TRABAJO FINAL DE GRADO

AGENTE ENCUBIERTO Y AGENTE REVELADOR EN ENTORNOS DIGITALES. INVESTIGACIÓN CRIMINAL VERSUS DERECHOS INDIVIDUALES

Autor: Gerardo E. Salemi

DNI N° 30.256.295

Universidad Empresarial Siglo XXI

Especialización en Cibercrimen

Año 2024

Índice

Resumen 3

Abstract 4

Introducción 5

Capítulo 1: Afectaciones a los Derechos Fundamentales por Agentes Encubiertos y Reveladores en Entornos Digitales 9

1.1 Diferenciación entre Agentes Encubiertos y Reveladores 9

1.2 Introducción a los Derechos Fundamentales en Entornos Digitales 10

1.2.1 La Protección de la Privacidad en el Ciberespacio 13

1.2.2 La Amenaza de la Vigilancia Masiva 14

1.2.3 Desafíos del Principio de Proporcionalidad en las Intervenciones Digitales 15

1.3 Agentes Encubiertos y Reveladores: Intervención e Implicaciones Legales 16

1.3.1 Implicaciones Éticas y Legales del Uso de Identidades Ficticias en Línea 18

1.3.2 Procesos de Control Judicial en el Uso de Agentes Encubiertos 19

1.4 Afectaciones Específicas a Derechos Fundamentales 20

1.4.1 Derecho a la Privacidad 20

1.4.2 Libertad de Expresión y Derecho a la No Autoincriminación 22

1.4.3 Derecho a la Presunción de Inocencia y Protección de Datos Personales 24

1.5 Estudios de Caso 26

Capítulo 2: Fundamentos Jurídicos y Límites de la Actuación de Agentes Encubiertos y Reveladores 29

2.1 Marco Legal de Actuación 29

2.1.1 Requisitos y Procedimientos para su Autorización 31

2.2 Derecho Comparado: España y Estados Unidos 32

2.2.1 Comparación con Otros Sistemas Legales: Canadá y Australia 33

2.3 Definición de los Límites de Actuación 35
2.4 Evaluación Crítica de la Legislación Argentina y Propuestas de Mejora..... 36
2.5 El Rol del Poder Judicial en la Supervisión de las Operaciones Encubiertas..... 37
2.5.1 Fortalecimiento del Control Judicial a través de la Capacitación y la Asistencia Técnica..... 38
Capítulo 3: Propuestas para Minimizar los Riesgos y Garantizar el Equilibrio entre Seguridad y Derechos Fundamentales..... 39
3.1 Proporcionalidad como Garantía de los Derechos Fundamentales..... 39
3.1.1 Estrategias para la Implementación Efectiva del Principio de Proporcionalidad 40
3.2 Ideas para Mejorar la Regulación y Supervisión 42
3.3 Propuestas para un Equilibrio entre Seguridad y Derechos Fundamentales 43
3.4 Mecanismos de Minimización de la Intrusión y Protección de Datos..... 45
3.5 Revisión y Actualización Continua de la Legislación y Procedimientos 46
3.6 Creación de Marcos Regulatorios Internacionales de Intervención 47
3.7 Integración de la Inteligencia Artificial en las Operaciones Encubiertas 47
Conclusiones..... 48
Referencias 50
Bibliografía..... 53

Resumen

El presente trabajo aborda el uso de agentes encubiertos y reveladores en entornos digitales, enfocándose en las potenciales afectaciones hacia los derechos fundamentales como la privacidad, la libertad de expresión, la presunción de inocencia y la protección de datos personales. A partir del análisis de la legislación argentina y del derecho comparado, se identifican desafíos y mejores prácticas para equilibrar la necesidad de la investigación criminal con la protección de los derechos individuales. La investigación destaca la importancia del principio de proporcionalidad en la autorización y control de estos agentes, resaltando la necesidad de lineamientos claros y sistemas de control judicial que aseguren que las intervenciones sean adecuadas, necesarias y no excesivas. También, se proponen medidas para mejorar la normativa actual, como la implementación de auditorías independientes, la creación de organismos de control y la intervención de expertos en derechos humanos en la revisión de las intervenciones. Además, se sugiere la adopción de protocolos específicos, con directivas precisas sobre la recolección y manejo de datos personales y establecer marcos regulatorios internacionales para asegurar que las intervenciones cumplan con los estándares internacionales de derechos humanos. En conclusión, el trabajo resalta que, aunque se trata de herramientas importantes en la persecución del cibercrimen, su utilización debe estar cuidadosamente reglada para evitar la vulneración de los derechos fundamentales.

Palabras clave: Cibercrimen, agentes encubiertos, agentes reveladores, derechos fundamentales, proporcionalidad, vigilancia digital, privacidad, regulación legal.

Abstract

This paper addresses the use of undercover agents and disclosers in digital environments, focusing on the potential effects on fundamental rights such as privacy, freedom of expression, presumption of innocence and protection of personal data. Based on the analysis of Argentine legislation and comparative law, challenges and best practices are identified to balance the need for criminal investigation with the protection of individual rights. The research highlights the importance of the principle of proportionality in the authorization and control of these agents, emphasizing the need for clear guidelines and judicial control mechanisms to ensure that interventions are adequate, necessary and not excessive. Measures are also proposed to improve the current regulations, such as the implementation of independent audits, the creation of control bodies and the intervention of human rights experts in the review of interventions. In addition, it suggests the adoption of specific protocols, with precise guidelines on the collection and handling of personal data and the establishment of international regulatory frameworks to ensure that interventions comply with international human rights standards. In conclusion, the paper emphasizes that, although these are important tools in the prosecution of cybercrime, their use must be carefully regulated to avoid the violation of human rights.

Keywords: Cybercrime, undercover agents, disclosing agents, fundamental rights, proportionality, digital surveillance, privacy, legal regulation.

Introducción

La hipótesis de partida de este trabajo afirma que es posible minimizar el riesgo de afectación a los derechos subjetivos por parte de los agentes en cuestión mediante la adopción de medidas que aseguren un equilibrio entre la necesidad de investigar delitos complejos y el respeto por los derechos individuales. A través de un análisis jurídico riguroso, se espera demostrar que es factible reducir los impactos negativos sobre los derechos fundamentales sin comprometer la eficacia de las investigaciones.

El constante desarrollo de las tecnologías de la información y la comunicación (TIC) transformó profundamente múltiples aspectos de la sociedad contemporánea, incluyendo el ámbito espacial en el que se cometen los delitos. En la actualidad, el cibercrimen se ha convertido en una de las principales amenazas para la seguridad y el bienestar de las personas y las instituciones.

Esta forma de delincuencia, facilitada por el uso de las tecnologías digitales, ha creado nuevos desafíos para los sistemas judiciales y las fuerzas policiales y de seguridad, que deben adaptarse permanentemente a la sofisticación y complejidad de las modalidades delictivas que ocurren en el ciberespacio. En este contexto, han surgido nuevas técnicas de investigación criminal, entre las que se destacan las figuras del agente encubierto y del agente revelador, cuya intervención en entornos digitales se torna cada vez más común y necesaria.

El agente encubierto, que tradicionalmente ha operado en el mundo físico, ha sido adaptado para actuar también en el ciberespacio, ámbito en el que su función consiste en infiltrarse en redes criminales utilizando identidades falsas, con el fin de obtener pruebas sobre delitos graves o bien, desarticular organizaciones criminales.

Por otro lado, el agente revelador desempeña un rol diferente, exponiendo a las autoridades tanto la maniobra criminal como sus autores, facilitando la acción directa de

aquellas. Ambos roles constituyen instrumentos esenciales en la lucha contra el cibercrimen, especialmente en casos en los que las técnicas convencionales de investigación no pueden penetrar los sofisticados recursos de anonimato, en muchas ocasiones valiéndose de comunicaciones encriptadas, de los que se valen las organizaciones criminales.

No obstante, el uso de estas figuras plantea una serie de dilemas éticos y legales, ya que su intervención eventualmente puede afectar los derechos inherentes a los ciudadanos que resultan objeto de la investigación o bien, a terceros como daño colateral. Derechos como la privacidad, la libertad de expresión, la protección de datos personales y a la no autoincriminación son principios fundamentales consagrados en las constituciones y en los tratados internacionales de derechos humanos.

En las investigaciones criminales, particularmente en aquellas desarrolladas en entornos digitales, el Estado enfrenta el desafío de equilibrar su derecho a investigar y sancionar delitos con la obligación de proteger los derechos individuales.

En la misma línea argumental, de acuerdo a Ramírez Jaramillo (2010) se produce una tensión entre dos intereses antagónicos en el que todo orden democrático debe "armonizar, por un lado, el interés público del Estado en conocer lo que realmente sucedió (…) y, por el otro, el interés del procesado en la salvaguarda de sus derechos fundamentales" (p. 95), una tarea que se torna especialmente delicada cuando se trata de actuaciones encubiertas en entornos digitales. La naturaleza misma del ciberespacio añade una capa de complejidad a este problema.

A diferencia del mundo físico, donde los límites entre lo público y lo privado se encuentran claramente definidos, en el entorno digital estas fronteras se desdibujan, adquieren una representación totalmente diferente de las que por definición conocemos.

La capacidad de las tecnologías digitales para recolectar y almacenar grandes

cantidades de datos personales representa un riesgo considerable de intromisión en la vida privada de las personas, incluso cuando estas no están involucradas directamente en actividades delictivas.

Un agente encubierto que bajo una identidad falsa se infiltra en una plataforma digital, como una red social o un foro, puede acceder a información personal sensible sin que el individuo sea consciente de la intervención. Esto genera un dilema en torno a la proporcionalidad de las medidas empleadas, ya que, si bien es fundamental obtener evidencias para desarticular redes criminales, también es necesario evitar violaciones innecesarias a los derechos humanos de las personas investigadas.

En la República Argentina, la Ley 27.319 de Investigación, Prevención y Lucha de los delitos complejos crea y regula diferentes técnicas especiales de investigación, entre las que se hallan las figuras de los agentes encubiertos y reveladores, para quienes establece una serie de controles y requisitos para su utilización.

Dicha norma se presenta como un marco normativo indispensable para asegurar que estas herramientas se utilicen de manera lícita y proporcional. Sin embargo, la velocidad con la que evoluciona el cibercrimen exige una revisión constante de la legislación, ya que las metodologías desplegadas por las organizaciones criminales mutan permanentemente.

En este sentido, es necesario realizar una comparación entre la legislación argentina con la de otras naciones que también enfrentan idénticos desafíos, como por ejemplo el Reino de España y los Estados Unidos de América, cuyos marcos regulatorios vienen evolucionado desde hace más tiempo.

El derecho comparado se convierte, por lo tanto, en una herramienta útil para identificar buenas prácticas y establecer posibles mejoras en el marco jurídico local.

El empleo de agentes encubiertos y reveladores no está exento de controversias, estas figuras han generado numerosos debates tanto en la esfera pública como académica.

Entre las críticas más comunes se encuentra el hecho de que la infiltración digital puede dar lugar a abusos por parte de las autoridades, afectando derechos como la presunción de inocencia o la integridad del proceso penal.

