Universidad de buenos aires

Facultades de ciencias económicas, ciencias exactas y naturales e ingeniería

Carrera de especialización en seguridad informática

Trabajo final de especialización

“Fundamentación técnica para la creación de un protocolo de buenas prácticas en investigaciones digitales”

Autor: Lic. Agustin Donamaria

Tutor: Mg. Lic. Antonio Maza

Cohorte 2024

Declaración jurada de contenido:

“Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual”

Alumno: Agustin Ignacio Donamaria.

DNI: 35.359.749

Firma:

Resumen

En la era digital actual, donde la información fluye de manera constante y la tecnología desempeña un rol esencial en todos los aspectos de la vida, las investigaciones digitales realizadas por las Fuerzas de Seguridad (en mi caso Prefectura Naval Argentina) y el Poder Judicial, se han convertido en herramientas indispensables para la obtención de datos precisos y relevantes. Sin embargo, el acceso a esta información trae consigo riesgos significativos, especialmente en términos de seguridad y cumplimiento de la legislación vigente.

La creciente incidencia de delitos informáticos, como el robo de identidad, la utilización de ransomware, phishing, la manipulación de datos, estafas virtuales y el crimen organizado, ha transformado el entorno digital en un espacio que exige investigaciones no solo eficientes, sino también éticas, legales y metodológicamente rigurosas. Estos delitos no solo afectan a los usuarios individuales de la tecnología, sino que también amenazan a las empresas, los gobiernos y a toda la sociedad. Ante este contexto, se propone una fundamentación técnica para la creación de un protocolo de buenas prácticas, que se presenta como una necesidad fundamental.

Palabras claves

Investigación, ciberdelitos, delitos asistidos tecnológicamente, fuerzas de seguridad, malware, ransomware, delincuencia, criptoactivos, fuentes digitales abiertas, datos personales, datos sensibles, perfil, red social, vpn, agente encubierto, agente revelador, Tor, agente, isp, dark web, Deep web, entidad simulada.

Índice de contenidos

1) Planteo del problema 6

1.1) Fundamentación del tema elegido 7

1.2) Objetivos del trabajo 9

1.3) Objetivo general 9

1.4) Objetivos específicos 9

1.5) Alcance y limitaciones 10

2) Plan de actividades de una investigación digital 10

3) Legislación 11

3.1) Antecedentes y fundamentos 11

3.2) Aplicación ley 27.319 13

4) Características de los grupos criminales 16

4.1) Cibercrimen como servicio 17

4.2) Principales amenazas en materia de cibercrimen 17

4.3) Ransomware 18

4.4) Crímenes relacionados con abuso sexual infantil 18

4.5) Botnets 18

4.6) Fraudes con medios de pago 19

4.7) Ingeniería social 19

4.8) Cryptojacking 19

4.9) Mayor cantidad de usuarios en la darknet 20

5) Puntos de conexión con la prevención del delito a través de fuentes digitales abiertas. 20

6) Intervención de la investigación criminal 24

7) Agente revelador / encubierto en entornos digitales y la prueba en el proceso. 26

8) Nace un agente 28

9) Interpol y la ciberdelincuencia 31

10) Naciones unidas y la ciberdelincuencia 34

10.1) El cibercrimen es una forma evolutiva de delincuencia transnacional. 34

10.2) ¿Qué es el delito cibernético? 34

10.3) Lucha contra el delito cibernético y los objetivos de desarrollo sostenible 35
11) Antecedentes en nuestro país. 37
11.1) Caso "David nazareno Ávila" 37
11.2) Antecedente: "Manuel Antu Carrera" 39
11.3) Antecedente "agente revelador en caso narco" 41
12) Conclusión 42
13) Bibliografía 44

Índice de ilustraciones

Ilustración 1 Principales amanezas en la Darknet [4] 20
Ilustración 2 Objetivos Interpol [20] 32
Ilustración 3 Efectos Previstos de los objetivos [20] 33
Ilustración 4 Capacidades de Ameripol [20] 34
Ilustración 5 Objetivos desarrollo sostenible UNODC 36
Ilustración 6 Posteo Ministerio de Seguridad Nacional [22] 37
Ilustración 7 Nota Diario La Nación - PNA [23] 38
Ilustración 8 Posteo Ministerio de Seguridad de la Nación – PFA [24] 39
Ilustración 9 Nota Diario Infobae - PFA 40
Ilustración 10 Nota Fiscales.gob.ar [26] 41

1) Planteo del problema

Para el presente trabajo, se requiere establecer las bases para la creación e implementación un protocolo bien estructurado que garantice llevar a cabo investigaciones digitales con un enfoque profesional, meticuloso y responsable.

El mismo debe contribuir a minimizar los riesgos de vulnerar la privacidad de las personas, infringir normativas legales o propagar inadvertidamente información errónea. Utilizar dicho protocolo como una guía clara y detallada para el uso adecuado de herramientas y técnicas, asegurando que los datos recopilados sean precisos, verificables, trazables y obtenidos de manera ética.

Asimismo, debe permitir la realización de investigaciones digitales con el máximo rigor y con estricta adhesión a estándares establecidos, dada la complejidad y evolución constante de los delitos informáticos; así como también prevenir, investigar y mitigar eficazmente las amenazas del ciberespacio a través de un enfoque disciplinado y profesional, con el objetivo de contribuir a la seguridad y la confianza en los entornos digitales.

Un protocolo de estas características puede readecuar antiguas prácticas delictivas a los avances tecnológicos de los últimos años, como el uso de técnicas de ingeniería social mediante medios y servicios electrónicos, la ejecución de delitos complejos y el aprovechamiento del anonimato; también adaptar las estrategias de las agencias investigativas del Estado para abordar sus investigaciones con nuevos enfoques, capacitar a los recursos humanos y actualizar los recursos materiales, con el fin de prevenir, investigar e identificar a los autores.

Por último, una correcta implementación del mismo favorece la superación de desafíos que se presentan debido a la novedad de los medios utilizados, la localización de los autores o de sus conexiones en jurisdicciones extranjeras que dificultan la persecución penal, y las limitaciones tecnológicas que obstaculizan una respuesta efectiva frente a la creciente demanda.

1.1) Fundamentación del tema elegido

En el panorama actual, los delitos informáticos son cada vez más sofisticados y frecuentes.

El phishing, por ejemplo, se ha convertido en una de las formas más comunes de ataque, logrando engañar a usuarios con y sin experiencia en el manejo de sistemas informáticos, logrando que revelen información sensible como contraseñas o detalles bancarios.

El robo de identidad es otro delito en alza, donde los ciberdelincuentes usan la información personal robada para realizar fraudes o suplantar la identidad de una víctima.

El ransomware ha surgido como una amenaza crítica, donde los atacantes secuestran los sistemas de las víctimas, encriptando sus datos y exigiendo un rescate a cambio de su liberación.

Otro fenómeno alarmante es la manipulación de datos, donde se alteran o eliminan informaciones críticas, afectando la integridad de los sistemas y generando graves consecuencias tanto económicas como sociales.

Todos estos delitos no solo representan un riesgo para la seguridad personal y corporativa, sino que también plantean desafíos importantes para la integridad de las investigaciones digitales. Por lo tanto, un protocolo de buenas prácticas no solo sirve como una guía para la recopilación y análisis de datos, sino también como una herramienta para garantizar que estas actividades se realicen de manera que no agraven la situación o comprometan la legalidad y ética de la investigación.

El desarrollo de investigaciones digitales implica la recopilación de grandes volúmenes de información, la cual debe ser gestionada de manera eficiente para evitar errores, asegurar su relevancia y su trazabilidad.

Un protocolo bien definido ayudaría a los investigadores a mantener un enfoque claro y ordenado durante todo el proceso, desde la selección de fuentes hasta la verificación de datos.

Por ejemplo, una práctica clave es la diversificación de fuentes. Confiar en una única fuente puede conducir a sesgos o a la obtención de datos incompletos. Un protocolo robusto establece la necesidad de consultar múltiples fuentes, lo que permite un

análisis más completo y equilibrado. Asimismo, la verificación de la información es crucial para asegurar que los datos recopilados sean precisos y confiables, minimizando el riesgo de basar conclusiones en información errónea o manipulada.

En este sentido, a la situación precitada, se suma la dificultad a la que enfrenta el investigador al momento de resguardar la evidencia digital colectada.

De ésta manera, surgen los siguientes interrogantes:

¿Cuándo debe autorizarse la utilización del Agente Revelador (digital) / agente encubierto (digital)?

¿Cómo debe ser utilizada dicha herramienta?

¿Se cuenta con pautas que regulen y delimiten su actuación?

¿De qué forma debe resguardarse la evidencia colectada por el Agente Revelador / encubierto en entornos digitales para asegurar un proceso transparente?

1.2) Objetivos del trabajo

1.3) Objetivo general

Crear las bases para generar un protocolo o guía de buenas prácticas y establecer normativas que sustenten el intercambio de información sobre ciberdelitos y delitos asistidos tecnológicamente, detallando sus tipos y el uso de herramientas para mitigar de forma efectiva la lucha contra el ciberdelito.

1.4) Objetivos específicos

Analizar las funciones principales del agente encubierto o del agente revelador, Indagar en las leyes relacionadas con la privacidad y la protección de datos, así como los términos de servicio de las plataformas utilizadas.

Comprometerse con la ética y la legalidad como aspecto fundamental de un protocolo de buenas prácticas para evitar cruzar líneas éticas o legales en el desarrollo de investigaciones digitales, actuando con el debido cuidado.

1.5) Alcance y limitaciones

El presente trabajo de investigación abordará desde una perspectiva investigativa, técnica, y legal, con el fin de analizar su impacto en el intercambio de información sobre ciberamenazas.
Las tareas de prevención mediante la exploración de fuentes digitales abiertas con el objeto de detectar conductas ilícitas, principalmente aquellas realizadas a través de redes sociales, presuponen la creación y utilización de un perfil de usuario determinado como así también se realizarán sobre la infraestructura informática y con la utilización de la virtualización como base en el despliegue de los equipos de trabajo, los cuales contarán con la cobertura necesaria.

2) Plan de actividades de una investigación digital

Es importante destacar que, en la investigación de ciberdelitos, no se puede establecer un tiempo fijo para llevar a cabo las acciones necesarias, ya que este depende de la naturaleza y complejidad del delito informático en cuestión. A diferencia de otros tipos de delitos tradicionales, los ciberdelitos presentan diversas características que requieren un enfoque flexible y adaptado a cada caso particular.

