su destinatario) un compendio en el cual se encuentren expresamente detalladas las reglas para la utilización del agente encubierto digital, sus requisitos y permisos, y que estos sean dirigidos a las Fiscalías de Instrucción para su inmediata aplicación en la investigación de los delitos cometidos por medios telemáticos o de investigaciones en curso, en las cuales la prueba deba ser recabada en entornos digitales y se necesite de un agente encubierto digital para la consecución de tal fin.

### 2) **Segundo:**

Utilizar en las investigaciones penales preparatorias relacionadas con evidencias digitales a los agentes judiciales de la Dirección de Investigaciones Operativas del Ministerio Público Fiscal e indicarles para que se abstengan de utilizar imágenes en sus perfiles encubiertos que pertenezcan a identidades reales.

Para ello, sería óptimo crear previamente una base de datos con perfiles de usuarios diseñados por una **inteligencia artificial**, que sean lo suficientemente creíbles para interactuar con los delincuentes informáticos.

**3) Tercero:**

Que la Legislatura Provincial, imite en parte a su par de la provincia de Mendoza, y sancione con fuerza de ley, una modificación al Código Procesal Penal de la Provincia que introduzca la figura del agente encubierto y la del agente encubierto digital.

**4) Cuarto:**

Instruir a los empleados de las Fiscalías y de la Dirección de Investigaciones Operativas, para que se adapten a la Instrucción General de Fiscalía General, y ulteriormente a la ley que pueda sancionar la Legislatura Provincial.

**5) Quinto:**

Atento al modelo acusatorio que rige en la provincia de Córdoba, y ante el eventual mal uso de imágenes o suplantaciones de identidades digitales que puedan cometer los agentes encubiertos en la provincia de Córdoba, y que derivan en denuncias de los damnificados de estos hechos, que los Fiscales de Instrucción, requieran el sobreseimiento a los Jueces de Control en virtud del artículo 34 del Código Penal Argentino, inciso 4 “*El que obrare en cumplimiento de un deber o en el legítimo ejercicio de su derecho, autoridad o cargo*” instando de este modo a la no punibilidad de estas acciones en el marco de las investigaciones penales en curso.

## VIII. Conclusión

El estudio del agente encubierto digital en Argentina y su relación con el delito de suplantación de identidad digital revela la necesidad de actualizar la legislación para abordar estos fenómenos emergentes de manera efectiva y respetuosa de los derechos fundamentales. Es imperioso garantizar un marco legal claro y actualizado que permita a las autoridades combatir la criminalidad digital sin comprometer la privacidad y la seguridad de los ciudadanos.

La proliferación de delitos cometidos en entornos digitales y el surgimiento de la identidad digital como un derecho fundamental de los individuos, nos han llevado a pensar en nuevas formas de rediseñar nuestras vidas y las investigaciones penales.

El agente encubierto digital es una realidad dentro de este nuevo contexto, y su actividad puede llegar a comprometer un derecho fundamental, como la intimidad, el secreto de las comunicaciones, o cómo lo hemos ya mencionado, la identidad digital de una persona, por lo que será preciso siempre acudir al Juez de Control que valorará la actuación bajo los principios de necesidad y proporcionalidad.

Sin lugar a duda, uno de los mayores desafíos que se presentan en la actualidad para el sistema de Justicia Penal consiste en brindar una respuesta eficaz contra los delincuentes cibernéticos, y los delitos informáticos que estos cometen, los cuales se expanden de forma exponencial. En ese desafío, la implementación del agente encubierto informático es indispensable. Por ello, esta figura debe ser utilizada respetando siempre el equilibrio que debe existir entre el ejercicio estatal de la coerción penal y los derechos fundamentales de los individuos, por lo que, los esfuerzos deben dirigirse a establecer lineamientos generales que permitan conciliar ese conflicto de intereses y la mejor forma de llevar a cabo esto, es introduciendo la figura del agente encubierto informático en el Código Procesal Penal de la Provincia de Córdoba.

## IX. Referencias

- ARCINIEGAS MARTÍNEZ, Guillermo Augusto (2007). *Policía judicial y sistema acusatorio*. Ed. Nueva Jurídica, 3ª edición
- BELLO, Lucas (2022). *Agente Encubierto Informático. Aspectos operativos y constitucionales*. Ed. Temas de Derecho Penal y Procesal Penal
- BORGHELLO, Cristian y otro. Año 2012. *Suplantación de Identidad Digital como delito informático en Argentina*. Pág. 79-93. Simposio de Informática y Derecho. Jornadas Argentinas de Informática N° 41 - 2012. ISSN 1850-2814
- BUENO de MATA, Federico (2012). *El Agente encubierto en internet: mentiras virtuales para alcanzar la justicia*. Ed. A Coruña: Universidade
- CAFFERATA NORES, José I. (2012, 314). *Manuel de Derecho Procesal Penal*. Ed. Ciencia, Derecho y Sociedad.
- CAFFERATA NORES – TARDITTI, (2003) “Código Procesal Penal de la Provincia de Córdoba Comentado”, Tomo 2 Pág. 89. Ed. Mediterránea
- DEL BONO, Patricia (2018, 109). *Cibercrimen y Delitos Informáticos. Los Nuevos Tipos Penales en la era de Internet*. Revista Pensamiento Penal
- FONTE, Pablo (2021). *OSINT, ¿Qué es? ¿Para qué sirve? ¿Qué es Osint? Una introducción a cómo generar inteligencia a partir de datos obtenidos en fuentes abiertas*. Derecho en la Red
- Honorable Cámara de Diputados de la Nación Argentina (2022). <https://www4.hcdn.gob.ar/dependencias/dsecretaria/Periodo2022/PDF2022/TP2022/4868-D-2022.pdf>

