Artículos

Revista Pensamiento Penal
Sección Medios digitales y delitos informáticos
Vol. 2, núm. 4 – 2025, págs. 1–15
ISSN: 1853 – 4554
DOI: https://doi.org/10.64178/wev12245

El agente digital encubierto y el acceso transfronterizo de datos

Julia M. Torrez[1]

Resumen

Este trabajo explora el uso de nuevas tecnologías por parte de organizaciones criminales y el impacto de los avances tecnológicos en la labor de las fuerzas de seguridad para prevenir y castigar delitos graves como el tráfico de drogas, armas, la trata de personas, la pedofilia y el terrorismo. Se introduce el concepto de agente digital encubierto, una figura que permite a los investigadores infiltrarse en redes criminales en el ámbito digital, analizando sus implicancias legales y éticas. El documento examina la operación *EncroChat* y *Trojan Shield*, que expusieron cómo las fuerzas de seguridad desarticularon redes criminales transnacionales mediante la infiltración de dispositivos de comunicación encriptados. Se aborda la problemática del acceso transfronterizo de datos, destacando la cooperación internacional necesaria para combatir delitos en el ciberespacio y el marco normativo que lo respalda, como el *convenio de Budapest*. Finalmente, se discuten las implicancias del agente encubierto digital en la legislación argentina, señalando su regulación en la provincia de Mendoza.

Sumario

Palabras clave

convenio de Budapest – agente digital encubierto – cibercrimen – crimen organizado transnacional – bitcoin

[1] Abogada (Universidad Nacional del Litoral); Diploma de Experto en ciberdelincuencia y tecnologías aplicadas a la investigación (Universidad Austral); maestrando en Derecho penal (Universidad de Palermo); abogada litigante matrícula del Colegio de Abogados de Rosario L° XXXVI-F° 543; jefa Sucursal Rosario Norte de la Empresa Provincial de la Energía de Santa Fe. Correo electrónico: jutorrez8@gmail.com

1. Contexto

En los últimos veinticinco años, la evolución de las tecnologías informáticas de comunicación, en particular el desarrollo de internet ha traído aparejado un problema grave para los investigadores penales y por tanto a los Estados para lograr prevenir y eventualmente castigar delitos, especialmente aquellos graves tales como el tráfico y comercialización de estupefacientes, la trata de personas, la compra venta de armas, la pedofilia y el terrorismo.

Por lo cual el viejo adagio popular que reza «el crimen siempre va un paso adelante de la ley», se hace más real que nunca. Años atrás era posible realizar envíos de droga y comunicar a sus receptores el día, lugar y hora de llegada de los mismos, utilizando las líneas telefónicas públicas o teléfonos celulares prepagos desechables («*burners*») sin que dichas llamadas pudieran ser rastreadas o intervenidas por la policía. La misma metodología se utilizaba para traficar armas, personas y coordinar la ejecución de actos terroristas.

Sin embargo, con el correr del tiempo y la evolución de la tecnología informática esto permitió a los investigadores comenzar a acceder a esas comunicaciones telefónicas y por tanto poder frustrar dichos delitos y eventualmente recopilar evidencia para ser utilizada en procesos penales que llegaran a condenar los sujetos que cometieran dichos ilícitos.

A medida que las fuerzas del orden empezaron a intervenir con mayor asiduidad las conversaciones telefónicas de los miembros de bandas criminales, estos se vieron en la necesidad de recurrir a métodos que les permitieran seguir con su actividad sin poder ser detectados por la policía o mejor dicho que esta última no pudiera recabar información de la actividad criminal en forma válida, y someter a los criminales a un debido proceso. Mas aún si tenemos en cuenta que los delitos antes citados, se llevan a cabo con la participación de individuos radicados en distintos países, es decir: son de carácter transnacional. En los supuestos de tráfico de estupefacientes o armas, el cargamento de drogas ilícitas o armas se prepara en el país A, se lo acondiciona de manera de no ser detectado por las fuerzas policiales, se realiza el contacto con quien será encargado de recepcionar el mismo en el país B y finalmente será remitido a los sujetos que en el país C se encargarán de vender o bien utilizar. Dicha metodología se aplica también al caso de compraventa de armas y a la trata de personas.

a. Nuevas tecnologías

La evolución de las tecnologías informáticas les ha brindado a las organizaciones delictivas, nuevas formas de camuflar sus actividades o desempeñarlas con mayor sigilo.