El plan de actividades en una investigación de ciberdelitos debe ser meticuloso y dinámico, considerando los siguientes pasos fundamentales:

I. Detección e identificación del ciberdelito.
II. Recopilación de evidencia
III. Determinación del autor del ciberdelito

IV. Cooperación internacional (si hubiera).
V. Informe y presentación de pruebas

3) Legislación

3.1) Antecedentes y fundamentos

La figura en análisis es reciente en nuestro país, fue concebida por la Ley 27.319 [1], publicada en el Boletín Oficial de la República Argentina el 22 de noviembre de 2016.

Asimismo, el objeto de dicha norma de cuyo texto surgen otras herramientas y figuras tales como el agente encubierto, el informante y la entrega vigilada, se basa en "brindar a las fuerzas policiales y de seguridad, al Ministerio Público Fiscal y al Poder Judicial las herramientas y facultades necesarias para ser aplicadas a la investigación, prevención y lucha de los delitos complejo" (Art. 1º).

En lo concerniente a sus antecedentes más próximos, podemos mencionar la figura del Agente Encubierto-prevista por la ley 23.737 "Tenencia y Tráfico de Estupefacientes" (Sanción: 21/IX/1989 - Promulgación: 10/X/1989 - Publicación: B.O. 11/X/1989) al momento de ser modificada por la Ley 24.424, ésta última sancionada el 7 de diciembre de 1994 y promulgada el 2 de enero de 1995, en cuyo Artículo 31 bis (hoy derogado) establecía

> Durante el curso de una investigación y a los efectos de comprobar la comisión de algún delito previsto en esta ley o en el artículo 866 del Código Aduanero, de impedir su consumación, de lograr la individualización o detención de los autores, partícipes o encubridores, o para obtener y asegurar los medios de prueba necesarios, el juez por resolución fundada podrá disponer, si las finalidades de la investigación no pudieran ser logradas de otro modo, que agentes de las fuerzas de seguridad en actividad, actuando en forma encubierta: a) Se introduzcan como integrantes de organizaciones delictivas que tengan entre sus fines la comisión de los delitos previstos en esta ley o en el artículo 866 del Código Aduanero, y b) Participen en la realización de alguno de los hechos previstos en esta ley o en el artículo 866 del Código Aduanero.

Ésta última figura, fue recogida para investigaciones en casos determinados por la citada Ley 27.319 [1].

Técnicas de investigación como la entrega vigilada, la vigilancia electrónica y las operaciones encubiertas, previstas en la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional (Convención de Palermo) [2] y el agente revelador, entre otras, se originan como respuesta a la constante evolución que demuestran las organizaciones criminales, muchas veces aprovechando las nuevas tecnologías de la información y comunicaciones.

No sólo se ha vuelto difícil la identificación de estructuras compuestas por grupos delictivos organizados, entendidos estos como “tres o más personas que exista durante cierto tiempo y que actúe concertadamente con el propósito de cometer uno o más delitos graves o delitos tipificados con arreglo a la presente Convención con miras a obtener, directa o indirectamente, un beneficio económico u otro beneficio de orden material” [2], dada la complejidad que estas de por sí presentan, sino por factores como el anonimato a través del cual se solapan simples personas que cometen en su propio beneficio delitos tales como la distribución de representaciones de imágenes de índole sexual infantil, fraudes y estafas informáticas, daños a sistemas informáticos, denegaciones de servicios a privados y entidades estatales, entre otros.

En base a ello, es que necesariamente las técnicas investigativas deben evolucionar en pos de una eficaz persecución criminal; ante cada nueva conducta que lesione o amenace derechos tutelados de los individuos, deben avanzar proporcionalmente las técnicas que permitan contrarrestarlas.

Una de las cuestiones principales e importantes que surge del debate parlamentario sobre la Ley 27.319, se presentó en términos generales al tratarse el modo en que el funcionario designado para la función de Agente Revelador (en el caso en análisis se vería representado por el agente revelador en entornos digitales), introduce la prueba al proceso. En este caso, ello se torna justificado y relevante toda vez que a la fecha del presente trabajo no existen pautas claras que indiquen cómo hacerlo. Cabe aclarar que acorde se lo tratará más adelante, sí existen protocolos generales de actuación locales y nacionales, particularmente enfocados en el tratamiento de la

evidencia digital, aunque éstos no prevén la especificidad necesaria que se requiere en este caso.

Por ello, resulta fundamental que se establezcan lineamientos que permitan trazar, dar transparencia y dotar de formalidad a las tareas desarrolladas por el Agente Revelador / encubierto en entorno digitales, con base en derechos humanos y participación multidisciplinaria, particularmente de informáticos y abogados enfocados en la investigación criminal a través del ciberespacio.

3.2) Aplicación ley 27.319

Conforme fuera adelantado en el Capítulo que antecede, fue dentro del texto de esta Ley sobre Investigación, Prevención y Lucha de los delitos complejos publicada en noviembre de 2016, donde el legislador introdujo la novedosa figura del Agente Revelador como técnica especial de investigación, limitando su actuación en el tiempo y solo para casos concretos.

Éstos últimos se encuentran previstos en su Artículo 2º, cuyo texto dice

Las siguientes técnicas especiales de investigación serán procedentes en los siguientes casos:

a) Delitos de producción, tráfico, transporte, siembra, almacenamiento y comercialización de estupefacientes, precursores químicos o materias primas para su producción o fabricación previstos en la ley 23.737 o la que en el futuro la reemplace, y la organización y financiación de dichos delitos;

b) Delitos previstos en la sección XII, título I del Código Aduanero;

c) Todos los casos en que sea aplicable el artículo 41 quinquies del Código Penal;

d) Delitos previstos en los artículos 125, 125 bis, 126, 127 y 128 del Código Penal;

e) Delitos previstos en los artículos 142 bis, 142 ter y 170 del Código Penal;

f) Delitos previstos en los artículos 145 bis y ter del Código Penal;

g) Delitos cometidos por asociaciones ilícitas en los términos de los artículos 210 y 210 bis del Código Penal;

h) Delitos previstos en el libro segundo, título XIII del Código Penal.

Asimismo, en el Artículo 5º de dicho plexo normativo, se trata categóricamente la figura del Agente revelador, señalándose que este rol será desarrollado por “todo aquel agente de las fuerzas de seguridad o policiales designado”.

En torno a tal designación y a diferencia de lo que ocurre con la figura del Agente Encubierto en la cual ésta se encuentra a cargo del Ministerio de Seguridad de la Nación, con control judicial, como así también su selección y capacitación, en el caso del funcionario que desarrollará tareas como Agente Revelador, tanto su disposición, designación e instrumentación se encuentran a cargo del Juez, quien admite tal medida de oficio o a pedido del Ministerio Público Fiscal; tal prerrogativa surge del Artículo 6º de la misma norma. Asimismo, cabría tener presente que ello no resulta totalmente discrecional, sino que la decisión de utilizar ésta última figura, debe encontrarse fundada. Al respecto, la norma prevé que:

“La adopción de las disposiciones contenidas en la presente ley deberá estar supeditada a un examen de razonabilidad, con criterio restrictivo, en el que el juez deberá evaluar la imposibilidad de utilizar una medida más idónea para esclarecer los hechos que motivan la investigación o el paradero de los autores, partícipes o encubridores”.

El fin u objetivo del funcionario designado, es el 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”. Ésta última tarea de “recolectar material probatorio”, es quizá para la cual resulte más efectiva la utilización del Agente Revelador en entornos digitales.

Asimismo, la Ley 27.319 [3] tiene una serie de disposiciones comunes a las figuras del agente revelador y del agente encubierto, relacionadas con su actuación y con su protección personal. Así, prevé lo siguiente:

“ARTÍCULO 7º — La información que el agente encubierto y el agente revelador vayan logrando, será puesta de inmediato en conocimiento del juez y del representante del Ministerio Público Fiscal interviniente en la forma que resultare más conveniente para posibilitar el cumplimiento de su tarea y evitar la revelación de su función e identidad.

ARTÍCULO 8º — El agente encubierto y el agente revelador serán convocados al juicio únicamente cuando su testimonio resultare absolutamente imprescindible. Cuando la declaración significare un riesgo para su integridad o la de otras personas, o cuando frustrare una intervención ulterior, se emplearán los recursos técnicos necesarios para impedir que pueda identificarse al declarante por su voz o su rostro. La declaración prestada en estas condiciones no constituirá prueba dirimente para la condena del acusado, y deberá valorarse con especial cautela por el tribunal interviniente.

ARTÍCULO 9º — No será punible el agente encubierto o el agente revelador que, como consecuencia necesaria del desarrollo de la actuación encomendada, se hubiese visto compelido a incurrir en un delito, siempre que éste no implique poner en peligro cierto la vida o la integridad psíquica o física de una persona o la imposición de un grave sufrimiento físico o moral a otro.

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

ARTÍCULO 11. — Ningún integrante de las fuerzas de seguridad o policiales podrá ser obligado a actuar como agente encubierto ni como agente revelador. La negativa a hacerlo no será tenida como antecedente desfavorable para ningún efecto.

ARTÍCULO 12. — Cuando peligre la seguridad de la persona que haya actuado como agente encubierto o agente revelador por haberse develado su verdadera identidad, ésta tendrá derecho a optar entre permanecer activo o pasar a retiro, cualquiera fuese la cantidad de años de servicio que tuviera. En este último caso se le reconocerá un haber de retiro igual al que le corresponda a quien tenga dos (2) grados de escalafón mayor por el que cumpliera su función.

Deberán adoptarse, de ser necesarias, las medidas de protección adecuadas, con los alcances previstos en la legislación aplicable en materia de protección a testigos e imputados.

La adopción de las disposiciones contenidas en la presente ley deberá estar supeditada a un examen de razonabilidad, con criterio restrictivo, en el que el juez deberá evaluar la imposibilidad de utilizar una medida más idónea para esclarecer los hechos que motivan la investigación o el paradero de los autores, partícipes o encubridores".

De lo señalado surge que tanto el Agente Encubierto como el Agente Revelador, se encontrarían a priori en condiciones de actuar en entornos digitales; no obstante ello, teniendo presente la actual redacción de la norma en análisis, particularmente del Artículo 5 del cual surge claramente el campo de actuación del Agente Revelador, como así también las características particulares del primero quien "… se infiltra o introduce en las organizaciones criminales o asociaciones delictivas…" (Art. 3) y precisa de una capacitación especial pues corre serio riesgo su integridad física, para el caso de la investigación a través del ciberespacio resultaría suficiente con la actuación del Agente Revelador con conocimientos en informática y experiencia en el campo de la investigación criminal, que se encuentre en condiciones de rendir cuenta de sus diligencias ante Juez que lo designó.