Quienes se oponen, argumentan que el simple acto de desplegar a un agente encubierto implica una forma de engaño que, en algunos casos, puede distorsionar la investigación al inducir al investigado a cometer delitos bajo la influencia cierta de la intervención estatal. Estos riesgos ponen de manifiesto la necesidad de que los jueces encargados de autorizar estas medidas actúen con un alto grado de vigilancia y seguimiento de las acciones, evaluando cuidadosamente la necesidad y la proporcionalidad de la intervención en el caso concreto.

También, se examinarán casos de estudio relevantes en el plano internacional en los que la utilización de estas figuras ha generado debates, para extraer aprendizajes y posibles mejoras en la regulación y el uso de estas herramientas. Finalmente, se explorarán propuestas concretas para minimizar el impacto sobre los derechos humanos sin comprometer la seguridad pública ni la efectividad de las investigaciones en la lucha contra el cibercrimen.

Al respecto, Alcolado Chico (2016) sostiene que “el carácter excepcional del empleo de medios extraordinarios de investigación penal, encuentra su camino en sus características, sobre todo, por la restricción de derechos fundamentales inherentes a las técnicas de las operaciones encubiertas” (p. 11).

En síntesis, este trabajo pretende contribuir al debate sobre cómo las tecnologías y las técnicas de investigación deben interactuar en una sociedad democrática, garantizando siempre el respeto a los derechos individuales. La importancia de este tema radica en la

necesidad de hallar un equilibrio entre el interés del Estado en perseguir y sancionar conductas delictivas que afectan a la comunidad en su conjunto, y la protección de los derechos individuales, esenciales para la preservación del Estado de Derecho y la justicia en cualquier sociedad moderna.

Capítulo 1: Afectaciones a los Derechos Fundamentales por Agentes Encubiertos y Reveladores en Entornos Digitales

1.1 Diferenciación entre Agentes Encubiertos y Reveladores

Los agentes encubiertos y reveladores constituyen herramientas valiosas en la lucha contra el cibercrimen y la delincuencia organizada. Su capacidad para infiltrarse en redes delictivas y recopilar información crítica se transforma en un recurso sumamente importante para las autoridades al momento de identificar y desmantelar organizaciones que, de otro modo, podrían operar con relativa o total impunidad. La actuación de estos efectivos adquiere especial relevancia en el contexto digital, ámbito en el que las redes criminales utilizan la tecnología como medio o como fin, para coordinar u organizar actividades ilegales, ocultar sus rastros y evadir la vigilancia de las fuerzas de seguridad.

El artículo 3 de la Ley 27.319 define qué entiende por agente encubierto:

Será considerado agente encubierto 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.

Mientras que el artículo 5 del mismo texto legal hace lo propio en relación al agente revelador:

Será considerado agente revelador todo aquel agente de las fuerzas de seguridad o policiales designado a fin de simular interés y/o ejecutar el transporte, compra o consumo, para sí o para terceros de dinero, bienes, personas, servicios, armas, estupefacientes o sustancias psicotrópicas, o participar de cualquier otra actividad de un grupo criminal, con la finalidad de identificar a las personas implicadas en un delito, detenerlas, incautar los bienes, liberar a las víctimas o de recolectar material probatorio que sirva para el esclarecimiento de los hechos ilícitos. En tal sentido, el accionar del agente revelador no es de ejecución continuada ni se perpetúa en el tiempo, por lo tanto, no está destinado a infiltrarse dentro de las organizaciones criminales como parte de ellas.

Como vemos, surge una clara distinción de roles, ya que el agente encubierto asume una identidad falsa para integrarse en la organización criminal y recolectar información que puede ser vital para la investigación penal. Esta técnica se basa en la construcción de una narrativa que permita al agente ganar la confianza de los investigados y obtener pruebas que no podrían ser conseguidas por otros medios convencionales. Por contraparte, el agente revelador tiene la tarea de exponer a los autores de los delitos mediante la recopilación activa de pruebas que permitan la intervención directa de las autoridades, es decir, su tarea es dejar al descubierto o exponer la maniobra criminal y a sus autores.

1.2 Introducción a los Derechos Fundamentales en Entornos Digitales

En las últimas décadas, la tecnología digital modificó radicalmente los modos en que las sociedades funcionan y se estructuran. El acceso a internet y la proliferación de dispositivos conectados a la red han creado un entorno globalizado caracterizado por el hecho de que barreras físicas y jurisdiccionales tradicionales han sido reemplazadas por

redes digitales que trascienden fronteras, dando lugar a la existencia de delitos transnacionales.

Según la Unión Internacional de Telecomunicaciones (UIT) (2022), más del 60% de la población mundial tiene acceso a internet, lo que representa un aumento exponencial y sostenido en la creación y circulación de datos tanto personales como sensibles. Este fenómeno no solo ha traído beneficios inmensos en términos de conectividad y acceso a la información, sino que también ha expuesto a los usuarios a nuevos riesgos, particularmente en lo que respecta a la protección de sus derechos fundamentales.

Estos últimos, son definidos por Casal (2020) como "derechos subjetivos garantizados constitucionalmente a toda persona o todo ciudadano en su condición de tal por ser considerados primordiales para el pleno desarrollo del individuo" (p. 22) e incluyen la privacidad, la libertad de expresión, el derecho a la no autoincriminación y la protección de los datos personales. Se encuentran consagrados por la Constitución Nacional y en tratados internacionales como la Convención Americana sobre Derechos Humanos y el Pacto Internacional de Derechos Civiles y Políticos y requieren que cualquier injerencia esté justificada por la ley, a la vez que sea proporcional al objetivo que se persigue.

El mismo autor sostiene que "son inalienables y deben ser protegidos de manera exhaustiva para asegurar la dignidad y el libre desarrollo de la persona" (p. 45).

Sin embargo, en el contexto digital, la protección de los mismos enfrenta desafíos únicos debido a la capacidad intrínseca de las tecnologías para recopilar, analizar y utilizar datos personales de formas que antes eran inimaginables y potenciados aún más por la aparición y desarrollo de la inteligencia artificial.

El derecho a la privacidad, por ejemplo, tradicionalmente se ha entendido como el derecho a estar libre de intrusiones indeseadas en la vida personal. Sin embargo, en el

ciberespacio, esta definición se ha extendido para incluir la protección contra la vigilancia y la recolección no autorizada de datos personales. Armenta Deu (2007) describe la privacidad como un "derecho fundamental que salvaguarda la integridad del individuo frente a la injerencia externa, tanto física como informativa" (p. 75). Esta idea se vuelve especialmente crítica cuando se considera el alcance y la profundidad de la recolección de información en línea, donde la información personal puede ser recopilada sin el conocimiento o consentimiento del usuario.

Gracias a las tecnologías de la información, tanto gobiernos como empresas pueden acceder a grandes volúmenes de datos con una facilidad y rapidez sin precedentes. Esto comprende no solo a aquellos de carácter explícito como correos electrónicos, mensajes de texto y registros de llamadas, sino también información más sutil como patrones de comportamiento, opiniones, intereses, tendencias, ubicaciones geográficas y relaciones sociales, etcétera. En muchos casos, los mismos son recabados por agencias del gobierno bajo el pretexto de la seguridad nacional o la prevención del delito, lo que plantea serias preocupaciones sobre la potencial violación de derechos.

El despliegue de agentes encubiertos y reveladores en entornos digitales añade una capa adicional de complejidad. Como vimos, su función principal es infiltrarse en redes delictivas o bien desenmascarar acciones criminales para recolectar pruebas e identificar a sus autores, con la capacidad de acceder a grandes volúmenes de datos representados por diversa información personal.

Alcolado Chico (2016) señala que "la utilización de agentes encubiertos en el ciberespacio puede generar conflictos serios entre la necesidad de proteger la sociedad y la obligación de respetar los derechos individuales" (p. 39).

La regulación de estas prácticas es, por lo tanto, esencial para asegurar que se mantenga un balance entre la seguridad pública y la protección de los derechos subjetivos.

1.2.1 La Protección de la Privacidad en el Ciberespacio

La privacidad ha sido históricamente uno de los pilares fundamentales de las sociedades democráticas y su protección en el entorno digital ha evolucionado de manera significativa debido al crecimiento de la tecnología y la globalización de las comunicaciones. En el ciberespacio, los derechos a la privacidad y a la protección de datos personales enfrentan desafíos sin precedentes.

La facilidad con la que se pueden recopilar, almacenar y analizar los mismos ha llevado al desarrollo de marcos regulatorios más detallados en todo el mundo. Legislaciones como el Reglamento General de Protección de Datos (en adelante GDPR, por sus siglas en inglés) en Europa establecen estándares rigurosos para la recolección y manejo de datos, exigiendo un consentimiento explícito y protegiendo los derechos de los usuarios.

En este contexto, la privacidad se convierte en un derecho especialmente vulnerable. La intervención de los agentes mediante los roles descriptos, puede implicar la recolección de información personal sin el conocimiento ni el consentimiento de los individuos afectados, lo que genera un conflicto directo con las normas de protección de datos. Por ejemplo, un agente que se infiltra en una red social bajo una identidad falsa e interactúa con un usuario o más, puede acceder bajo engaño a mensajes privados, listas de contactos y otros de índole sensible que en circunstancias normales estarían protegidos.

En la República Argentina, la implementación de protecciones efectivas para la privacidad digital sigue siendo un desafío. La Ley 27.319 regula algunas de las prácticas de recolección de datos, especialmente en el contexto de investigaciones penales, pero no

abarca completamente las complejidades del ciberespacio moderno, situación similar que ocurre con la Ley 25.326 de Protección de Datos Personales.

Según Alcolado Chico (2016), "la regulación de la privacidad en línea sigue siendo fragmentaria y en muchos casos inadecuada para enfrentar las realidades de la vigilancia digital y la recolección masiva de datos" (p. 42).

Esta situación plantea la necesidad de una legislación clara y mecanismos de control efectivos que garanticen que su recolección se limite estrictamente a lo necesario para la investigación y se minimice cualquier intrusión innecesaria.

Además, las nuevas tecnologías han permitido que las autoridades puedan realizar minería de datos a gran escala, analizando patrones de comportamiento y relaciones en redes sociales que pueden no estar directamente relacionadas con el objetivo de la investigación. Esta recolección indiscriminada no solo compromete la privacidad de los investigados, sino que también puede involucrar a terceros que no tienen relación con actividad delictiva alguna.

La falta de transparencia en estos procesos y la ausencia de controles pueden llevar a abusos de poder y a un desgaste o incluso pérdida de la confianza pública en las instituciones encargadas de hacer cumplir la ley.

1.2.2 La Amenaza de la Vigilancia Masiva

La vigilancia masiva se ha convertido en una herramienta común para los gobiernos y las agencias de inteligencia en su lucha contra el terrorismo y otros delitos graves. Sin embargo, la capacidad de recolectar y analizar datos de forma generalizada plantea serios riesgos para la privacidad y otros derechos fundamentales. Roxin (2000) menciona que "la vigilancia sin control judicial y sin límites claros puede conducir a una sociedad de

vigilancia donde los derechos individuales son constantemente sacrificados en nombre de la seguridad" (p. 88).