- Honorable Cámara de Diputados de la Nación Argentina. (24 de mayo de 2017). *Expediente 2714-D-2017 sumario: Delitos Complejos. Ley 27319 Modificaciones, Sobre incorporación De La Figura De Agente Encubierto Informático*. Publicado En: Trámite Parlamentario N° 55. <https://www2.hcdn.gob.ar/proyectos/proyectoTP.jsp?exp=2714-D-2017>
- PILNIK, Franco (2021). *Comentarios sobre la suplantación de identidad digital*. SAIJ
- RODRIGUEZ CARO, María Victoria. (2015). *Agente encubierto. La infiltración policial: en el límite del Estado de Derecho. El inminente agente encubierto informático*. Revista Pensamiento Penal
- SIMO, Juan (9 de septiembre de 2013). “El “Francés”: informante arrepentido ¿o agente encubierto digital?”. <https://www.lavoz.com.ar/sucesos/el-frances-informante-arrepentido-o-agente-encubierto-ilegal/>
- TEMPERINI, Marcelo (2018, 219-254). Delitos informáticos y cibercrimen: Técnicas y tendencias de investigación penal y su afectación a los derechos constitucionales. *Dupuy y otros (2018) Cibercrimen II*. Ed. B. d F.
- TEMPERINI, Marcelo – MACEDO, Maximiliano (2015). *La problemática de los perfiles falsos en Facebook y su relación con el Cibercrimen*. Simposio Argentino de Informática y Derecho
- TEMPERINI, Marcelo – MACEDO, Maximiliano (2017, 481-514). *Nuevas herramientas de investigación penal: el agente encubierto digital. Dupuy (2017) Cibercrimen*. Ed. B. d F.
- Tribunal Superior de Justicia de Córdoba - Sala Penal, Sentencia n° 184, 06/08/2010, “AGUIRRE, Gustavo Celestino p.s.a abuso de arma agravado reiterado – Recurso de casación”
- ZAFFARONI, Eugenio R. (1998). *Impunidad del agente encubierto y del delator: una tendencia legislativa latinoamericana*. Editorial Leyer

## X. Bibliografía

- ABOSO, Gustavo E. (2021). *Delito de distribución de pornografía infantil en la era digital* - Ed. Hammurabi
- ABOSO, Gustavo E. (2022). *Ciberdelitos. Análisis doctrinario y jurisprudencial*. Ed. elDial.com
- ABOSO, Gustavo E. (2023). *Evidencia Digital en el proceso penal*. Ed. B. d F.
- BLANCO, Hernán. (2020). *Tecnología Informática e investigación digital*. Ed. La Ley
- CATALDI de ANUN, María (1998). *Agente encubierto, informante, ética y moral para combatir el narcotráfico. ¿Lucha desapareja?*. Revista de la Asociación de Magistrados y Funcionarios de la Justicia Nacional
- DIAZ, Rogelio (2020). *El agente encubierto en el marco de un sistema procesal garantista*. Revista de Derecho Procesal y Litigación de Córdoba.
- DUPUY, Daniela y otros. (2017). *Ciberdelitos. Aspectos de derecho penal y procesal penal. Cooperación internacional. Recolección de evidencia digital. Responsabilidad de los proveedores de servicios de Internet*. Ed. B. d F.
- DUPUY, Daniela y otros. (2021) *Acosos en la red a niños, niñas y adolescentes* - Ed. Hammurabi
- DUPUY, Daniela y otros. (2022). *Innovación en investigaciones digitales*. Ed. Hammurabi
- FERRER, Ezequiel (2021). *Estudios de Ciberdelitos*. Ed. Olejnik
- FERRER GUILLAMONDEGUI, Ramón Agustín (2021). *El agente encubierto y el agente revelador como nuevas técnicas especiales de investigación para delitos complejos*. Revista de Estudios Jurídicos y Sociales

- MAZZONE, Fabiana (2003). *El agente encubierto: un caso paradigmático de las nuevas concepciones jurídicas*. Ed. Zeus
- RAMIREZ JARAMILLO, Andrés David. (2010). *El Agente Encubierto Frente a los Derechos Fundamentales a la Intimidad y a la no Autoincriminación*. Universidad de Antioquia, Facultad de Derecho y Ciencias Políticas
- SUEIRO, Carlos Christian. (2023). *Ciberdelitos cometidos mediante códigos QR, Bluetooth e Inteligencia Artificial*. Ed. Hammurabi