4) Características de los grupos criminales

SI bien debido a la complejidad de las organizaciones criminales no resulta factible definir este fenómeno, si resulta posible señalar algunas características que las identifican.

- Poseen una estructura jerárquica claramente establecida, con alto grado de adaptabilidad, lo que les permite mantenerse en el tiempo.
- Restringen la selección de sus miembros, quienes deben posees capacidad con alta exigencia profesional.

- Se destacan por el grado de profesionalismo con el que realizan sus actividades, llegando al grado de captar especialistas para determinadas tareas.

- Sus actividades criminales revisten un grado de complejidad elevado y son desarrolladas a nivel internacional.

4.1) Cibercrimen como servicio

En la actualidad, debido a la rentabilidad del modelo de negocio de servicios en Internet los cibercriminales proporcionan soporte para quienes deseen contratarlos, ya sea para introducirse en este mundo y obtener un rédito económico o bien solamente para adquirir algún tipo de producto, como por ejemplo malware diseñado a medida.

Este tipo de actividades se desarrollada por sujetos con un alto grado de experiencia y conocimiento técnico, quienes tienen inclusive cierta reputación que los avala. [4]

4.2) Principales amenazas en materia de cibercrimen

El cibercrimen se ha instaurado como una amenaza latente en la vida que nos rodea y el entorno digital donde desarrollamos nuestras actividades, ya sea como individuos o sociedad, al mismo tiempo que las estadísticas indican que las víctimas se incrementan de forma exponencial.

Durante los últimos periodos se ha visto que la tendencia de actividades cibercriminales ha evolucionado notablemente, expandiéndose hacia diferentes sectores como la salud y el sector financiero.

La sustentabilidad y crecimiento de este tipo de actividades genera un movimiento continuo de las propias organizaciones criminales, las cuales se ven obligadas a expandirse sin restricciones geográficas.

A este fenómeno se suma en contrapartida la alta demanda de profesionales en materia de seguridad de la información, a fin de afrontar este flagelo que muy lejos

está de ser contenido y mucho menos mitigado, mutando constantemente en diferentes tipos de actividades cibercriminales y marcando tendencias.

4.3) Ransomware

A pesar de las múltiples campañas de concienciación llevadas a cabo a nivel global, este tipo de actividades aún se perfila como líder en cuanto a infecciones se refiere.

Estas aplicaciones maliciosas tienen como finalidad infectar dispositivos informáticos, cifrando los archivos del usuario y exigiendo el pago de un rescate, que por lo general se cotiza en criptoactivos como Bitcoin y Monero.

Si bien en sus orígenes este tipo de malware afectaba a usuarios comunes, hoy sus objetivos principales son grandes organizaciones o entidades como pueden ser los hospitales u organismos estatales.

4.4) Crímenes relacionados con abuso sexual infantil

Hoy el anonimato e interconectividad que brinda Internet ha sido aprovechado por delincuentes sexuales, quienes transmiten y comparten material vinculado a abuso sexual infantil.

Dichas actividades suelten utilizar como medios de comunicación servicios de correo electrónico, redes sociales o aplicaciones móviles.

4.5) Botnets

Existen grandes redes conformadas por equipos informáticos infectados, situación por lo general desconocida por su propietario.

Dichas infraestructuras, obedecen a un centro de comando y control, que ante una orden determinada podría ser capaz de realizar una denegación de servicio a un servidor Web, interrumpiendo su operatividad.

Por lo general, este tipo de servicios puede ser rentado por una cantidad de tiempo o volumen de datos determinados.

4.6) Fraudes con medios de pago

Aun cuando las medidas de seguridad en torno a los medios de pago se han robustecido durante los últimos años, continúan los ataques contra las tarjetas de crédito y débito.

Un claro ejemplo es la técnica denominada como skimming, que logra hacerse de la información almacenada en la banda magnética de las tarjetas, permitiendo su posterior clonación.

Por otro lado, técnicas más avanzadas como el jackpotting han logrado vulnerar los sistemas instalados en los cajeros automáticos mediante técnicas de malware que se aprovechan de diferentes vulnerabilidades, ya sea de hardware como de software.

4.7) Ingeniería social

Consiste en manipular a una persona o grupo de personas para obtener un resultado determinado.

Esta técnica es empleada habitualmente para efectuar fraudes como por ejemplo phishing o comprometer un e-mail corporativo, a fin de impersonar a sus legítimos usuarios y autorizar o solicitar operatorias bancarias fraudulentas.

4.8) Cryptojacking

Debido al incremento de costo computacional requerido para la minería de criptoactivos, los ciberdelincuentes han optado por esta novedosa técnica, mediante la que se busca tomar control todo tipo de dispositivos, desde computadoras de

escritorio y equipos portátiles hasta teléfonos inteligentes e incluso servidores web, a fin de utilizar dicho poder de procesamiento.

Esta amenaza emergente, tiene como capacidad permanecer oculto de forma casi imperceptible, salvo por aquellos casos donde el equipo comprometido ve disminuido significativamente su rendimiento.

4.9) Mayor cantidad de usuarios en la darknet

Dado que la complejidad para acceder a esta porción de Internet ha disminuido, la cantidad de personas que visitan la Darkweb se ha visto incrementada.

Si bien muchos de sus usuarios se conectan por curiosidad, otro tanto lo hacen para enmascarar actividades ilegales.

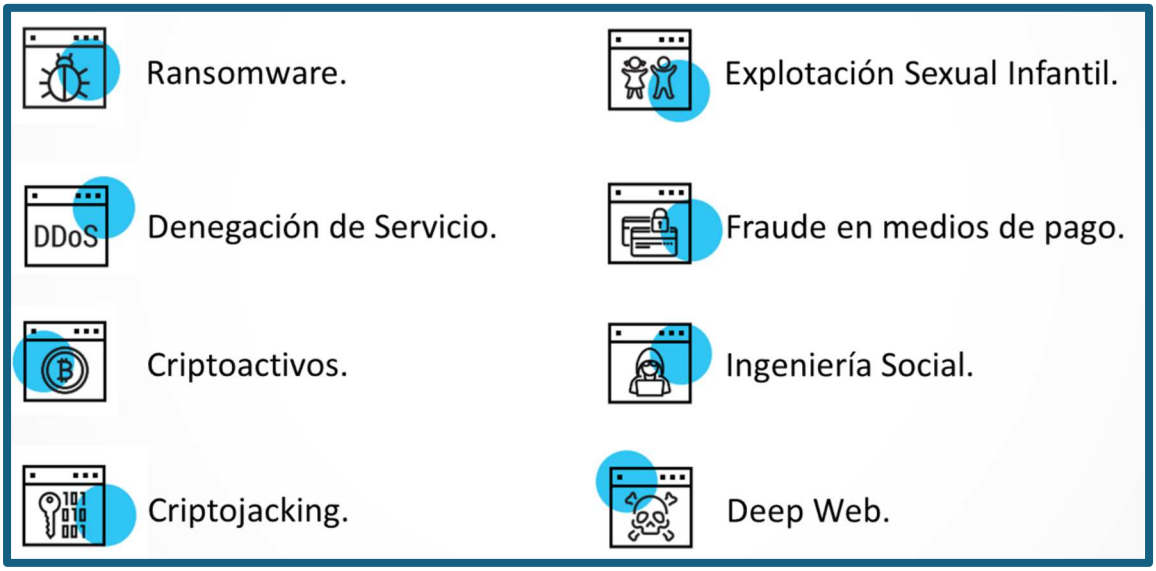


Ilustración 1 Principales amanezas en la Darknet [4]

5) Puntos de conexión con la prevención del delito a través de fuentes digitales abiertas.

De acuerdo con lo previsto por las normas antes mencionadas, la figura del Agente Revelador/ Encubierto resulta ser de carácter excepcional y solo para los casos allí previstos.

Sin perjuicio tales preceptos, deben tenerse en cuenta las particularidades técnicas y el espacio a través del cual aquel desarrolla diligencias investigativas.

En este sentido, no existen dentro de la reglamentación local vigente, lineamientos mínimos que regulen tal actividad con la especificidad que el caso amerita.

De forma reciente y con el aporte de diferentes asociaciones civiles, el Ministerio de Seguridad de la Nación sancionó las resoluciones RESOL-2020-144APN-MSG [5] de fecha 31/05/2020, cuyo foco principal es establecer un marco de actuación para la "prevención policial" del delito con el uso de Fuentes Digitales Abiertas, fijando criterios y principios de actuación para las distintas fuerzas de seguridad. En el caso, cabría tener en cuenta que son también funcionarios de dichas fuerzas de seguridad, quienes a requerimiento del Ministerio Público Fiscal desarrollaran tareas bajo la figura del agente revelador.

A esta parte, es importante resaltar que existe una diferencia sustancial entre el contexto de actuación del funcionario designado como agente revelador y de aquel que lo hace debido a las resoluciones antes mencionadas. Así, mientras el primero se desempeña en el marco de una "investigación en curso" con intervención del Juez y del Ministerio Público Fiscal, el segundo lo hace en la etapa de "prevención" del delito, al constatar conductas presuntamente ilícitas y limitando su actuación a fuentes de información acceso público.

En el caso particular, las actividades de prevención mediante el uso de fuentes digitales abiertas, conocidas corrientemente como ciberpatrullaje [6] también exhiben un carácter excepcional y sólo se mantendrán vigentes y operativas hasta el término del plazo previsto por Ley N° 27.541 [7], ampliada por el Decreto N° DECNU-2020-260-APN-PTE [8], en virtud de la Pandemia declarada por la ORGANIZACIÓN MUNDIAL DE LA SALUD (OMS) en relación con el coronavirus COVID-19.

De forma análoga a lo que sucede con las técnicas especiales de investigación que prevén la figura del Agente Revelador, la prevención policial en el espacio cibernético solo puede realizarse en delitos concretos; a saber:

a) criminalidad vinculada a la comercialización, distribución y transporte de medicamentos apócrifos y de insumos sanitarios críticos;

b) a la venta de presuntos medicamentos comercializados bajo nomenclaturas y referencias al COVID-19 o sus derivaciones nominales, sin aprobación ni certificación de la autoridad competente;

c) a los ataques informáticos a infraestructura crítica -especialmente a hospitales y a centros de salud-;

d) al desarrollo de indicios relativos a los delitos a los que hace referencia el Decreto N° DECNU-2020-260-APN-PTE del 12 de marzo de 2020 y su modificatorio, previstos en los artículos 205, 239 y concordantes del Código Penal;

e) la trata de personas;

f) el tráfico de estupefacientes;

g) el lavado de dinero y terrorismo;

h) conductas que puedan comportar situaciones de acoso y/o violencia por motivos de género, amenaza y/o extorsión de dar publicidad a imágenes no destinadas a la publicación;

i) el grooming;

j) la producción, financiación, ofrecimiento, comercio, publicación, facilitación, divulgación o distribución de imágenes de abuso sexual de niñas, niños y adolescentes.