La vigilancia masiva en el ciberespacio no solo afecta a los sospechosos de participar en actividades delictivas, sino también a millones de ciudadanos comunes cuyos datos pueden ser capturados, almacenados y analizados sin una justificación coherente. Esto incluye la recolección de registros de navegación, ubicaciones GPS, y hasta interacciones en redes sociales. En algunos casos, lo recabado puede ser utilizado para crear perfiles detallados de los individuos, que luego pueden ser explotados para diversos fines, desde la vigilancia política hasta el marketing dirigido.

Bravo Sandoval (2021) advierte que "la falta de restricciones claras en la recolección de datos y la insuficiencia de supervisión judicial puede llevar a abusos significativos de los derechos fundamentales" (p. 134). En un entorno digital donde la información personal está constantemente en juego y es considerada el oro del siglo XXI, es fundamental que las leyes y las políticas públicas sean lo suficientemente firmes como para proteger los derechos de privacidad de los ciudadanos contra la vigilancia no autorizada o excesiva.

1.2.3 Desafíos del Principio de Proporcionalidad en las Intervenciones Digitales

El principio de proporcionalidad es fundamental para asegurar que las medidas adoptadas en la investigación penal no vulneren los derechos individuales más allá de lo necesario. Este principio exige que cualquier restricción de derechos sea adecuada, necesaria y proporcional al fin que se persigue. Sin embargo, su aplicación en el contexto digital presenta desafíos únicos debido a la naturaleza expansiva de la recolección de información.

En el caso de los agentes encubiertos y reveladores, la proporcionalidad no solo debe evaluarse en términos de la gravedad del delito que se investiga, sino también en relación con la cantidad y tipo de datos recabados. Según Armenta Deu (2007), "la proporcionalidad en el contexto de la recolección de datos digitales debe incluir consideraciones específicas sobre la extensión y profundidad de la intervención, así como los impactos potenciales en la privacidad de terceros" (p. 75), quienes no están exentos de ser alcanzados por la actividad investigativa policial. Esto requiere un nivel de escrutinio judicial que vaya más allá de las prácticas tradicionales de vigilancia y que considere las particularidades del entorno digital.

1.3 Agentes Encubiertos y Reveladores: Intervención e Implicaciones Legales

Como se ha mencionado, el marco legal para la actuación de los agentes encubiertos y reveladores en la República Argentina se encuentra regulado por la Ley 27.319, la cual establece que sus intervenciones deben ser autorizadas por un juez y solo pueden ser utilizadas como medida de última ratio, es decir, cuando otros métodos menos invasivos hayan sido agotados o se consideren inadecuados. Esta exigencia enfatiza que cualquier intervención en los derechos fundamentales debe ser proporcional al delito investigado y lo menos invasiva posible, un principio fundamental para asegurar que la actuación estatal no se convierta en una violación sistemática de los derechos individuales.

La Cámara Federal de Mar del Plata ha dicho que:

Por la propia naturaleza y modalidad de venta de estupefaciente a través de redes sociales de acceso público mediante comunicaciones anónimas y encriptadas, la intervención del agente revelador como técnica investigativa resultó la más adecuada en términos de razonabilidad y proporcionalidad, máxime cuando el delito se encontraba en pleno curso de ejecución (Resolución del 27/03/2024 - Causa FMP 11434/2023/10/CA7).

Sin embargo, la aplicación práctica de estas técnicas presenta desafíos significativos, especialmente en los entornos digitales. La infiltración en plataformas digitales, redes sociales y foros o grupos en línea puede implicar la recolección masiva de datos no solo de los sospechosos directos, sino también de terceros que no están involucrados en las actividades delictivas que resultan objeto de persecución.

Esta recolección indiscriminada plantea preocupaciones sobre la privacidad y el uso potencialmente indebido de la información obtenida. Para mitigar estos riesgos, es esencial que el control judicial sea estricto y que se apliquen rigurosamente los principios de proporcionalidad y necesidad.

Armenta Deu (2007) señala que "la actuación de los agentes reveladores requiere una regulación aún más estricta, dado que sus acciones pueden inducir o incentivar comportamientos delictivos que, de otro modo, no se habrían producido" (p. 82). Este aspecto subraya la importancia de los controles judiciales y la necesidad de normas claras para diferenciar entre la recolección legítima de información y la provocación indebida de conductas delictivas. En este sentido, la jurisprudencia ha desarrollado criterios para evaluar la legitimidad de las acciones de los agentes reveladores, especialmente en términos de su impacto en los derechos de los investigados.

Bravo Sandoval (2021) señala que "mientras más meticuloso sea el juez al evaluar lo ‘imprescindible’ del despliegue del agente, menor será el riesgo de afectación a los derechos fundamentales" (p. 134). Esto resalta la necesidad de un control judicial efectivo, que no solo evalúe la legalidad de las intervenciones, sino que también valore su impacto potencial sobre los derechos de las personas involucradas.

La supervisión judicial debe ir más allá de la mera autorización inicial y extenderse en forma continua durante todo el proceso de intervención para asegurar que las operaciones se mantengan dentro de los límites autorizados. Además, el derecho

comparado ofrece valiosas enseñanzas acerca de cómo otros sistemas legales han abordado la regulación de agentes encubiertos y reveladores.

En España, por ejemplo, la Ley de Enjuiciamiento Criminal exige una justificación detallada y específica de la necesidad de la intervención encubierta, así como una evaluación exhaustiva de alternativas menos invasivas. Mientras que, en los Estados Unidos, la protección constitucional contra registros e incautaciones no razonables impone restricciones claras sobre la actuación de agentes encubiertos, requiriendo que todas las intervenciones sean aprobadas por un juez con una evaluación previa de la expectativa razonable de privacidad de los ciudadanos.

Estas comparaciones internacionales ponen de manifiesto la importancia de contar con regulaciones detalladas y un control judicial firme para evitar abusos. En Argentina, se podría considerar la adopción de directivas o protocolos de actuación adicionales que especifiquen con mayor claridad los criterios para la autorización y supervisión de las intervenciones encubiertas, con el fin de proteger de modo más eficaz los derechos fundamentales y asegurar que las investigaciones se realicen observando todos los preceptos legales.

1.3.1 Implicaciones Éticas y Legales del Uso de Identidades Ficticias en Línea

El uso de identidades falsas por parte de los agentes encubiertos y reveladores en el ámbito digital plantea importantes dilemas éticos y legales. Por un lado, estas técnicas son necesarias en pos de intentar penetrar redes criminales altamente organizadas y/o clandestinas, que de otro modo serían inaccesibles para las autoridades. Sin embargo, la creación de identidades falsas y la interacción engañosa con sospechosos y terceros pueden llevar a violaciones de confianza y privacidad. Según Ramírez Jaramillo (2010), "el uso de identidades ficticias debe ser cuidadosamente regulado para evitar que se

convierta en una herramienta de abuso que comprometa la integridad del proceso judicial y la protección de los derechos fundamentales" (p. 30).

Una preocupación que se agrega a la temática es la posibilidad de que los agentes encubiertos, en su afán de cumplir con la misión asignada, puedan inducir a los sospechosos a cometer delitos, es decir provocar su comisión que, de otro modo, sin la participación del agente quizás no se habría producido.

Esto se conoce como *entrapment* o incitación indebida, y puede comprometer la validez posterior de las pruebas obtenidas, principalmente al momento de ser exhibidas en el debate oral (etapa de juicio) con el objeto de ser valoradas y en función de ellas dictar una sentencia absolutoria o condenatoria. Roxin (2000) advierte que "la incitación a cometer un delito por parte de un agente del estado no solo socava la confianza en la justicia, sino que también viola principios básicos de proporcionalidad y necesidad" (p. 95). Este riesgo evidencia la importancia de contar con normas estrictas y de una supervisión judicial permanente para asegurar que las acciones de los agentes se mantengan dentro de los límites legales y éticos.

1.3.2 Procesos de Control Judicial en el Uso de Agentes Encubiertos

El control judicial constituye un componente esencial para garantizar que la actuación de los agentes encubiertos y reveladores se desarrolle acorde a Derecho y de forma proporcional. En muchos sistemas legales, incluyendo el argentino, la intervención de estos agentes debe ser aprobada previamente por un juez, quien evalúa la necesidad y proporcionalidad de la medida. Sin embargo, la aprobación inicial no es suficiente; se requiere una supervisión continua para asegurar que la medida se mantenga dentro de los límites autorizados y que no se vulneren los derechos fundamentales de los investigados o de terceros.

Clusa López (2019) enfatiza que "el juez instructor debe guiar las actividades del agente encubierto bajo criterios de proporcionalidad y necesidad, y debe estar facultado para intervenir en cualquier momento si se detectan excesos o desviaciones" (p. 89). Esto implica no solo la revisión de los informes presentados por los agentes, sino la posibilidad de realizar auditorías independientes y de incluir defensores de los derechos humanos en el proceso de control.

1.4 Afectaciones Específicas a Derechos Fundamentales

1.4.1 Derecho a la Privacidad

El derecho a la privacidad es uno de los pilares fundamentales en las sociedades democráticas y está protegido por múltiples instrumentos legales tanto a nivel nacional como internacional. En el entorno digital, la vulnerabilidad de este derecho se intensifica debido a la capacidad de las tecnologías para recolectar, almacenar y analizar grandes cantidades de datos personales sin el conocimiento o consentimiento explícito de los usuarios. Esta recolección masiva y, a menudo, indiscriminada, con nulos o escasos controles, plantea desafíos significativos sobre la protección de la privacidad en un mundo interconectado.

Los agentes encubiertos, al infiltrarse en diversas plataformas digitales y otros espacios virtuales, pueden invadir considerablemente la privacidad de los usuarios, ya que estos suelen participar en el ciberespacio con la expectativa de un cierto grado de confidencialidad y protección de sus datos.

La Ley 27.319 establece ciertos límites para la actuación de los agentes encubiertos, pero la rápida evolución del entorno digital frecuentemente supera la capacidad de respuesta y adaptación legislativa. Como resultado, pueden surgir brechas en la protección de los datos personales, especialmente cuando la recolección de información

va más allá del alcance que la investigación criminal especifica y afecta a terceros no involucrados en actividades delictivas. La implementación de controles más estrictos y la adopción de protocolos específicos para la recolección y manejo de datos en investigaciones encubiertas son necesarios para minimizar los riesgos que conlleva y garantizar que las intervenciones respeten los estándares de privacidad establecidos.

Además, la falta de transparencia en la utilización de datos obtenidos por los agentes puede llevar a abusos de poder y a una erosión de la confianza pública en las instituciones encargadas de hacer cumplir la ley. Para evitar esto, es fundamental que las regulaciones no solo limiten su recolección y almacenamiento, sino que también impongan obligaciones claras sobre la destrucción o anonimización de la información recolectada una vez que ya no sea necesaria para los fines de la investigación.

1.4.1.1 Minería de Datos y Análisis de Redes Sociales como Amenazas a la Privacidad. Una de las actividades más desplegadas en el ciberespacio para la recolección de información es la minería de datos y el análisis de redes sociales. Estas técnicas permiten a los agentes encubiertos y reveladores mapear relaciones y actividades de los usuarios de manera extremadamente detallada. Por ejemplo, al analizar los patrones de interacción de un sospechoso en una red social, los agentes pueden identificar no solo sus contactos directos, sino también redes secundarias de personas que pueden estar completamente desvinculadas de hecho ilícito alguno.