Una de las cuestiones interesantes que traen aparejadas dichas resoluciones, es que comienzan a sentar bases formales a través de las cuales los agentes de las fuerzas de seguridad rendirán cuenta de su navegación a través del espacio cibernético, permitiendo la trazabilidad de los resultados obtenidos de un modo transparente, cuestión que fue relevante en las inserciones realizadas en el debate de la Ley 27.319 (Período 134 - Reunión 7° - 6° Sesión Ordinaria del 01 de junio de 2016), durante el

cual se planteó en términos generales y entre otras cuestiones, que "…en razón de que el agente revelador solo debe declarar en juicio de manera excepcional no existirá control de las partes ni inmediación del juez…".

Uno de los objetivos del presente trabajo, es exponer la importancia y la necesidad de documentar eficazmente la labor del agente revelador / encubierto en el ciberespacio.

En la actualidad, sin la regulación de técnicas especiales como la analizada, resultaría poco probable lograr que la persecución criminal resulte eficaz a la luz de las múltiples posibilidades de ocultamiento o anonimato tras las cuales operaran no solo las organizaciones criminales, sino también simples individuos con conductas delictivas que actúan aisladamente y en su propio beneficio.

Por ejemplo, luego de incoada una investigación a través de la cual se averigua la venta de estupefacientes a través de alguna red social, supongamos para el caso que sea ésta una de las más conocidas como Facebook o Twitter, el Ministerio Público Fiscal con la colaboración de alguna de las áreas especializadas en delitos informáticos, enfrentaría diversos desafíos. Podríamos decir que en tal investigación deberían al menos, realizarse las siguientes diligencias:

a) verificar si el perfil o el grupo realmente existen;

b) identificarlos, en este caso mediante su ID (éste identifica la cuenta y no puede ser cambiado por el usuario);

c) preservarlo a través del portal web previsto a tal efecto;

d) realizar diligencias, tal vez a través de fuentes digitales abiertas, a los efectos de individualizar elementos que permitan identificar a las personas físicas usuarias del perfil o administradores del grupo;

e) solicitar colaboración a la empresa (en el ejemplo, Facebook Inc.), a los fines de que brinde Información Básica de Suscriptor e IPs de conexión de los mismos; cabría aclarar, que debido a las políticas de privacidad de algunas de las empresas situadas en el extranjero, resulta imprescindible contar con una orden fundada y rubricada por el Juez de la causa, para obtener la información requerida por medios electrónicos; asimismo, ello se encuentra limitado a BSI y registro de conexiones IP, exceptuándose

en todos los casos, información de contenido del usuario, verbigracia, mails y chats, entre otras.

f) Procesar y analizar la eventual respuesta, a fin de proceder de forma análoga con los proveedores de servicios de internet locales –ISP–.

g) Continuar con la investigación en el campo.

Dichas diligencias son básicas dentro del marco investigativo en entornos digitales y no demandarían la utilización de otra técnica más compleja como la utilización del Agente Revelador.

Ahora bien, existen otras causas cada vez más frecuentes con las cuales debe lidiar el Agente Fiscal y en el marco de las cuales sí resultaría oportuna la disposición de un Agente Revelador.

Continuando con el mismo ejemplo relacionado con el tráfico de estupefacientes, el investigador podría encontrarse con un grupo en la red social cuyo administrador haya configurado el ajuste de privacidad más restringido, con el fin de imposibilitar que terceros ajenos a éste obtengan información de las posibles actividades criminales que se desarrollen dentro de la comunidad.

El anonimato de una persona en la web resulta conveniente para su propia seguridad al navegar por el espacio cibernético. No obstante, cuando éste es utilizado para solaparse con fines delictivos, deberían existir herramientas que permitan revelar la verdadera identidad del usuario.

Asimismo, dichas herramientas deberían prever procedimientos claros de actuación que permitan monitorear en todo momento la labor desarrollada por el investigador, construidas sobre los pilares de los derechos humanos fundamentales recogidos por nuestra Carta Magna y garantizando la persecución penal, sin desmedro de éstos.

6) Intervención de la investigación criminal

Dicha tarea debería ser realizada con la intervención de informáticos expertos preferentemente orientados en la investigación criminal, no puedo dejar de señalar que existen a la fecha múltiples técnicas para lograr el anonimato y en lo que interesa para llevar a cabo actividades criminales, tales como la utilización de servicios prestados por empresas ubicadas en el extranjero que permiten el acceso a la red con el uso de VPN; portales web también hosteados en el exterior que permiten por ejemplo la creación de correos temporales, conocidos también como “correos basura”, que se utilizan para establecer contacto con víctimas del delitos, por ejemplo de ransomware entre otros; el conocido navegador TOR (The Onion Route) el cual funciona como VPN pero no solo utilizando un salto entre la IP de origen y la de destino sino cuatro (impactando cada una de ellas en servidores ubicados en países diferentes); portales web que brindan soporte en línea a aquellas personas interesadas en actividades criminales determinadas y extremadamente peligrosas para nuestras niñas, niños y adolescentes, como por ejemplo los que ofrece un conocido – en el ambiente criminal – portal web que “ayuda” a pedófilos a no ser detectados por las autoridades.

No puede soslayarse que la sociedad ha evolucionado a la par de la tecnología y que en la web existen riesgos reales. Cada vez más personas que utilizan servicios digitales, se vuelven posibles víctimas de phishing, estafas, fraudes, daños informáticos, delitos contra la integridad sexual, etc.

La llamada “internet de las cosas” cuya tecnología permite desde el manejo remoto de una aspiradora (que en casos como algunos modelos Roomba de la firma I Robot pueden incluso obtener información de cómo se compone el domicilio por ambiente mediante un escaneo y mapeo del lugar “para desarrollar eficazmente su tarea”), hasta la utilización de vehículos autónomos, también presupone un riesgo que debe ser prevenido por las autoridades. En estos casos, el anonimato del atacante solo podría ser investigado con herramientas como el Agente Revelador / encubierto (digital) “capacitado en informática para actuar en entornos digitales”.

Técnicas especiales como la utilización del Agente Revelador, sumadas a la suscripción de acuerdos de colaboración internacional como el Convenio sobre Ciberdelito del Consejo de Europa aprobado en nuestro país mediante Ley 27.411 [9],

resultan imprescindibles para lograr una persecución penal eficaz y la tutela efectiva de los derechos fundamentales de las personas.

Por lo expuesto, es que resulta esencial que se establezcan lineamientos que permitan trazar y dar transparencia a las tareas desarrolladas por el Agente Revelador en el proceso, ello con independencia del cuerpo al cual pertenezca la persona designada, sea ésta un agente de las fuerzas de seguridad o de la policía judicial, debería encontrarse en la misma condición de rendir cuentas a la vez que se preserve su integridad física.

7) Agente revelador / encubierto en entornos digitales y la prueba en el proceso.

Conforme evoluciona la tecnología, el mundo pareciera volverse más pequeño. Ya no hace falta otear más allá del horizonte pues éste se encuentra a un par de clics. Como fuera referido al iniciar el trabajo, cada vez es mayor la cantidad de cibernautas que utilizan internet a través de diferentes dispositivos electrónicos con el fin de realizar tareas relacionadas con las esferas principales de la vida cotidiana. Dentro de este contexto, dijimos que resultan necesarias normas que regulen técnicas especiales de investigación, que permitan la persecución criminal de quienes que utilicen la tecnología en menoscabo de aquellos.

Técnicas investigativas como la del Agente Revelador / encubierto en entornos digitales, deben prever para ser eficaces, que la persona designada al efecto pueda a través de una metodología determinada y transparente de trabajo, demostrar cómo obtuvo la evidencia digital aportada en el proceso.

Entendiendo que la normativa de forma tradicional no resultaba suficiente para abarcar el plano intangible sobre el cual se desarrolla la evidencia digital y la información electrónica, diferentes reparticiones del país han elaborado guías, protocolos y pautas mínimas de actuación para su tratamiento. No obstante, si bien se ha avanzado mucho en la materia y aquellas se encuentran en permanente evolución puesto que a diario surgen casuísticas novedosas, aún no se han tratado cuestiones relacionadas a la metodología y forma en que el Agente Revelador en entornos digitales, debería ingresar la prueba al proceso. Tampoco se han tratado

adecuadamente temas relacionados con la materialización de la identidad ficticia o perfil de tal figura, lo cual resulta de gran importancia pues en el caso particular ello traería mayor transparencia al proceso. Antes de avanzar en ésta última cuestión, cabría repasar algunas de las normas vigentes en el país relacionadas con la evidencia digital.

En este sentido, de acuerdo con lo previsto por la Resolución PGN N° 756/16 [10], puede definirse la evidencia digital como "…el conjunto de datos e información, relevantes para una investigación, que se encuentra almacenada en o es transmitida por una computadora o dispositivo electrónico…". Asimismo, dada su volatilidad, es "…asimilada a la evidencia de ADN o a las huellas dactilares…" y "…en su estado natural, no nos deja entrever qué información es la que contiene en su interior, sino que resulta ineludible para ello, examinarla a través de instrumentos y procesos forenses específicos...".

Sentado ello, a continuación, se listan algunos de los protocolos a través de los cuales se establecen lineamientos relacionados con el tratamiento de la evidencia digital, incluyendo el caso de la telefonía celular.

a) Protocolo de Pericias Telefónicas de la Provincia de Neuquén – B.O. 3362 - Acuerdo 5024 - 03-07-2013 [11]

b) Protocolo de Actuación del Departamento de Informática Forense de la Provincia de Río Negro – Acordada 5/14 – 30/04/2014 [12]

c) Protocolo de Cadena de Custodia de la Provincia de Provincia de Buenos Aires – Resol. General 889/15- 19/10/2015 [13]

d) Guía de Obtención, Preservación y Tratamiento de Evidencia Digital del Ministerio Público de la Nación - Resolución PGN 756-16 – 2016 [14]

e) Actualización 2020 - Unidad Fiscal Especializada en Ciberdelincuencia (UFECI) y la Dirección General de Cooperación Regional e Internacional (DIGCRI) de la Procuración General de la Nación [15]

f) Protocolo unificado de los Ministerios Públicos de la República Argentina. Guía para el levantamiento y conservación de la evidencia 1ra. edición – (punto 2.5) - abril de 2017 [16]

g) Guía de Cooperación Internacional del Ministerio Público Fiscal De La Nación Argentina - Dirección General de Cooperación Regional e Internacional (DIGCRI) – 2019;

h) Protocolo de actuaciones para informática forense - Ministerio Público Fiscal de la Provincia de Corrientes – 2015 [17]

i) Guía de Ciberdelitos de la Provincia de Provincia de Salta [18]

j) Protocolo General de Actuación N° 234/16 - MINSEG – 07/06/2016 [19]

k) Adhesión de la Provincia de Misiones al PGA 234/16 MINSEG 09/06/2016.

Los preceptos que surgen de la normativa precitada enriquecen la labor realizada por los distintos actores que participan de la investigación criminal, estableciendo de qué forma debe ser tratada la evidencia digital desde su primer contacto con el proceso, generalmente durante la prevención, hasta que ésta es sometida a la pericia pertinente he incluso, su resguardo posterior a dicha etapa. Ello, ha resultado efectivo a la vez que consolida las garantías del debido proceso.

De modo análogo, debería tratarse la forma en que el agente revelador debe ser concebido y dentro de qué marcos debe actuar para documentar la preservación de sus resultados y que éstos puedan ser aprobados incluso desde el punto de vista técnico. En el caso de la evidencia digital, se prevé el uso de una planilla de cadena de custodia; aquí, debería al menos preverse una “hoja de vida” desde el nacimiento mismo del perfil que podría ser incorporada a la actuación judicial (datos personales ficticios, datos de la máquina virtual, etc).

8) Nace un agente

Tomando como base la normativa existente en materia de preservación de la evidencia digital, se estima necesario el tratamiento de un Protocolo General de Actuación que siente los lineamientos relacionados con la creación y utilización del Agente Revelador en entornos digitales. Allí, deberían tratarse al menos las siguientes cuestiones:

Tipo de tareas a realizar por el ARD (Agente Revelador Digital) / AED (Agente Encubierto Digital) , monitoreo o interacción: En el primero de los casos, la utilización de dicha figura resultaría necesaria cuando el investigador deba colectar evidencia digital a través de redes sociales en las cuales el usuario del perfil o el administrador del grupo, han configurado un ajuste de privacidad cerrado; foros de portales web incluidos aquellos existentes en la Deep web, entre otros casos, y solo resulta necesario tal monitoreo para avanzar con la pesquisa. Por ejemplo, luego de ser admitido dentro de un grupo, podría realizarse un monitoreo sobre los posibles usuarios relacionados con la actividad ilícita para posteriormente requerir información básica de suscriptor –BSI– a la red social. Dejando de caso de redes sociales, puesto que éste resulta algo más complejo al momento de ser admitido dentro de la comunicad, para casos de foros web, bastaría sólo con registrarse en el sitio para tener acceso. Por ejemplo, existen sitios dedicados a la venta de estupefacientes; aquellos que brindan soporte técnico a atacantes informáticos; otros que hacen lo propio asesorando a pedófilos sobre cómo mantener el anonimato o encriptar sus dispositivos electrónicos, etc.

Por otra parte, las investigaciones en las que resulte necesaria la interacción del Agente Revelador /Encubierto Digital se presentan como más complejas, puesto que requieren para todos los casos la previsibilidad de cuestiones tales como una “historia de vida” relacionada con el perfil para no ser descubierto, qué imágenes se utilizaran, etc.

Imágenes utilizadas por el Agente Revelador Digital: De acuerdo con el tipo de objetivo encomendado al agente en el marco de la investigación, surgen diferentes interrogantes al momento de materializar la identidad ficticia, en este caso, en el ciberespacio.

Continuando con los ejemplos precitados, debería establecerse qué imágenes pueden ser utilizadas como fotografía del perfil, estado, portada, historias, etc. Cabría tener presente, que, al tratarse de comunidades cerradas, el Agente Revelador /Encubierto Digital será sometido a una “auditoría” antes de ser aceptado y que resulta relativamente sencillo descubrir si detrás de aquel puede encontrarse un agente policial o judicial.

Por ello, podrían utilizarse imágenes de investigaciones prexistentes, cuya información sea reditada en su totalidad (incluidos sus metadatos) por profesionales designados al efecto.

Sin perjuicio de la casuística prevista por el nuevo Código Procesal Penal Federal, cabría tener presente que existen casos abandonados por la actual legislación cuyo delicado objeto se centra en cuestiones relacionadas con la producción y/o distribución de representaciones de menores de dieciocho años dedicados a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, tras los cuales se hallan verdaderas organizaciones criminales. Éstos presentan cuestiones particulares tales como por ejemplo la necesidad de aportar material sexual novedoso para escalar en los privilegios de acceso previstos por la organización criminal y obtener información útil para la pesquisa, en cuyo caso debería procurarse un minucioso y anticipado estudio en torno a su utilización y edición, asegurando que de ningún modo se distinga la real persona detrás de éstas; ello, sin profundizar en cuestiones tales como la generación de imágenes de personas mediante el uso de software basado en IA.

“Vida” del perfil: En el mismo orden de ideas y teniendo presente la multiplicidad de actividades ilícitas que por su complejidad llevarían a la utilización del Agente Revelador / Encubierto Digital, puntualmente para el caso de redes sociales o plataformas afines, debería existir un equipo de profesionales encargados de generar y mantener “con vida” perfiles con las características que cada caso amerite; asimismo, éstos deberían ser ajenos al investigador. Para este caso, al momento de ser designado un nuevo Agente Revelador / Encubierto en entornos digitales, podría preverse algún documento que funcione de forma análoga a la planilla de cadena de custodia prevista y utilizada para la preservación de la evidencia digital, encomendándose en este último, la responsabilidad de continuar con el registro de actividad del perfil hasta que concluyan sus tareas y deba informar al Juez acerca de los resultados obtenidos en la causa.

Algunos aspectos técnicos: Con el objeto de evitar cualquier tipo de trasgresión de las garantías del debido proceso, relacionadas con el tipo de técnica investigativa adoptada y con el modo en que la evidencia digital utilizada como elemento de prueba es introducida al proceso, deben preverse procedimientos técnicos claros en torno a

su tratamiento que permitan su posterior auditoría; los siguientes aspectos son solo algunos de ellos:

a) Entorno a utilizar por el Agente Revelador Digital (Ejemplo, máquinas virtuales y servidores seguros en las que sean alojadas);

b) Método utilizado para enmascaramiento (Ejemplo, VPN, Agente de usuario/User Agent, uso de tecnologías Do Not Track (DNT);

c) Modo de preservación de la evidencia digital colectada por el Agente Revelador Digital (Ejemplo, id y cálculos de hash sobre la máquina virtual);

9) Interpol y la ciberdelincuencia

La Estrategia Mundial de INTERPOL de Lucha contra la Ciberdelincuencia (en adelante, la Estrategia) presenta el plan para apoyar a sus 195 países miembros en la lucha contra la ciberdelincuencia, de acuerdo con el Marco Estratégico de INTERPOL para el periodo 2022-2025 [20]

Ilustración 2 Objetivos Interpol [20]

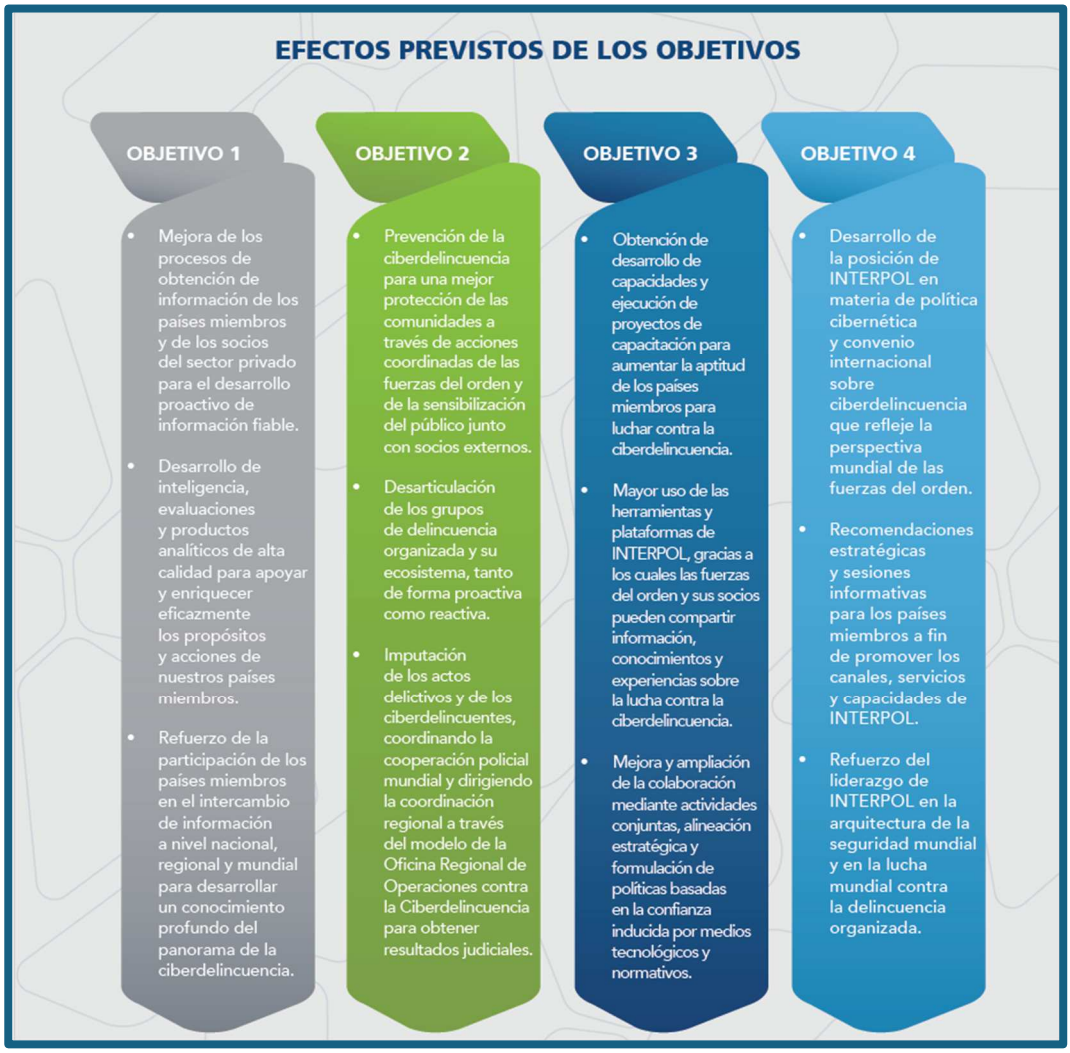


Ilustración 3 Efectos Previstos de los objetivos [20]

Ilustración 4 Capacidades de Ameripol [20]

10) Naciones unidas y la ciberdelincuencia

10.1) El cibercrimen es una forma evolutiva de delincuencia transnacional.