Este tipo de vigilancia extendida plantea riesgos considerables para la privacidad, especialmente cuando se lleva adelante de manera masiva.

Según Alcolado Chico (2016), "la minería de datos y el análisis de redes sociales deben ser manejados con extrema cautela y siempre bajo estricta supervisión judicial para asegurar que no se violen los derechos de individuos no implicados" (p. 42). La

implementación de técnicas de minimización de datos y el uso de algoritmos que limitan la recolección a la información estrictamente necesaria para la investigación constituyen pasos críticos para proteger la privacidad en este medio.

1.4.2 Libertad de Expresión y Derecho a la No Autoincriminación

La libertad de expresión es un pilar esencial de toda sociedad democrática, permitiendo a los individuos compartir ideas, opiniones y creencias sin temor a represalias. En el entorno digital, esta libertad se manifiesta en un sinfín de páginas web, aplicaciones y otras plataformas virtuales donde los usuarios pueden interactuar y debatir sobre una amplia variedad de temas. Sin embargo, la percepción de vigilancia, especialmente cuando se trata de agentes encubiertos, puede tener un efecto disuasorio, llevando a los usuarios a autocensurarse y a limitar su participación y exposición públicas.

Este "efecto de enfriamiento" puede socavar la calidad del discurso público y restringir la diversidad de opiniones, lo cual es esencial para un debate democrático saludable. Clusa López (2019) expresa que "la presencia de agentes encubiertos en plataformas digitales puede crear un entorno de vigilancia percibida que lleva a los usuarios a evitar discusiones sensibles o controvertidas por temor a repercusiones" (p. 89). Esto es especialmente problemático en ámbitos donde las redes sociales son utilizadas para la movilización política o el activismo social.

Según Alcolado Chico (2016), "la confianza pública en las instituciones es fundamental para el funcionamiento de una sociedad democrática, y cualquier percepción de abuso o vigilancia excesiva puede tener un impacto desproporcionado en la relación entre el Estado y sus ciudadanos" (p. 55).

El derecho a no autoincriminarse también se ve comprometido cuando los agentes encubiertos inducen a los investigados a proporcionar información que podría ser

utilizada en su contra. Esta práctica no solo compromete la integridad del proceso judicial, sino que también plantea cuestiones éticas sobre el uso de la manipulación y el engaño en la recolección de pruebas.

La Sala A de la Cámara Federal de Córdoba ha mencionado que:

Respecto al trayecto de la investigación en el cual los funcionarios, simulando interés en la compra, ingresan al domicilio sin autorización judicial, considero que allí se configura una lesión a la esfera de la intimidad con efectiva violación al debido proceso y a la garantía de prohibición de la autoincriminación (Resolución del 19/08/2022 - Causa FCB 9942/2020/1/CA1).

Ramírez Jaramillo (2010) señala que "la obtención de pruebas a través de la coacción o el engaño socava la confianza en el sistema de justicia y viola principios fundamentales de equidad y debido proceso" (p. 30). Por ello, es muy importante que las intervenciones encubiertas sean cuidadosamente supervisadas para asegurar que las pruebas obtenidas no violen los derechos fundamentales de los investigados.

1.4.2.1 Desafíos del Derecho a la No Autoincriminación en Intervenciones Digitales. Los desafíos para el derecho a no autoincriminarse en los entornos digitales, se expanden debido a la facilidad con la que los funcionarios policiales pueden interactuar con los investigados y obtener información a través del engaño. A diferencia de las investigaciones convencionales, donde la interacción física limita la posibilidad de manipulación directa, en el ciberespacio, las barreras son mucho menores, y las oportunidades para inducir declaraciones autoincriminatorias son significativamente mayores.

Roxin (2000) argumenta que "la protección contra la autoincriminación debe extenderse al entorno digital con la misma rigurosidad que en los contextos tradicionales,

asegurando que cualquier interacción con agentes del estado se realice bajo condiciones justas y equitativas" (p. 105). Esto requiere que los jueces evalúen no solo la legalidad de la intervención, sino también la ética de las tácticas desplegadas por los agentes encubiertos, asegurando que no se comprometan los derechos de los individuos bajo investigación.

1.4.3 Derecho a la Presunción de Inocencia y Protección de Datos Personales

El derecho a la presunción de inocencia es un principio cardinal del derecho penal que garantiza a toda persona ser considerada inocente hasta que se demuestre su culpabilidad más allá de toda duda razonable. En el contexto digital, este derecho se enfrenta a desafíos particulares debido a la facilidad con la que los datos personales pueden ser objeto de evidencia en investigaciones penales. El uso de agentes encubiertos y reveladores en entornos digitales puede comprometer la presunción de inocencia cuando la información recolectada es interpretada fuera de contexto o utilizada de forma parcializada.

Los agentes pueden reunir grandes volúmenes de datos, algunos de los cuales pueden ser irrelevantes o incluso exculpatorios para el sospechoso. Sin embargo, la presentación de esta información en un tribunal puede ser selectiva y tendenciosa, apartándose del principio de objetividad, lo que podría llevar a conclusiones erróneas sobre la culpabilidad del acusado.

Armenta Deu (2007) sostiene que "la manipulación o interpretación sesgada de los datos recolectados por agentes encubiertos puede comprometer gravemente la presunción de inocencia y la equidad del proceso penal" (p. 83). Por lo tanto, es esencial que existan garantías para asegurar que aquellos expuestos en los juicios sean precisos, pertinentes y presentados de manera justa.

Además, la protección de los datos personales se ha convertido en un derecho fundamental en la era digital, reconocida en regulaciones internacionales como el GDPR de la Unión Europea. En Argentina, su protección está regulada por la Ley 25.326, que establece normas para el tratamiento de los datos personales y sensibles, por parte de las personas jurídicas públicas y privadas. Sin embargo, la implementación de estas normas en el contexto de las investigaciones penales, particularmente de aquellas que involucran a agentes encubiertos, presenta desafíos únicos.

Según Bravo Sandoval (2021), "la recolección de datos por agentes encubiertos en el ciberespacio plantea la necesidad de mecanismos específicos que aseguren la protección de los derechos de privacidad y la integridad" (p. 137). Esto abarca la necesidad de protocolos claros acerca de cómo se deben manejar y almacenar los mismos, así como procedimientos para la eliminación segura de aquellos que no sean necesarios para la investigación.

1.4.3.1 El Desafío de la Gestión de Datos Sensibles en Investigaciones Digitales.

En el ciberespacio, los funcionarios policiales tienen la capacidad de acceder a datos extremadamente sensibles, incluyendo información de salud, económica-patrimonial, y detalles íntimos de la vida personal de los usuarios. La gestión de los mismos es un desafío crítico, ya que su recolección y uso indebido pueden tener consecuencias devastadoras para los derechos de los sujetos afectados. Alcolado Chico (2016) argumenta que "la falta de controles adecuados en la gestión de datos sensibles por parte de los agentes encubiertos puede llevar a violaciones graves de los derechos humanos y a la erosión de la confianza pública en las instituciones encargadas de la justicia" (p. 45).

Para minimizar estos riesgos, se sugiere la adquisición de sistemas confiables de gestión de datos que incluyan su cifrado o encriptación, el acceso restringido basado en

permisos por usuario, y auditorías regulares para garantizar que lo reunido se gestione de acuerdo con los estándares internacionales de protección de aquellos. Además, se debe asegurar que cualquier recolección de datos sea directamente relevante y necesaria para los fines de la investigación, y que se minimice la exposición de aquellos correspondientes a personas no implicadas en actividades delictivas o ajenas a la investigación.

1.5 Estudios de Caso

Los estudios de caso son fundamentales para representar cómo la actuación de agentes encubiertos y reveladores puede impactar sobre los derechos humanos en la práctica. A través de ejemplos concretos, se pueden examinar los dilemas éticos y legales que surgen de la aplicación de estas técnicas, como así también se pueden identificar áreas donde son necesarias determinadas mejoras en la regulación y el control.

1. Operación Pacifier (Estados Unidos)

Descripción: En 2015, el FBI llevó a cabo la Operación Pacifier, una intervención encubierta en la *dark web* para desmantelar una red de pornografía infantil. Durante la operación, el FBI tomó control de un sitio web ilegal y permitió que continuara operando durante varias semanas, recopilando información sobre los usuarios.

Implicaciones legales y éticas: Esta operación suscitó críticas por la recolección masiva de datos de usuarios, muchos de los cuales no estaban directamente involucrados en delito alguno. Se cuestionó si las acciones del FBI eran proporcionales y si respetaban la privacidad de aquellos.

Lecciones: Este caso resalta la importancia de establecer límites claros y la necesidad de una supervisión judicial rigurosa para evitar la recolección indiscriminada de datos personales.

Según Bravo Sandoval (2021), "la Operación Pacifier puso de relieve la necesidad de regulaciones más estrictas sobre cómo y cuándo los agentes encubiertos pueden recolectar datos de individuos que no están bajo sospecha directa" (p. 140).

2. Operación Bayonet

Descripción: La Operación Bayonet fue una acción coordinada internacional liderada por el FBI, la DEA, la Europol y otras agencias de seguridad para desmantelar AlphaBay y Hansa Market, dos de los mercados más grandes en la *dark web* dedicados al tráfico de drogas, armas, datos robados, y otros bienes ilegales. AlphaBay, en particular, era uno de los mayores mercados de la *dark web* con más de 200,000 miembros y 40,000 vendedores. La operación fue significativa porque, tras cerrar AlphaBay, las autoridades redirigieron a sus usuarios a Hansa Market, que ya estaba bajo control de la policía, lo que permitió la captura de cientos de involucrados y la recolección de datos de sumo interés.

Implicaciones legales y éticas: La operación se destacó por su innovador enfoque de doble golpe y evidenció la importancia de la cooperación internacional en la lucha contra el cibercrimen. En contraposición, también planteó algunas preocupaciones sobre la recolección masiva de datos y la vigilancia sin el conocimiento de los usuarios, cuestionando los límites de la proporcionalidad y el respeto a los derechos fundamentales.

Lecciones: Este caso resalta la efectividad de la cooperación internacional y las tácticas innovadoras en la lucha contra el crimen en la *dark web*. No obstante, exhibe la necesidad de protocolos claros en torno a las fases de tratamiento de la información y de un control judicial fuerte en pos de garantizar que las operaciones no vulneren los derechos de los individuos no implicados directamente en la investigación.

3. Operación Trojan Shield / Ironside (Internacional)

Descripción: Esta operación internacional, liderada por el FBI y la Policía Federal Australiana, utilizó una aplicación de mensajería encriptada que había sido secretamente desarrollada por las agencias de seguridad para infiltrarse en redes de crimen organizado.

Los agentes monitorizaron las comunicaciones durante meses, lo que llevó al arresto de cientos de delincuentes en todo el mundo.

Consideraciones éticas: Aunque fue exitosa, la operación generó cuestionamientos sobre la ética de usar herramientas diseñadas especialmente para la privacidad y cómo se gestionó la recolección masiva de registros de comunicaciones.

Aspectos legales: La operación muestra la necesidad de normativas claras sobre el uso de herramientas tecnológicas en investigaciones encubiertas y cómo se equilibran estas acciones con los derechos a la privacidad y la protección de datos.