La naturaleza compleja del crimen como uno que tiene lugar en el ámbito sin fronteras del ciberespacio se ve agravada por la creciente participación de los grupos del crimen organizado. Los perpetradores del delito cibernético y sus víctimas pueden ubicarse en diferentes regiones, y sus efectos pueden extenderse a través de las sociedades de todo el mundo, destacando la necesidad de montar una respuesta urgente, dinámica e internacional.

10.2) ¿Qué es el delito cibernético?

No existe una definición internacional de cibercrimen o ciberataques. Los delitos generalmente se agrupan en torno a las siguientes categorías:

Delitos contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos;

- Delitos relacionados con la informática;

- Delitos relacionados con el contenido;
- Delitos relacionados con infracciones de derechos de autor y derechos conexos.

En términos generales, el delito cibernético puede describirse como delitos ciberdependientes, delitos cibernéticos habilitados y, como un tipo específico de delito, explotación y abuso sexual infantil en línea.

- La delincuencia ciberdependiente requiere una infraestructura de tecnología de la información y las comunicaciones y, a menudo, se caracteriza por la creación, difusión y despliegue de malware, ransomware, ataques a infraestructuras nacionales críticas (por ejemplo, la toma de control cibernético de una central eléctrica por parte de un grupo del crimen organizado) y desconectar un sitio web sobrecargándolo con datos (un ataque DDOS).
- El crimen habilitado para el ciberespacio es el que puede ocurrir en el mundo fuera de línea, pero también puede ser facilitado por la tecnología de la información y las comunicaciones. Esto generalmente incluye fraudes en línea, compras de drogas en línea y lavado de dinero en línea.
- La explotación y el abuso sexual infantil incluyen el abuso en Internet claro, los foros de darknet y, cada vez más, la explotación de imágenes autocreadas a través de la extorsión, conocida como "sextorsión". No usamos el término "pornografía infantil", ya que esto crea un juicio de valor sobre los niños inocentes.

10.3) Lucha contra el delito cibernético y los objetivos de desarrollo sostenible

Si bien no existe un Objetivo de Desarrollo Sostenible específico para abordar la ciberdelincuencia, puede considerarse un obstáculo para alcanzar una serie de objetivos, como los del Objetivo 16, que se relacionan con la violencia y otras formas de delincuencia, como la corrupción y el tráfico de armas (Objetivos 16.1, 16.4, 16.5). [21]

Además, algunas actividades delictivas pueden facilitarse mediante la tecnología de la información y las comunicaciones, como el reclutamiento de víctimas de la trata de personas o la explotación sexual de la mujer, que caracterizaría una forma de violencia contra la mujer.

Al elegir tener el delito cibernético como un problema Modelo de las Naciones Unidas, los participantes pueden:

- Obtener más conocimiento sobre los diferentes fenómenos relacionados con el delito cibernético, como los tipos de delitos dependientes, habilitados y específicos;
- Aumentar su comprensión de los esfuerzos de los Estados miembros para abordar la ciberdelincuencia en foros intergubernamentales;
- Aumentar su conocimiento de las mejores prácticas y las formas en que los Estados miembros y la sociedad pueden cooperar para hacer frente a la ciberdelincuencia. [21]

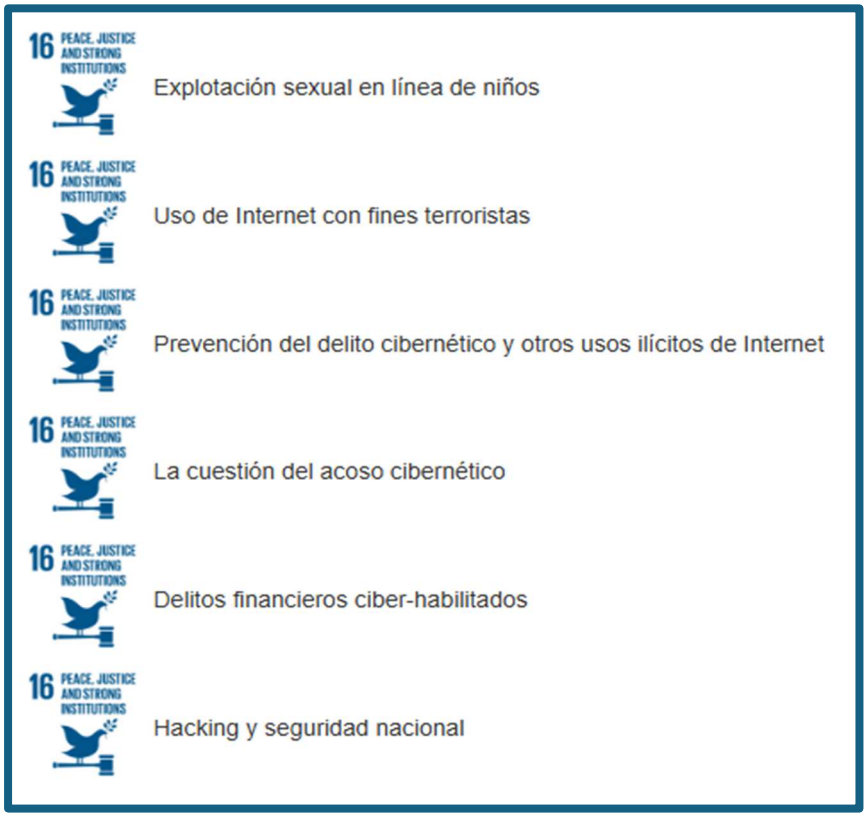


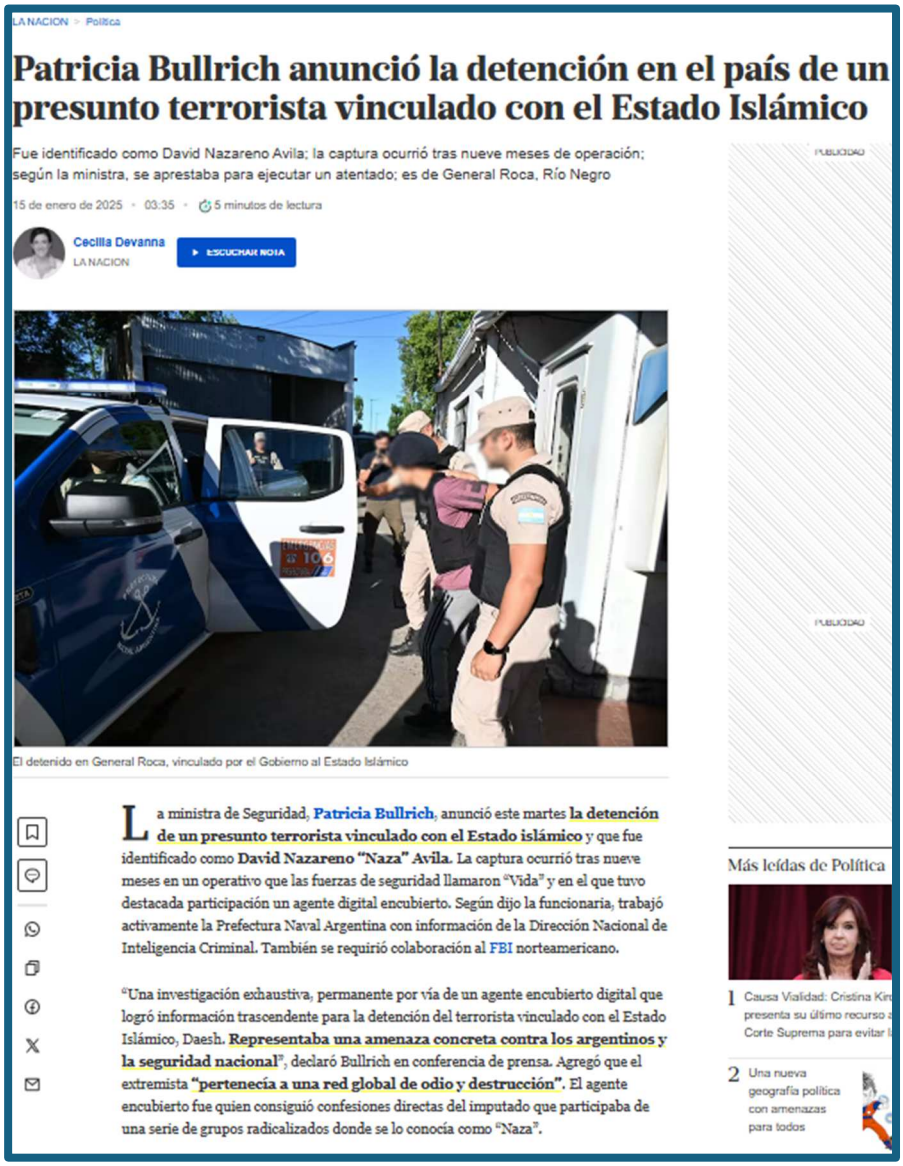
Ilustración 5 Objetivos desarrollo sostenible UNODC

11) Antecedentes en nuestro país.

11.1) Caso “David nazareno Ávila”

En enero de 2025, las fuerzas de seguridad detuvieron en la ciudad de General Roca, provincia de Río Negro, a David Nazareno Ávila, acusado de mantener presuntos vínculos con el grupo terrorista Estado Islámico. La investigación, que se extendió durante nueve meses y contó con la colaboración del FBI, reveló que Ávila se dedicaba a difundir propaganda extremista y a reclutar personas a través de redes sociales. Un “agente encubierto digital” desempeñó un papel clave en el seguimiento de sus actividades y en la recolección de pruebas que permitieron concretar su arresto. [22] [23]

Ilustración 6 Posteo Ministerio de Seguridad Nacional [22]



LA NACION » Política

Patricia Bullrich anunció la detención en el país de un presunto terrorista vinculado con el Estado Islámico

Fue identificado como David Nazareno Avila; la captura ocurrió tras nueve meses de operación; según la ministra, se aprestaba para ejecutar un atentado; es de General Roca, Río Negro

15 de enero de 2025 · 03:35 · 5 minutos de lectura

Cecilia Devanna
LA NACION

ESCUCHAR NOTA

El detenido en General Roca, vinculado por el Gobierno al Estado Islámico

La ministra de Seguridad, **Patricia Bullrich**, anunció este martes **la detención de un presunto terrorista vinculado con el Estado islámico** y que fue identificado como **David Nazareno "Naza" Avila.** La captura ocurrió tras nueve meses en un operativo que las fuerzas de seguridad llamaron "Vida" y en el que tuvo destacada participación un agente digital encubierto. Según dijo la funcionaria, trabajó activamente la Prefectura Naval Argentina con información de la Dirección Nacional de Inteligencia Criminal. También se requirió colaboración al FBI norteamericano.