4. Operación Gold Dust (Canadá)

Descripción: En Canadá, la Operación *Gold Dust* involucró a la RCMP (Policía Montada de Canadá) en la infiltración de redes de lavado de dinero en criptomonedas.

Los agentes encubiertos accedieron a foros y plataformas online donde se intercambiaban criptomonedas de forma ilegal.

Desafíos identificados: La operación exhibió la dificultad de definir límites claros para la recolección de datos en plataformas donde los usuarios frecuentemente combinan actividades legales e ilegales. Ello provocó debates sobre cómo asegurar que las intervenciones encubiertas no invadan la privacidad de los usuarios legítimos.

Recomendaciones: La implementación de auditorías independientes y la participación de especialistas en privacidad para revisar la recolección de datos y asegurar el cumplimiento con los estándares internacionales en derechos humanos.

5. Caso de la Vigilancia Masiva en Hong Kong

Descripción: Durante las protestas en Hong Kong en 2019, se reveló que las autoridades utilizaban agentes encubiertos en plataformas digitales para identificar y vigilar a los organizadores de las protestas. Esta intervención se extendió también al seguimiento de conversaciones en redes sociales y aplicaciones de mensajería.

Implicaciones en Derechos Humanos: El caso ejemplifica cómo la falta de restricciones y control judicial puede conducir al abuso de las técnicas de vigilancia digital, afectando gravemente la libertad de expresión y el derecho a la privacidad.

Medidas propuestas: Refuerza la necesidad de protocolos internacionales para regir el uso de agentes encubiertos en contextos políticos y proteger los derechos.

Bravo Sandoval (2021) propone que "las lecciones aprendidas de operaciones como Pacifier y Darknet deben guiar la formulación de nuevas políticas y regulaciones que fortalezcan la protección de los derechos fundamentales en el contexto de las investigaciones penales" (p. 142).

Capítulo 2: Fundamentos Jurídicos y Límites de la Actuación de Agentes Encubiertos y Reveladores

2.1 Marco Legal de Actuación

En la República Argentina, como ya se ha mencionado, la Ley 27.319 regula las técnicas especiales de investigación, entre ellas las inherentes a los agentes encubiertos y reveladores. Cabe destacar que la norma en cuestión no alude específicamente al desempeño de dichas figuras en el entorno digital, al no mencionar un ámbito espacial específico de intervención, a diferencia por ejemplo de la provincia de Mendoza, que crea la figura del agente encubierto digital a través de la Ley 9.510 de reforma al Código Procesal Penal de la provincia, idéntica reforma ha sido incluida en el ordenamiento procesal penal de la provincia de Salta.

Si bien en el ámbito nacional se han redactado proyectos de reforma a la Ley 27.319 a fin de crear la figura del agente encubierto informático, la aprobación de los mismos a la fecha no ha prosperado.

No obstante, la redacción de esta última ley responde, aunque en forma parcializada y con limitaciones, a la creciente complejidad de los delitos informáticos y la necesidad de dotar a las autoridades de herramientas efectivas para enfrentar tales desafíos. La normativa establece que las intervenciones de los agentes encubiertos y reveladores deben estar respaldadas por una autorización judicial previa y ser consideradas como última ratio, es decir, deben emplearse solo cuando otros métodos menos invasivos hayan fracasado o sean inadecuados.

El marco legal enfatiza la importancia de los principios de legalidad, necesidad y proporcionalidad como ejes fundamentales para la autorización de estas intervenciones.

El principio de proporcionalidad, en particular, desempeña un rol central al exigir que cualquier intervención sobre los derechos individuales sea proporcionada al objetivo de la investigación, minimizando así las afectaciones innecesarias a la privacidad, la libertad de expresión y otros derechos individuales. Según Armenta Deu (2007), "la proporcionalidad es una técnica jurídica que permite ponderar los intereses públicos y los derechos individuales, garantizando que la persecución de los delitos no se realice a costa de la vulneración de los derechos fundamentales" (p. 75).

A pesar de las disposiciones legales, la práctica pone de manifiesto determinados obstáculos en la implementación efectiva de estas garantías. Uno de los problemas recurrentes viene dado por la interpretación y aplicación del principio de proporcionalidad, que puede variar entre jueces y tribunales, generando decisiones dispares y, en ocasiones, inconsistentes. Para abordar esta problemática, es fundamental que se desarrollen guías y criterios más detallados para los jueces encargados de evaluar

las solicitudes de intervención encubierta, asegurando una aplicación uniforme y equitativa de la ley.

La normativa también requiere que los jueces realicen una supervisión continua de las operaciones encubiertas, evaluando periódicamente la necesidad y proporcionalidad de la medida. Este control se advierte esencial para evitar desviaciones del propósito autorizado y garantizar que las actuaciones de los agentes no se extiendan más allá de los límites permitidos por la ley.

2.1.1 Requisitos y Procedimientos para su Autorización

El proceso destinado a la autorización del empleo de agentes encubiertos en la República Argentina está diseñado para incluir múltiples recaudos que protejan los derechos subjetivos. El juez a cargo de la investigación o ante el cual sea solicitada la autorización de la medida por parte del fiscal, previo a autorizar la intervención debe evaluar rigurosamente la necesidad y proporcionalidad de la misma, y debe asegurarse de que todas las demás alternativas menos invasivas hayan sido agotadas.

Clusa López (2019) menciona que "la supervisión judicial no debe ser un mero trámite burocrático, sino un proceso activo y reflexivo que evalúe todos los posibles impactos de la intervención en los derechos fundamentales" (p. 92).

Para Daray (2019) un amplio sector de la doctrina sostiene que los derechos no son absolutos frente a determinadas situaciones de urgencia y excepcionales, y que tales derechos se pueden restringir o afectar en mayor medida que la ordinaria cuando, por ejemplo, estén en juego la seguridad o el bien común en una sociedad democrática.

El juez también debe establecer los límites precisos de la actuación del agente, incluyendo el ámbito de la infiltración, la duración de la operación, y los tipos de datos que pueden ser reunidos. Este nivel de especificidad es importante para prevenir abusos

y garantizar que la intervención se mantenga dentro de los parámetros legales establecidos. Además, cualquier modificación en el alcance o la duración de la medida debe ser aprobada nuevamente por el juez, lo que garantiza una supervisión continua y dinámica de la intervención.

2.2 Derecho Comparado: España y Estados Unidos

El análisis comparativo con otros sistemas legales proporciona una perspectiva de sumo interés acerca de cómo se regula la actuación de agentes encubiertos y reveladores en diferentes contextos. En España, la Ley de Enjuiciamiento Criminal establece estrictos requisitos para la autorización de estas técnicas de investigación, destacando la necesidad de que los jueces evalúen no solo la legalidad de la intervención, sino también su proporcionalidad y necesidad en cada caso concreto. Esta legislación exige una justificación detallada que explique por qué la intervención encubierta es la mejor opción en detrimento de otras y evalúe exhaustivamente las alternativas disponibles.

El Tribunal Constitucional Español ha insistido en que la actuación de agentes encubiertos debe estar sujeta a un control judicial riguroso para evitar abusos y proteger los derechos de los investigados. Este control incluye la revisión continua de las actuaciones y la obligación de documentar todas las actividades realizadas por los agentes, asegurando que la información obtenida sea utilizada exclusivamente para los fines autorizados y no se viole la privacidad de los individuos no relacionados con el delito investigado.

En Estados Unidos, la actuación de *undercover agents* (agentes encubiertos) en investigaciones cibernéticas está regulada principalmente por la Cuarta Enmienda de la Constitución, que protege a los ciudadanos contra registros e incautaciones no razonables.

La intervención de agentes encubiertos debe ser aprobada por un juez que evalúe la

justificación y la proporcionalidad de la medida, asegurando que se cumplan los estándares constitucionales de protección de los derechos individuales. La jurisprudencia estadounidense ha desarrollado un enfoque centrado en la "expectativa razonable de privacidad", evaluando cómo la intervención de los mismos afecta esta expectativa y qué medidas son necesarias para protegerla.

En ambos países, la existencia de garantías judiciales consolidadas y un marco normativo claro ha permitido un uso más controlado y ético de las técnicas de investigación encubierta. La adopción de elementos de estos sistemas extranjeros podría mejorar la regulación en Argentina, especialmente en lo que respecta a la especificación de criterios para la autorización judicial y la implementación de procesos de revisión independientes. La creación de un estándar más detallado para la actuación de agentes encubiertos podría contribuir a una mayor uniformidad en las decisiones judiciales.

2.2.1 Comparación con Otros Sistemas Legales: Canadá y Australia

Además de España y los Estados Unidos, otros sistemas legales como los de Canadá y Australia han desarrollado marcos regulatorios específicos para la actuación de agentes encubiertos en el contexto del cibercrimen, abordando la protección de los derechos y la transparencia en las operaciones encubiertas. Los mismos incluyen disposiciones detalladas para la documentación, supervisión y auditoría de las actividades de los agentes, y ofrecen importantes lecciones que podrían ser aplicadas en otros países, como Argentina.

En Canadá, la actuación de los agentes encubiertos está regulada por la Ley de Protección de Información Personal y Documentos Electrónicos (PIPEDA), que establece estrictos requisitos para la recolección y uso de datos personales, incluyendo aquellos recolectados durante investigaciones penales. Esta ley no solo impone la necesidad de

documentar todas las actividades realizadas durante una intervención encubierta, sino que también facilita la supervisión judicial y la auditoría independiente, proporcionando un marco sólido para la protección de los derechos individuales en el ámbito digital.

Además, las operaciones encubiertas en Canadá deben ser aprobadas por un juez, quien evalúa la legalidad y proporcionalidad de las intervenciones, conforme a los principios establecidos en la Carta Canadiense de Derechos y Libertades, que exige que cualquier interferencia en los derechos fundamentales sea razonable y justificada en una sociedad libre y democrática. Según Alcolado Chico (2016), "la documentación detallada y la supervisión judicial continua son elementos clave en la regulación canadiense, proporcionando un alto nivel de transparencia y rendición de cuentas" (p. 55).

Similarmente, en Australia, la regulación de los agentes encubiertos en entornos digitales está contemplada en la Ley de Vigilancia y Control de Delitos *(Surveillance Devices Act)*, la cual establece procedimientos claros para la autorización y control de las operaciones encubiertas. Esta ley no solo regula la recolección de datos personales, sino también cómo deben ser almacenados, utilizados y, eventualmente, eliminados.

La normativa australiana enfatiza la minimización de la intrusión, limitando la recolección de datos a lo estrictamente necesario para la investigación y asegurando que cualquier uso adicional de estos sea justificado y aprobado judicialmente. Bravo Sandoval (2021) destaca que "el enfoque australiano en la minimización de la intrusión y la protección de los datos personales podría servir como un modelo para mejorar las regulaciones en otras jurisdicciones, incluyendo Argentina" (p. 148).

La normativa australiana también incluye disposiciones específicas para la protección de los datos personales reunidos durante las operaciones, exigiendo que sean gestionados de acuerdo con estándares estrictos de protección, y limitando su uso al propósito original de la investigación. Alcolado Chico (2016) argumenta que "la adopción

de principios similares en Argentina podría ayudar a mitigar los riesgos de abuso y proteger mejor los derechos a la privacidad y la protección de datos personales" (p. 47).