"Una investigación exhaustiva, permanente por vía de un agente encubierto digital que logró información trascendente para la detención del terrorista vinculado con el Estado Islámico, Daesh. **Representaba una amenaza concreta contra los argentinos y la seguridad nacional**", declaró Bullrich en conferencia de prensa. Agregó que el extremista **"pertenecía a una red global de odio y destrucción".** El agente encubierto fue quien consiguió confesiones directas del imputado que participaba de una serie de grupos radicalizados donde se lo conocía como "Naza".

PUBLICIDAD

PUBLICIDAD

Más leídas de Política

1 Causa Vialidad: Cristina Kir... presenta su último recurso ... Corte Suprema para evitar l...

2 Una nueva geografía política con amenazas para todos

Ilustración 7 Nota Diario La Nación - PNA [23]

11.2) Antecedente: “Manuel Antu Carrera”

Esta noticia informa sobre la detención de Manuel Antu Carrera, un ciudadano argentino oriundo de Río Negro, por presuntos vínculos con la violencia extremista en Siria e Irak, según registros de Interpol. La detención se llevó a cabo en Corrientes, Argentina, y está relacionada con una causa en la Justicia federal argentina. [24] [25]

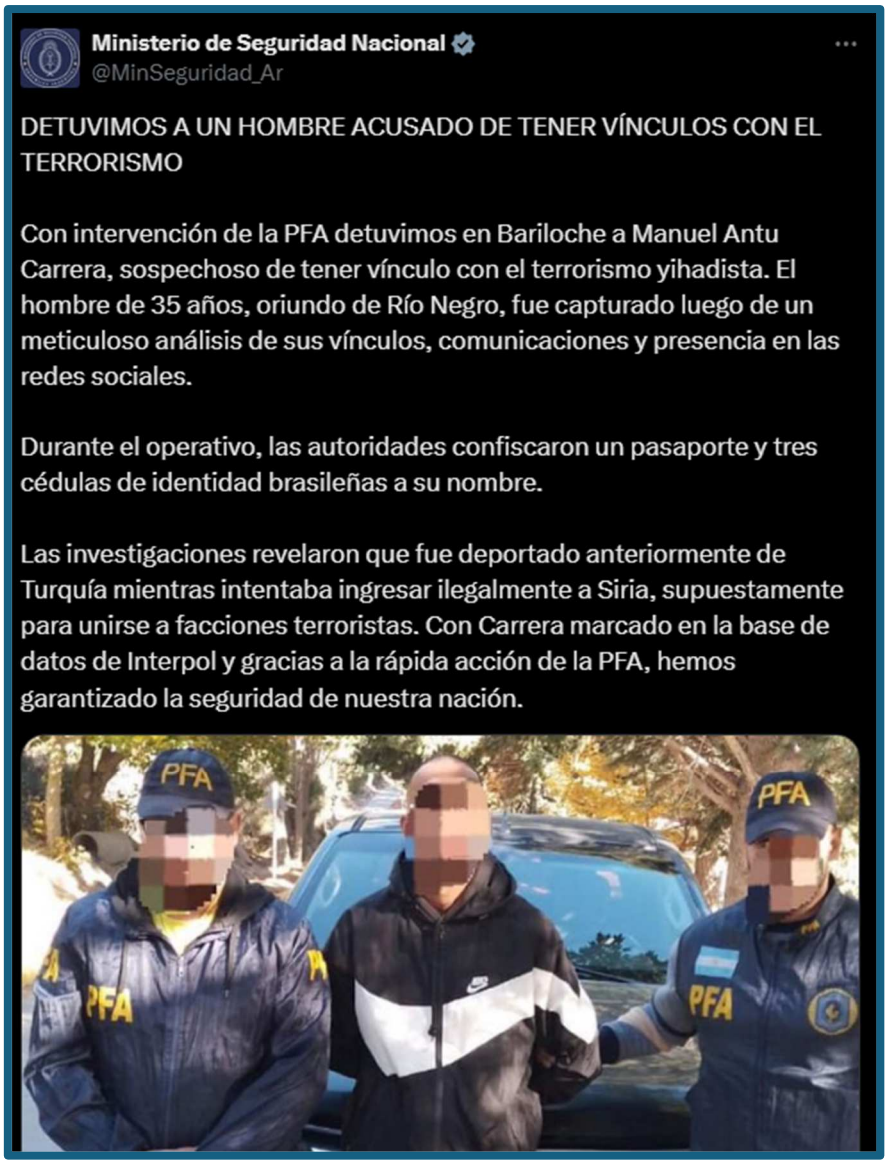


Ilustración 8 Posteo Ministerio de Seguridad de la Nación – PFA [24]

infobae

Últimas Noticias Política Economía Dólar hoy Deportes Sociedad Policiales

CRIMEN Y JUSTICIA ›

Detuvieron a un misterioso argentino en Corrientes sospechado de vínculos con el terrorismo en Oriente Medio

Oriundo de Río Negro, Manuel Antu Carrera tiene un expediente a su nombre por presuntos vínculos con la violencia extremista en Siria e Irak en los archivos de Interpol. También está involucrado en una causa en la Justicia federal argentina

17 Abr, 2024 02:30 p.m. AR

Guardar

PUBLICIDAD

Antu Carrera tras ser detenido

El 11 de abril último, **Manuel Antu Carrera** -de 35 años, oriundo de General Roca, Rio Negro- **arribó al país desde Brasil por el paso fronterizo de Paso de los Libres**, provincia de Corrientes. La Dirección Nacional de Migraciones alertó que pesaba sobre Antu Carrera una alerta a requerimiento de la Justicia federal de Lomas de Zamora, por una causa de 2017.

PUBLICIDAD

Ese no era el único problema: **el área local de Interpol, a cargo de la Policía Federal, reveló que fue deportado desde Turquía el 29 de diciembre de ese mismo año**, ya que se encuentra catalogado como un supuesto combatiente terrorista, con presunta relación con grupos radicales en Siria e Irak, un **dato que fue confirmado por Rick Hernández, agregado jurídico del FBI en Argentina**, de histórica relación con las fuerzas de seguridad nacionales y sus autoridades políticas.

"En la base de datos I-24/7 de la Secretaría General de Interpol se encuentra registrado con **anotación "TSC" por "delito relacionado con el terrorismo"** por Interpol Estados

Ilustración 9 Nota Diario Infobae - PFA

11.3) Antecedente “agente revelador en caso narco”

Esta noticia informa que la Cámara Federal de Apelaciones de Mar del Plata rechazó los pedidos de nulidad presentados por las defensas en una causa donde se investiga a cinco personas por comercialización de estupefacientes a través de redes sociales. Las defensas habían objetado el uso de un “agente revelador” en la investigación. La resolución de los jueces Alejandro Tazza y Eduardo Jiménez se alineó con lo dictaminado por el fiscal general ante la Cámara, Daniel Adler. La causa se inició a partir de una nota de la División Unidad Operativa Federal de Mar del Plata de la PFA, que brindó información sobre publicaciones en redes sociales que evidenciaban posibles delitos relacionados con la ley 23.737. La investigación fue derivada a la Fiscalía Federal N.º 2, a cargo de Santiago Eyherabide, quien solicitó la designación de un agente revelador según la ley 27.319, lo que permitió identificar a los imputados y las maniobras de comercio investigadas. Los camaristas señalaron que, debido al uso de redes sociales y comunicaciones encriptadas para la venta de estupefacientes, la intervención del agente revelador fue adecuada y proporcional, especialmente considerando que el delito estaba en curso de ejecución. [26]

Fiscales.gob.ar

01 de abril de 2025 | Las Noticias del Ministerio Público Fiscal

En línea con lo dictaminado por el Ministerio Público Fiscal

Mar del Plata: confirmaron el uso de un “agente revelador” en una causa por narcocriminalidad

5.04.2024 en Fiscalías, Narcocriminalidad

La decisión de la Cámara Federal de Apelaciones de Mar del Plata se efectuó en el marco de una investigación que derivó en veinte allanamientos por comercialización de estupefacientes a través de redes sociales y la detención de cinco personas, en agosto de 2023.

EN ESTA NOTA:

Tags

Agente Revelador | comercializacion-de-estupefacientes | fiscal federal Santiago Eyherabide | fiscal general Daniel Adler

Notas relacionadas

Mar del Plata: realizaron veinte allanamientos por comercialización de estupefacientes a través de redes sociales y detuvieron a cinco personas

18.08.2023 en Fiscalías, Narcocriminalidad

La Cámara Federal de Apelaciones de Mar del Plata rechazó los pedidos de nulidad presentados por las defensas en una causa donde se investiga a cinco personas por comercialización de estupefacientes a través de redes sociales. En que sus planteos, habían objetado el uso de un “agente revelador” para nutrir la investigación. La resolución de los jueces Alejandro Tazza y Eduardo Jiménez se dio en línea con lo dictaminado por el fiscal general ante la Cámara, Daniel Adler.

La causa se había iniciado a partir de una nota elevada por la División Unidad Operativa Federal de Mar del Plata de la PFA, que brindó información sobre la existencia de distintas publicaciones en redes sociales que demostraban la posible comisión de delitos en infracción a la ley 23.737, a través de grupos de WhatsApp.

La investigación fue derivada a la Fiscalía Federal N°2, a cargo de Santiago Eyherabide, y entre las variadas medidas de prueba solicitadas, se requirió -y dispuso- la designación de un agente revelador en los términos de la ley 27.319, que permitió conocer la identidad de los imputados y las maniobras de comercio investigadas.

Tras esto, las defensas cuestionaron la implementación de un agente revelador. En su fallo, los camaristas indicaron: "el avance tecnológico, los medios digitales y la virtualidad han hecho mutar los medios de comisión del delito, por lo tanto las fuerzas preventoras deben actualizar constantemente sus medios y acudir en determinados casos a estas herramientas en espacios virtuales a fin de procurar un resultado satisfactorio frente al flagelo que importa el crimen organizado".

Ilustración 10 Nota Fiscales.gob.ar [26]

12) Conclusión

A partir de los expuesto, se ha intentado ofrecer una perspectiva crítica y actualizada sobre el fenómeno creciente de la criminalidad en entornos digitales, fenómeno que avanza de forma transversal e indiscriminada, afectando tanto a individuos como a instituciones, sin importar el grado de conocimiento técnico ni la actividad desplegada en el ciberespacio. En este nuevo escenario, donde el delito se desplaza con fluidez por fronteras digitales, se impone una urgente reconfiguración de las herramientas investigativas y los marcos normativos que rigen el accionar del Estado.

Uno de los debates más relevantes en este proceso de modernización legislativa y operativa es la incorporación formal de la figura del Agente Revelador o Encubierto en Entornos Digitales como técnica especial de investigación autónoma. Esta figura, ya contemplada en la Ley N.º 27.319 para delitos complejos, adquiere un carácter estratégico en el plano digital dada la facilidad con que los agresores ocultan su identidad, emplean canales cifrados y operan desde jurisdicciones extranjeras. Su implementación exige una regulación específica que contemple la creación de identidades simuladas, el uso controlado de recursos tecnológicos, y un estricto control judicial y fiscal, para evitar vulneraciones de derechos fundamentales.

La importancia de actuar conforme a lineamientos claros y verificables ha sido reconocida por el propio Ministerio de Seguridad de la Nación mediante la Resolución N.º 234/2016, que aprueba el Protocolo General de Actuación para las Fuerzas Policiales y de Seguridad en la investigación y proceso de recolección de pruebas en Ciberdelitos. Esta norma obliga a las fuerzas federales —Gendarmería Nacional, Prefectura Naval, Policía Federal Argentina y Policía de Seguridad Aeroportuaria— a adecuar sus intervenciones a criterios técnicos, jurídicos y procedimentales que garanticen la trazabilidad y legalidad de la evidencia digital.

Sin embargo, estas iniciativas aún enfrentan numerosas problemáticas estructurales que dificultan el éxito de las investigaciones en materia de ciberdelitos:

- Una legislación dispersa y desactualizada, con vacíos legales frente a nuevas modalidades delictivas que utilizan las organizaciones criminales, tales como el ransomware, el phishing o los delitos contra la privacidad en redes sociales.

- Falta de capacitación específica en delitos informáticos entre operadores judiciales, fuerzas de seguridad y peritos.
- Déficit en infraestructura tecnológica, especialmente en provincias del interior del país, lo que impide realizar pericias complejas en tiempo útil.
- Dificultades para la cooperación internacional, tanto en la obtención de datos como en la ejecución de medidas urgentes con proveedores de servicios digitales extranjeros.
- Ausencia de una red nacional integral de ciberdelito, que coordine de forma efectiva a nivel federal y provincial.

Superar estos obstáculos exige una estrategia estatal integral y sostenida, que incluya inversión, formación técnica, marcos normativos modernos y un enfoque interinstitucional. La articulación entre el Poder Judicial, el Ministerio Público Fiscal y las fuerzas federales es fundamental para garantizar una respuesta eficaz frente a los desafíos del delito digital en el siglo XXI

13) Bibliografía

[1] Ministerio de Justicia y Derechos Humanos de la Nación. (2016). Ley 27.319 - Prevención e investigación de delitos complejos. InfoLEG. http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=268004

[2] Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional. (2000). Protocolo de Palermo. Organización de los Estados Americanos. https://www.oas.org/csh/spanish/documentos/Convención%20de%20Palermo%20_ESP.pdf

[3] Boletín Oficial de la República Argentina. (2016, 22 de noviembre). Ley 27.319 - Delitos complejos. https://www.boletinoficial.gob.ar/detalleAviso/primera/154375/20161122?busqueda=1

[4] Maza, A. J. (2019). *Normalización de la práctica forense: Una mirada hacia un sistema de gestión de evidencia digital* (Trabajo final de especialización, Universidad Tecnológica Nacional). Tutor: H. Pagola. Cohorte 2017.

[5] Ministerio de Seguridad de la Nación. (2020, 2 de junio). Resolución 144/2020. Boletín Oficial de la República Argentina. https://www.boletinoficial.gob.ar/detalleAviso/primera/230060/20200602

[6] Ministerio de Seguridad de la Nación. (2024, 28 de mayo). Resolución 428/2024. Boletín Oficial de la República Argentina. https://www.boletinoficial.gob.ar/detalleAviso/primera/308291/20240528

[7] Congreso de la Nación Argentina. (2019, 23 de diciembre). Ley N.º 27.541: Ley de Solidaridad Social y Reactivación Productiva en el Marco de la Emergencia Pública. Boletín Oficial de la República Argentina. https://www.boletinoficial.gob.ar/detalleAviso/primera/5217929/20191223?suplemento=1

[8] Poder Ejecutivo Nacional. (2020, 12 de marzo). Decreto de Necesidad y Urgencia N.º 260/2020: Emergencia Sanitaria por Coronavirus (COVID-19). Boletín Oficial de

la República Argentina. https://www.boletinoficial.gob.ar/detalleAviso/primera/5217883/20200312?busqueda=1&suplemento=1

[9] Congreso de la Nación Argentina. (2017, 15 de diciembre). Ley N.º 27.411: Aprobación del Convenio sobre Ciberdelito del Consejo de Europa. Boletín Oficial de la República Argentina. https://www.boletinoficial.gob.ar/detalleAviso/primera/176168/20171215

[10] Procuración General de la Nación. (2016, 31 de marzo). Resolución PGN N.º 756/2016: Guía de obtención, preservación y tratamiento de evidencia digital. Ministerio Público Fiscal de la Nación. https://www.fiscales.gob.ar/wp-content/uploads/2016/04/PGN-0756-2016-001.pdf

[11] Procuración General de la Nación. (2016, 31 de marzo). Resolución PGN N.º 756/2016: Guía de obtención, preservación y tratamiento de evidencia digital. Ministerio Público Fiscal de la Nación. https://www.fiscales.gob.ar/wp-content/uploads/2016/04/PGN-0756-2016-001.pdf

[12] Superior Tribunal de Justicia de la Provincia de Río Negro. (2014, 30 de abril). Acordada N.º 5/2014: Protocolo de Actuación del Departamento de Informática Forense: Procedimientos Internos y Guías Operativas. Boletín Oficial de la Provincia de Río Negro.

[13] Procuración General de la Suprema Corte de Justicia de la Provincia de Buenos Aires. (2015, 19 de octubre). Resolución General N.º 889/2015: Protocolo de Cadena de Custodia. Ministerio Público de la Provincia de Buenos Aires. https://www.mpba.gov.ar/files/documents/889-15.pdf

[14] Procuración General de la Nación. (2016, 31 de marzo). Resolución PGN N.º 756/2016: Guía de obtención, preservación y tratamiento de evidencia digital. Ministerio Público Fiscal de la Nación. https://www.mpf.gob.ar/ufeci/resoluciones/

[15] Unidad Fiscal Especializada en Ciberdelincuencia & Dirección General de Cooperación Regional e Internacional. (2020). Guía de Buenas Prácticas para Obtener Evidencia Electrónica en el Extranjero. Ministerio Público Fiscal de la Nación. https://www.mpf.gob.ar/ufeci/files/2021/07/UFECI-2020-Gui%CC%81a-de-Evidencia-Digital.pdf

[16] Consejo Federal de Procuradores, Fiscales y Defensores Generales de la República Argentina. (2017, abril). Protocolo unificado de los Ministerios Públicos de la República Argentina: Guía para el levantamiento y conservación de la evidencia (1ra. ed., punto 2.5). https://www.fiscales.gob.ar/wp-content/uploads/2017/04/Protocolo-Unificado-Levantamiento-Conservacion-Evidencia.pdf

[17] Ministerio Público Fiscal de la Provincia de Corrientes. (2015). Protocolo de actuaciones para informática forense. https://www.mpfcorrientes.gov.ar/documentos/Protocolo_Informática_Forense_2015.pdf

[18] Poder Judicial de la Provincia de Salta. (2017). Guía de Ciberdelitos. https://www.justiciasalta.gov.ar/es/guia-ciberdelito

[19] Ministerio de Seguridad de la Nación. (2016, 7 de junio). Resolución N.º 234/2016: Protocolo General de Actuación para las Fuerzas Policiales y de Seguridad en la Investigación y Proceso de Recolección de Pruebas en Ciberdelitos. https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-234-2016-262787

[20] INTERPOL. (2022). Estrategia Mundial de INTERPOL de Lucha contra la Ciberdelincuencia 2022–2025. https://www.interpol.int/es/content/download/19846/file/Cybercrime%20Global%20Strategy_ES.PDF

[21] United Nations Office on Drugs and Crime. (s.f.). *Cybercrime*. https://www.unodc.org/e4j/en/mun/crime-prevention/cybercrime.html

[22] Ministerio de Seguridad [@MinSeguridad_Ar]. (2025, 14 de enero). Detención de un terrorista yihadista en Río Negro. [Tweet]. X. https://x.com/MinSeguridad_Ar/status/1879245414198624725Urgente24

[23] Devanna, C. (2025, 15 de enero). Patricia Bullrich anunció la detención en el país de un presunto terrorista vinculado con el Estado Islámico. La Nación. https://www.lanacion.com.ar/politica/patricia-bullrich-anuncio-la-detencion-en-el-pais-de-un-terrorista-vinculado-con-estado-islamico-nid14012025

[24] Ministerio de Seguridad [@MinSeguridad_Ar]. (2025, 18 de abril). Capacitación para personal de inteligencia criminal en el uso de herramientas tecnológicas para investigaciones complejas. [Tweet]. X. https://x.com/MinSeguridad_Ar/status/1781079936071041264

[25] Infobae. (2024, 17 de abril). Detuvieron a un misterioso argentino en Corrientes sospechado de vínculos con el terrorismo en Oriente Medio. https://www.infobae.com/sociedad/policiales/2024/04/17/detuvieron-a-un-misterioso-argentino-en-corrientes-sospechado-de-terrorismo-en-oriente-medio/

[26] Fiscales.gob.ar. (2024, 5 de abril). Mar del Plata: confirmaron el uso de un “agente revelador” en una causa por narcocriminalidad. https://www.fiscales.gob.ar/narcocriminalidad/mar-del-plata-confirmaron-el-uso-de-un-agente-revelador-en-una-causa-por-narcocriminalidad/