El análisis comparativo con otras jurisdicciones, como las de Canadá y Australia, no solo proporciona una perspectiva sobre cómo estos países abordan la actuación de los agentes encubiertos y reveladores, sino que también permite identificar prácticas que podrían mejorar la regulación en Argentina. La integración de estas mejores prácticas podría fortalecer la regulación argentina, garantizando una mayor protección de los derechos fundamentales mientras se preserva la eficacia de las investigaciones criminales en el entorno digital.

2.3 Definición de los Límites de Actuación

Establecer límites a la actuación de los agentes encubiertos y reveladores resulta esencial para evitar abusos y proteger a la ciudadanía. Los mismos incluyen la necesidad de una autorización judicial previa, la evaluación rigurosa de la proporcionalidad y la necesidad de la intervención en función de los resultados obtenidos, y la implementación de controles y supervisión continuos durante todo el proceso de investigación.

Clusa López (2019) afirma que "el juez instructor debe guiar las actividades del agente encubierto bajo criterios de proporcionalidad, como medida garantista de los derechos fundamentales" (p. 89). Estos controles judiciales son fundamentales para asegurar que las investigaciones no comprometan los derechos individuales y se desarrollen de modo equitativo.

Uno de los aspectos clave en la definición de los límites es la duración de la operación encubierta. La ley establece que las autorizaciones deben ser temporales y sujetas a renovación periódica basada en la revisión de la necesidad continua de la intervención. Esto asegura que las operaciones no se prolonguen indefinidamente y que

los jueces tengan la oportunidad de evaluar regularmente la proporcionalidad de la intervención en función de los resultados obtenidos.

Roxin (2000) enfatiza que *"la limitación temporal de las operaciones encubiertas es esencial para prevenir la escalada de la vigilancia y para mantener un control efectivo sobre las actividades de los agentes"* (p. 108).

Además, es fundamental establecer límites claros sobre el ámbito de la operación, especificando qué áreas o plataformas digitales pueden ser objeto de infiltración y qué tipos de datos pueden ser recolectados. Estos límites deben basarse en la relevancia directa de la información para la investigación y en la minimización del impacto en los derechos de los individuos no implicados en actividades delictivas. La definición precisa de estos parámetros es esencial para garantizar que la intervención se mantenga dentro de los límites legales y éticos.

2.4 Evaluación Crítica de la Legislación Argentina y Propuestas de Mejora

Aunque la Ley 27.319 proporciona el marco legal para la actuación de agentes encubiertos y reveladores en Argentina, existen áreas en las que la legislación podría mejorarse para asegurar una protección más sólida de los derechos fundamentales. Una de las críticas comunes a la ley es que, aunque exige autorización judicial previa para la actuación de los agentes, no especifica de manera detallada los criterios que los jueces deben utilizar para evaluar la proporcionalidad y necesidad de la intervención. Esto puede llevar a una variabilidad en la aplicación de la ley y a decisiones inconsistentes o discrecionales basadas en aspectos subjetivos que comprometan los derechos individuales.

Para abordar estas limitaciones, se propone la introducción de criterios más específicos en la ley que guíen a los jueces en su evaluación de las solicitudes de

intervención encubierta. Estos criterios podrían incorporar una evaluación detallada de los riesgos para los derechos fundamentales de acuerdo al caso concreto, la consideración de alternativas menos invasivas o gravosas y la obligación de realizar una revisión periódica con el objeto de evaluar la necesidad de continuar con la intervención. Además, se sugiere la implementación de procesos de revisión independientes, como grupos de supervisión o la participación de especialistas externos, para asegurar que las decisiones sean acordes al Derecho.

Otras propuestas son la ampliación de los derechos de los sujetos afectados por las intervenciones encubiertas, incluyendo el derecho a ser informado post facto sobre la intervención, el acceso a vías efectivas de reparación en caso de excesos que hayan vulnerado sus derechos y garantías y la incorporación de programas de capacitación continua específica para jueces y fiscales. Esto alinearía la legislación argentina con las mejores prácticas internacionales.

2.5 El Rol del Poder Judicial en la Supervisión de las Operaciones Encubiertas

El poder judicial desempeña un papel crucial en la supervisión y control de las operaciones encubiertas, asegurando que estas se realicen dentro de los límites legales y respeten los derechos individuales. La autorización judicial previa es un requisito esencial, pero la supervisión no debe detenerse allí; debe ser un proceso continuo que involucre la revisión regular de los informes de los agentes encubiertos, la evaluación de la proporcionalidad de la intervención y la capacidad de intervenir rápidamente si se detectan excesos o desviaciones.

En Argentina, los jueces tienen la responsabilidad de autorizar y supervisar las operaciones encubiertas, pero la eficacia de esta supervisión puede variar dependiendo de la carga de trabajo, la disponibilidad de recursos y la formación específica en derechos

digitales y privacidad. Clusa López (2019) sugiere que "la capacitación continua de los jueces en temas relacionados con la protección de los derechos digitales y la vigilancia en el ciberespacio es esencial para asegurar que las decisiones judiciales se alineen con los más altos estándares de protección de los derechos fundamentales" (p. 96).

2.5.1 Fortalecimiento del Control Judicial a través de la Capacitación y la Asistencia Técnica

Para mejorar la supervisión judicial, se propone la implementación de programas de capacitación continua para jueces, fiscales y otros actores judiciales que participan en el diligenciamiento de intervenciones encubiertas. Estos programas deberían incluir módulos específicos sobre derechos digitales, protección de datos personales, y las técnicas de investigación más comunes en el ciberespacio. La actualización constante de los conocimientos y habilidades de los funcionarios es crucial para adaptarse a las rápidas evoluciones del cibercrimen y las tecnologías digitales, y para asegurar que las decisiones judiciales se tomen con un enfoque equilibrado y basado en el respeto a los derechos fundamentales.

Además, los agentes deberían recibir capacitación específica sobre cómo operar en entornos digitales de manera que minimice las afectaciones a los derechos humanos. Esto podría incluir entrenamiento en la identificación y manejo de datos sensibles, la comunicación con los investigados y la documentación adecuada de todas las interacciones y actividades realizadas durante la operación.

Alcolado Chico (2016) sugiere que "la capacitación especializada y continua es fundamental para asegurar que los agentes encubiertos actúen de manera ética y legal, y para minimizar los riesgos de abusos en las intervenciones encubiertas" (p. 67).

Además, debe considerarse la creación de unidades de asistencia técnica dentro del poder judicial, compuestas por especialistas en tecnología, derecho informático y protección de datos, que puedan brindar asesoramiento especializado a los magistrados en casos complejos de vigilancia digital. Estas unidades podrían ayudar a evaluar la legalidad y la proporcionalidad de las intervenciones propuestas, ofreciendo una perspectiva técnica que complemente la evaluación jurídica tradicional. Según Bravo Sandoval (2021), "la integración de expertos técnicos en el proceso judicial puede mejorar significativamente la capacidad de los jueces para tomar decisiones informadas y equilibradas en casos de vigilancia digital" (p. 152).

Capítulo 3: Propuestas para Minimizar los Riesgos y Garantizar el Equilibrio entre Seguridad y Derechos Fundamentales

3.1 Proporcionalidad como Garantía de los Derechos Fundamentales

Según Armenta Deu (2007), la proporcionalidad es un enfoque jurídico que equilibra los intereses del público con los derechos individuales, asegurando que la persecución de delitos no comprometa los derechos fundamentales.

Se trata de una piedra angular en la regulación de las intervenciones encubiertas, ya que busca equilibrar la necesidad de una investigación eficaz con la protección de los derechos fundamentales de los individuos. Este principio exige que cualquier restricción de derechos sea no solo adecuada y necesaria, sino también proporcional al objetivo legítimo que se persigue. En el contexto de los agentes encubiertos y reveladores, la proporcionalidad debe ser evaluada minuciosamente en cada etapa de la intervención, desde la autorización inicial hasta la supervisión continua de las actividades.

En la práctica, la aplicación del principio de proporcionalidad requiere que los jueces consideren alternativas menos invasivas antes de autorizar el despliegue de agentes

encubiertos. Esto conlleva una evaluación detallada de todas las opciones disponibles y una justificación clara de por qué una intervención encubierta es imprescindible. Además, debe haber una revisión continua de la intervención para asegurarse de que sigue siendo necesaria y proporcional en todas sus fases.

La proporcionalidad también se extiende al manejo de los datos recolectados durante las operaciones encubiertas. Deben establecerse límites claros sobre qué tipo de información puede ser recopilada y cómo debe ser utilizada, garantizando que cualquier injerencia en la vida privada de los individuos esté estrictamente relacionada con los fines de la investigación.

Armenta Deu (2007) señala que "la proporcionalidad en el contexto de la recolección de datos digitales implica no solo una evaluación de la necesidad de la intervención, sino también una consideración cuidadosa de la cantidad y calidad de los datos recolectados, y de los posibles impactos en los derechos de los individuos no implicados" (p. 94).

3.1.1 Estrategias para la Implementación Efectiva del Principio de Proporcionalidad

Para asegurar la implementación efectiva del principio de proporcionalidad en aquellas investigaciones que involucren tanto a agentes encubiertos como reveladores, es menester contar con estrategias detalladas y procedimientos estandarizados, que incorporen:

1. **Evaluaciones de Impacto en los Derechos Humanos (EIDH):** Previo a autorizar cualquier intervención encubierta, es fundamental que los jueces lleven a cabo evaluaciones detalladas de los posibles impactos en los derechos fundamentales de los sujetos afectados. Estas evaluaciones no deben centrarse únicamente en los beneficios de la intervención para la investigación criminal, sino que también deben considerar los

riesgos significativos para los derechos de privacidad, libertad de expresión, y otros derechos humanos esenciales.

Bravo Sandoval (2021) enfatiza que "las EIDH son herramientas críticas para asegurar que las decisiones judiciales se basen en un entendimiento completo de los impactos de las intervenciones encubiertas en los derechos de los individuos" (p. 157). Además, la integración de especialistas en derechos humanos durante el proceso de evaluación podría enriquecer la perspectiva.

2. **Limitaciones Claras y Específicas de la Recolección de Datos:** La recolección de datos debe estar estrictamente limitada a la información directamente relevante y necesaria para la investigación en curso, evitando en la medida de lo posible que no afecte a terceros no involucrados.

Esto requiere la definición precisa de los tipos de datos permitidos, protocolos específicos sobre cómo deben ser manejados y almacenados, y medidas rigurosas para garantizar su seguridad y confidencialidad. Según Alcolado Chico (2016), "la implementación de controles estrictos sobre la recolección y manejo de datos es esencial para proteger la privacidad y otros derechos fundamentales en las investigaciones encubiertas" (p. 60).

3. **Revisión Periódica de la Necesidad y Proporcionalidad:** La autorización de operaciones encubiertas no debe considerarse un evento único; en cambio, debe someterse a una revisión periódica para asegurar que la intervención siga siendo necesaria, proporcional y adecuada a la luz de los avances en la investigación.

Los jueces deberían reevaluar la intervención en intervalos regulares, teniendo en cuenta cualquier cambio en las circunstancias del caso, los resultados obtenidos, y el impacto continuo sobre los derechos fundamentales. Roxin (2000) destaca que "la revisión continua de la proporcionalidad es crucial para evitar que las operaciones

encubiertas se prolonguen más allá de lo necesario y para asegurar que los derechos fundamentales sean respetados en todo momento" (p. 114).

3.2 Ideas para Mejorar la Regulación y Supervisión

El desarrollo de regulaciones mejoradas y un sistema de supervisión más estricto es esencial para garantizar que la utilización de agentes encubiertos y reveladores en entornos digitales cumpla con altos estándares legales y éticos. Las propuestas incluyen:

1. **Creación de un Marco Normativo Detallado para la Actuación en Entornos Digitales:** Aunque la Ley 27.319 establece un marco general para la actuación de agentes encubiertos, no aborda de manera específica las complejidades y particularidades que presentan las intervenciones en entornos digitales.

Es importante desarrollar reglas que aborden estos desafíos, incluyendo la recolección masiva de datos, la vigilancia en redes sociales, y el uso de tecnologías avanzadas como la inteligencia artificial y la analítica de big data. Según Alcolado Chico (2016), "un marco normativo específico para las intervenciones digitales es esencial para garantizar que los derechos fundamentales sean protegidos adecuadamente en el contexto de la investigación criminal" (p. 64).

2. **Establecimiento de Equipos de Supervisión Independientes:** La creación de equipos de supervisión independientes que incluyan a especialistas en derecho informático, tecnología, y ética judicial, así como representantes de la sociedad civil, puede contribuir significativamente al control y monitoreo de las operaciones encubiertas.

Estos equipos serían responsables de revisar las solicitudes de intervención, monitorear las operaciones en curso, y realizar auditorías periódicas para asegurar que las prácticas de los agentes se alineen con los estándares legales y éticos establecidos. Bravo Sandoval (2021) sugiere que "la inclusión de expertos independientes en la supervisión

de las operaciones encubiertas puede proporcionar una evaluación objetiva y equilibrada de los riesgos y beneficios de estas intervenciones" (p. 160).

3. **Implementación de Protocolos de Transparencia y Rendición de Cuentas:** La transparencia y la rendición de cuentas son elementos fundamentales para mantener la confianza pública en las instituciones de justicia y seguridad. Se propone la implementación de protocolos que incluyan la publicación de informes sobre el uso de agentes encubiertos y reveladores y los resultados obtenidos.

La rendición de cuentas debe ser un componente central de la regulación, con procedimientos claros y estrictos para la revisión y auditoría de las intervenciones encubiertas. Armenta Deu (2007) enfatiza que "la transparencia y la rendición de cuentas son pilares esenciales para garantizar la legitimidad de las acciones del Estado y para proteger los derechos fundamentales en el contexto de las investigaciones penales" (p. 97).

3.3 Propuestas para un Equilibrio entre Seguridad y Derechos Fundamentales

El equilibrio entre la seguridad y la protección de los derechos fundamentales es un desafío central en el uso de agentes encubiertos en entornos digitales. Bernardo San José (2009) argumenta que mantener un equilibrio justo entre el respeto a los derechos del imputado y la eficacia en la persecución penal es esencial para el proceso penal.

Los fines del Estado de Derecho, como la protección de la sociedad y el resguardo de la libertad, a menudo son de naturaleza contrapuesta, lo que requiere un balance cuidadoso y continuo. Roxin (2000) afirma que "la injerencia en el ámbito privado sólo está permitida en tanto está autorizada expresamente por el legislador" (p. 122), destacando que estas injerencias deben cumplir condiciones estrictas para manifestar un

equilibrio entre el interés en la investigación criminal y la protección de los derechos individuales.

Para establecer un equilibrio entre seguridad pública y protección de los derechos fundamentales en el contexto de las intervenciones encubiertas, se proponen las siguientes acciones:

1. **Desarrollo de Protocolos de Actuación Específicos para Agentes Encubiertos y Reveladores en Entornos Digitales:** Es muy importante que los agentes que operan en el ciberespacio cuenten con protocolos específicos que orienten sus acciones. Los mismos deben incluir directivas claras sobre la recolección, almacenamiento y uso de datos personales, así como sobre la interacción con los investigados, asegurando que las intervenciones minimicen el impacto en terceros no implicados.

Clusa López (2019) enfatiza que "los protocolos específicos para las operaciones digitales son esenciales para proporcionar un marco claro y ético para la actuación de los agentes encubiertos" (p. 101). La constante actualización de estos protocolos, en respuesta a la evolución tecnológica, sería fundamental para mantener su relevancia y eficacia.

2. **Fomento de la Educación y la Concienciación Pública sobre los Derechos en el Ciberespacio:** La protección de los derechos en el ciberespacio requiere no solo de regulaciones y supervisión estatal, sino también de una ciudadanía informada y proactiva.

Se sugiere la implementación de programas educativos continuos para todas las edades, abordando temas como la privacidad en línea, la seguridad digital, y los derechos individuales en el entorno digital.

Bravo Sandoval (2021) destaca que "una ciudadanía informada es una de las mejores defensas contra los abusos y un pilar fundamental para el mantenimiento de una sociedad democrática y justa" (p. 164). Incluir módulos sobre derechos digitales en la

educación obligatoria y campañas de sensibilización a través de medios de comunicación masiva podría fortalecer la resiliencia social frente a las injerencias indebidas.

3. **Participación de Especialistas Independientes en la Evaluación de Solicitudes de Intervenciones Encubiertas:** Incluir a especialistas independientes en el proceso de evaluación de solicitudes para intervenciones encubiertas puede aportar una perspectiva adicional, asegurando que las decisiones se tomen con un enfoque equilibrado que contemple todos los riesgos y beneficios. Estos podrían evaluar tanto los criterios de proporcionalidad y necesidad como los impactos potenciales sobre los derechos fundamentales, proporcionando una capa adicional de protección y objetividad.

Armenta Deu (2007) sostiene que "la participación de expertos independientes en la evaluación de las intervenciones encubiertas puede fortalecer la legitimidad de las decisiones judiciales y asegurar que los derechos fundamentales sean protegidos adecuadamente" (p. 99). Se podrían establecer comisiones mixtas con representantes de distintas disciplinas, incluyendo tecnología, ética, derechos humanos y derecho penal, para abordar de manera integral y multidimensional las solicitudes de intervención.

3.4 Mecanismos de Minimización de la Intrusión y Protección de Datos

Para reducir al mínimo la injerencia en la privacidad y proteger los datos recabados, los protocolos deben incorporar medidas específicas tendientes a su minimización, que limiten la recolección a la información estrictamente necesaria para la investigación y eviten la recolección de aquellos pertenecientes a terceros no implicados.

Además, todos los datos reunidos deben ser almacenados de manera segura y manejados conforme a estándares estrictos de protección, incluyendo la encriptación de aquellos de carácter sensible y la restricción del acceso a personal autorizado, observando las previsiones de la Ley 25.326 y su decreto reglamentario.

La eliminación segura de datos innecesarios es otra medida crucial que debe incluirse en los protocolos, asegurando que cualquier dato que no sea relevante para la investigación sea eliminado de manera segura y permanente para evitar su uso indebido o la exposición accidental. Roxin (2000) enfatiza que "la implementación de medidas de minimización de la intrusión y la protección de datos no solo protege los derechos fundamentales, sino que también fortalece la legitimidad de las operaciones encubiertas al reducir los riesgos de abusos y violaciones de derechos" (p. 118).

3.5 Revisión y Actualización Continua de la Legislación y Procedimientos

Teniendo en cuenta la acelerada evolución de las tecnologías digitales como también de las técnicas utilizadas por los delincuentes en el ciberespacio, la legislación y los procedimientos relacionados con la actuación de agentes encubiertos y reveladores deben ser objeto de revisión y actualización continua. Para ello, se propone la creación de un grupo de trabajo permanente compuesto por especialistas en derecho penal, derechos humanos, ciberseguridad y tecnología, que supervise y revise periódicamente las leyes y regulaciones vigentes.

Este grupo de trabajo podría brindar recomendaciones y propuestas de reforma legislativa para la actualización de las normas legales vigentes, a fin de asegurar que se mantenga relevante y efectiva frente a los desafíos que el cibercrimen supone.

Además, la revisión permanente de los procedimientos policiales para los agentes podría ayudar a identificar áreas de mejora y asegurar que las intervenciones se realicen de la manera más eficiente y respetuosa posible con los derechos fundamentales. Esta revisión debería incluir la recopilación estadística y el análisis de datos sobre las intervenciones realizadas, con el objetivo de identificar tendencias, evaluar la eficacia de las mismas y proponer cambios que puedan mejorar los resultados.

3.6 Creación de Marcos Regulatorios Internacionales de Intervención

Considerando que el cibercrimen se caracteriza por trascender las fronteras nacionales, existe una necesidad creciente de marcos regulatorios internacionales que armonicen las prácticas de los agentes encubiertos y reveladores en las diferentes jurisdicciones. La ausencia de un marco jurídico común puede llevar a inconsistencias en la aplicación de la ley y a la posibilidad de que los delincuentes exploten las brechas legales entre países. Por lo tanto, se propone la creación de un marco regulatorio internacional, posiblemente bajo el aval de organismos como la ONU o de Interpol, que establezca estándares mínimos de actuación para los agentes encubiertos y reveladores en el ciberespacio.

Este marco debería incluir los principios fundamentales de legalidad, proporcionalidad y necesidad, así como lineamientos claros para la recolección, almacenamiento y uso de datos personales. También, deberían articularse acuerdos para la cooperación y coordinación internacional en investigaciones encubiertas, asegurando que los agentes que operan en distintas jurisdicciones cumplan con las leyes de cada país involucrado.

3.7 Integración de la Inteligencia Artificial en las Operaciones Encubiertas

La integración de inteligencia artificial (IA) y otras tecnologías avanzadas en las operaciones encubiertas representa tanto una oportunidad como un desafío. Por un lado, estas tecnologías pueden mejorar la eficacia de las investigaciones mediante el análisis de grandes volúmenes de datos y la identificación de patrones que podrían pasar desapercibidos para los investigadores humanos. Por otro lado, la utilización de IA

plantea nuevas preguntas sobre la privacidad, la precisión de los datos y la posibilidad de sesgos en los algoritmos.

Para mitigar estos riesgos, es crucial desarrollar protocolos éticos y legales específicos para el uso de IA en operaciones encubiertas. Estos protocolos deberían garantizar que la recolección de datos se realice de manera legal y proporcional, y que los algoritmos utilizados sean transparentes, auditables y libres de sesgos que puedan afectar negativamente a los individuos involucrados. Además, la supervisión humana debe ser un componente esencial en cualquier proceso que involucre IA, asegurando que las decisiones críticas no se dejen enteramente en manos de máquinas. Armenta Deu (2007) destaca que "la integración de tecnologías avanzadas en las operaciones encubiertas debe ser acompañada de salvaguardias robustas para proteger los derechos fundamentales y asegurar la equidad en las investigaciones" (p. 102).

Conclusiones

El uso de agentes encubiertos y reveladores en entornos digitales se ha convertido en una herramienta fundamental en la lucha contra el cibercrimen, especialmente en un contexto donde la criminalidad organizada aprovecha las ventajas tecnológicas para operar de manera clandestina y transnacional. A lo largo de este trabajo, se ha analizado la regulación vigente en la República Argentina, así como las prácticas de otros países, destacando la necesidad de encontrar un equilibrio adecuado entre la eficacia de las investigaciones y la protección de los derechos fundamentales de los ciudadanos.

Una de las conclusiones que más se destaca es la importancia del principio de proporcionalidad en la autorización y control posterior de estas intervenciones. No solo actúa como una garantía para evitar abusos en la recolección de los datos y la violación de la privacidad, sino que también sirve como un criterio esencial para evaluar la

necesidad y adecuación de las medidas adoptadas en cada caso. Esta cuestión es especialmente crítica en un entorno digital donde la capacidad para recopilar, almacenar y analizar información es prácticamente ilimitada.

Las propuestas presentadas en este trabajo abarcan la implementación de protocolos específicos para el despliegue de estos funcionarios en entornos digitales, la creación de organismos de control independientes y la introducción de medidas de reparación para los afectados por posibles abusos. Además, se destaca la necesidad de capacitar continuamente a los actores judiciales y a los funcionarios policiales en derechos digitales y protección de datos, asegurando que sus actuaciones se ajusten a los estándares de respeto a los derechos humanos.

Otra conclusión relevante es la urgencia de establecer marcos regulatorios internacionales que armonicen las prácticas de estos agentes a nivel global. Dado que el cibercrimen trasciende fronteras, la cooperación y coordinación internacional son esenciales para combatir de manera efectiva estas amenazas mientras se protegen los derechos individuales de los ciudadanos de las jurisdicciones involucradas.

En definitiva, este trabajo reafirma que la actuación de agentes encubiertos y reveladores en entornos digitales debe estar sujeta a un marco normativo consolidado, en constante revisión y alineado con los principios democráticos. Solo a través de una regulación adecuada, un control estricto y un compromiso claro con la protección de los derechos fundamentales, es posible utilizar estas técnicas de investigación de manera justa y efectiva en la lucha contra el cibercrimen.

Referencias

ALCOLADO CHICO, M. T. (2016). *La evolución hacia la moderna funcionalidad del "Agente Encubierto": Incidencia de las nuevas reglas de la Ley de Enjuiciamiento Criminal*. Revista jurídica de Asturias, núm. 39

ARMENTA DEU, T. (2007). *Lecciones de Derecho Procesal Penal*. 3ª ed., Madrid, Barcelona: Marcial Pons

BERNARDO SAN JOSE, A. (2009). *La restricción de los derechos fundamentales en las diligencias de investigación del proceso penal y las exigencias derivadas del principio de proporcionalidad*. Revista del Instituto de Ciencias Jurídicas de Puebla A.C., núm. 24, pp. 7-26

BRAVO SANDOVAL, C. (2021). *El agente encubierto en línea. Principales características, Derecho Comparado, y desafíos que subyacen a su regulación*. Memoria para optar al grado de Licenciado en Ciencias Jurídicas y Sociales. Santiago de Chile, Chile: Universidad de Chile, Facultad de Derecho, Departamento de Ciencias Penales

CASAL, J. M. (2020). *Los Derechos Humanos y sus restricciones*. Bogotá, Colombia: Temis

CLUSA LOPEZ, A. (2019). *El agente encubierto informático*. Trabajo fin de grado. Derecho Procesal Penal. Universidad de Zaragoza

DARAY, Roberto R. *Código Procesal Penal Federal Análisis doctrinal y jurisprudencial*. Tomo 2. Buenos Aires, Argentina: Hammurabi

HERNÁNDEZ SAMPIERI, R., Fernández Collado, C., & Baptista Lucio, P. (2014). *Metodología de la investigación* (6a. ed.). México D.F.: McGraw-Hill

RAMIREZ JARAMILLO, A. D. (2010). *El Agente Encubierto frente a los Derechos Fundamentales a la intimidad y a la no autoincriminación*. Antioquia, Universidad de Antioquia

ROXIN, C. (2000). *La evolución de la política criminal, el derecho penal y el proceso penal*. Traducción Carmen Gómez Rivero y María del Carmen García Cantizano. Valencia, España: Tirant Lo Blanch

Jurisprudencia

Causa FCB 9942/2020/1/CA1. Cámara Federal de Córdoba, Sala "A", Poder Judicial de la Nación

Causa FMP 11434/2023/10/CA7 "Incidente de nulidad". Cámara Federal de Mar del Plata, Poder Judicial de la Nación

Katz v. United States, 389 U.S. 347 (1967). Recuperado de https://supreme.justia.com/cases/federal/us/389/347/

Tribunal Constitucional Español. (s.f.). *Jurisprudencia sobre el control judicial de agentes encubiertos*. Recuperado de https://www.tribunalconstitucional.es

Legislación

Constitución de los Estados Unidos de América. (1787). Enmendada por última vez en 1992. Recuperada de https://www.archives.gov/founding-docs/constitution-transcript.

Decreto Reglamentario 1558/2001 del 29 de noviembre de 2001 de la Ley 25.326 de Protección de Datos Personales

Gobierno de Australia. (2004). *Surveillance Devices Act 2004 (Cth)*. Recuperado de https://www.legislation.gov.au/Details/C2004A01324

Gobierno de Canadá. (1982). *Carta Canadiense de Derechos y Libertades*. Recuperado de https://laws-lois.justice.gc.ca/eng/const/page-15.html

Gobierno de Canadá. (2000). Ley de Protección de Información Personal y Documentos Electrónicos (PIPEDA), S.C. 2000, c. 5. Recuperado de https://laws-lois.justice.gc.ca/eng/acts/P-8.6/

Ley 9.510 del 04 de marzo de 2024 de reforma al Código Procesal Penal de la provincia de Mendoza (Ley 6.730)

Ley 25.326 del 30 de octubre de 2000. Protección de Datos Personales

Ley 27.319 de 2016. *Técnicas Especiales de Investigación.* Boletín Oficial del 22 de noviembre de 2016

Ley de Enjuiciamiento Criminal española. (1882). https://www.boe.es/buscar/act.php?id=BOE-A-1882-6036

Parlamento Europeo y Consejo de la Unión Europea. (2016). *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de Protección de Datos)*. Diario Oficial de la Unión Europea, L 119, 1-88. Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679

Publicaciones periodísticas

Department of Justice (USA). (2017). *AlphaBay, the Largest Online "Dark Market," Shut Down*. https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down

Department of Justice (USA). (2021). *FBI's Encrypted Phone Platform Infiltrated Hundreds of Criminal Syndicates; Result is Massive Worldwide Takedown*. https://www.justice.gov/usao-sdca/pr/fbi-s-encrypted-phone-platform-infiltrated-hundreds-criminal-syndicates-result-massive

RACHMAN, G., & MANDER, B. (2019 10). *Leaderless rebellion: how social media enables global protests*. https://www.ft.com/content/19dc5dfe-f67b-11e9-a79c-bc9acae3b654

ROSEN, K. (2021 2). *Winnipeg police seize $11.5M in assets in major multi-provincial drug bust*. https://winnipeg.ctvnews.ca/winnipeg-police-seize-11-5m-in-assets-in-major-multi-provincial-drug-bust-1.5322297?cache=ztdsfbqaznqc

SIINO, N. (2016 10). *The FBI's "Operation Pacifier" Attempted to Catch Child Pornography Viewers But Courts Inquire Into the Validity of the Search Warrant*. https://sites.suffolk.edu/jhtl/2016/10/29/the-fbis-operation-pacifier-attempted-to-catch-child-pornography-viewers-but-courts-inquire-into-the-validity-of-the-search-warrant/

Unión Internacional de Telecomunicaciones. (2022). *Measuring digital development: Facts and figures 2022*. Recuperado de https://www.itu.int/en/ITU-D/Statistics/Pages/facts

Bibliografía

Doctrina

ERRECABORDE, J. D.; PARADA, R. A. (2018). *Cibercrimen y delitos informáticos: los nuevos tipos penales en la era de internet*. 1a. ed. Buenos Aires, Argentina: Erreius

INSUA, F. S. (2008). *El agente encubierto ¿Peligro o beneficio en estados democráticos?* Santiago de Chile, Chile: Universidad de Chile, Facultad de Derecho, Departamento de Ciencias Penales

LAMARRE, F. (2010). *Agentes Encubiertos y criminalidad organizada: derecho y demagogia*. Revista Lecciones y Ensayos de la Universidad de Buenos Aires, 10(88), 175-195

MATASSI, M. (2022). The Digital Environment. *How We Live, Learn, Work, and Play Now*. InMediaciones de la Comunicación, 17(1), 243-249

MOSCATO DE SANTA MARIA, C. (2000). *El agente encubierto en el Estado de Derecho*. Buenos Aires, Argentina: La Ley

NEIRA, C. *"El arrepentido y el agente encubierto - Reflexiones acerca del Proyecto de ley contra las actividades terroristas"*, L.L. 1997-B, 1431-1435

ORTIZ PRADILLO, J. C., *Vigilancias policiales y utilización de dispositivos de seguimiento*. Reflexiones en torno al Anteproyecto de Ley de Enjuiciamiento Criminal de 2020, Valencia 2022, pp. 834 y 835

RUIZ VADILLO, E. (1993). *Principios generales. Legalidad, Proporcionalidad, etc*. Cuadernos de Derecho Judicial, 29, 11-57

VILLAR FUENTES, I. *El agente encubierto y su especialidad informática: reto legislativo pendiente en un escenario digitalizado (análisis de la figura en el Anteproyecto de Ley Enjuiciamiento Criminal)*. Revista de Estudios Jurídicos y Criminológicos, n.º 6, Universidad de Cádiz, 2022, pp. 197-228

Legislación

Código Penal Argentino

Código Procesal Penal de la Nación

Constitución de la Nación Argentina

Decreto 1412 de la República del Perú del 12/09/2018

Ley 23.054 del 1 de marzo de 1984. Aprobación de la Convención Americana sobre Derechos Humanos

Ley 23.313 del 17 de abril de 1986. Aprobación del Pacto Internacional de Derechos Civiles y Políticos

Ley 23.737 del 21 de septiembre de 1989. Tenencia y Tráfico de Estupefacientes

Ley 24.424 del 7 de diciembre de 1994. Modificación de la Ley de Tenencia y Tráfico de Estupefacientes

Ley 25.632 del 1 de agosto de 2002. Aprobación de la Convención Internacional contra la Delincuencia Organizada Trasnacional

Documentos de Organismos Internacionales

Organización de las Naciones Unidas (2000). Convención contra la delincuencia organizada transnacional y sus protocolos. Recuperado el 14 de Abril de 2023 de http://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-s.pdf

Jurisprudencia

CACrim. y Corr. Fed., Sala I, “Levy, Gustavo R. s/procesamiento” (2007)

CFedCP, Sala II, “Russo, Rodolfo Alejandro s/ recurso de casación” (2009)

CACrim. y Corr. Fed. Cba., Sala A, "Aquiles, Valentín y otro s/Incidente de nulidad” (2022)

Juz. Inst. 27, Sec. 124, Sala IV, causa n° 1484/10 “D., V. s/nulidad” (2010)