El desarrollo que han tenido las redes que se dedican a intercambiar fotografías o videos de menores de edad (desde bebés hasta adolescentes) desnudos, en posiciones sexuales o incluso siendo víctimas de abusos sexuales son generalmente de tipo transnacional; ello hace complejo poder llegar a la detección y detención de los sujetos intervinientes, más aún si tenemos en cuenta que es de uso común que, aquellos que participan de dichas actividades para acceder a esas plataformas, deben compartir previamente dicho material, y a efectos de no ser detectados en sus lugares de origen utilizan redes *peer-to-peer* (en adelante, «P2P»).

Aquí debemos detenernos en el concepto de red P2P

> «Una red peer-to-peer (P2P) es un sistema de comunicación descentralizado en el cual cada nodo (par) en la red puede actuar simultáneamente como cliente y como servidor. Este tipo de red permite a los usuarios compartir recursos y datos directamente entre ellos sin necesidad de un servidor central. Las redes P2P se caracterizan por su capacidad de distribuir la carga de trabajo y de datos entre todos los participantes, lo que reduce la dependencia de una infraestructura centralizada y mejora la resistencia a fallos»[2].

Ejemplos de redes P2P son *eMule*, *skype* (en las primeras versiones) *freenet* y *bitcoin* entre otros; *E mule* utiliza *eDonkey* y la red *kad*[3] para permitir a los usuarios compartir archivos entre sí, se caracteriza por la capacidad de encontrar archivos raros y por su robustez en el sistema de intercambio de archivos. En el caso de *eDonkey* faculta a los usuarios a subir archivos de fotos, video, sonido y software que luego transforma en archivos más pequeños que facilitan su descarga y distribución. Así también otorga un sistema de créditos, de manera que los usuarios que suben mayor cantidad de archivos obtienen mayor prioridad en la red y por tanto incentiva el intercambio de material. Es una de las redes más populares entre aquellos que trafican material de abuso sexual infantil.

En el caso de bitcoin[4] es una red P2P que permite que se realicen transacciones directas de criptomonedas entre usuarios sin la necesidad de un intermediario central. Cada uno de los nodos de la red validan y registran las transacciones en una cadena de bloques lo que se conoce como *blockchain*. La empresa precitada en su página web brinda la siguiente definición

> Bitcoin usa tecnología peer-to-peer o entre pares para operar sin una autoridad central o bancos; la gestión de transacciones y la emisión de bitcoins es llevada a cabo de forma colectiva por la red. Bitcoin es de código abierto; su diseño es público, nadie es dueño o controla Bitcoin y todo el mundo puede participar.

Las redes *peer-to-peer* también son utilizadas por los grupos criminales para el desarrollo de actividades como el narcotráfico, compraventa de armas y lavado de activos de origen ilícito.

Teniendo en cuenta que en el siglo XXI, la forma más usual de comunicarse es a través de teléfonos celulares, es que en el año 2016 se comenzó a vender primariamente en Europa, un sistema de telefonía celular que poseía un software que brindaba un sistema de doble encriptación de las comunicaciones, denominado *EncroChat*; lo cual permitía a sus usuarios poder utilizar los mismos sin que las llamadas o mensajes, fueran interceptadas por las fuerzas de seguridad; además poseía un botón de pánico que permitía borrar todos los datos del teléfono.

Ello hizo que comenzara a hacerse popular su uso entre personas preocupadas por la seguridad y privacidad de las comunicaciones, actores, actrices, personas famosas y periodistas. Sin embargo, en la práctica, la explosión de popularidad la tuvo entre los individuos que desarrollaban actividades criminales; bandas organizadas dedicadas al tráfico de estupefacientes, armas de fuego, trata de personas y bandas de motociclistas. Esta empresa fue desarticulada por la policía francesa en conjunto con las fuerzas policiales holandesas en el año 2020, caso que analizaremos más adelante.

---

[2] Monastersky, D. (2018). *Cibercrimen: la nueva amenaza de la delincuencia en la era digital*. Ediciones Jurídicas.
[3] La red Kad es una red descentralizada que utiliza tecnología de tablas hash distribuidas (DHT) para búsqueda e intercambio de archivos entre pares. Enlace.
[4] Bitcoin Project. (s.f.). Bitcoin. Enlace.

Ante la caída de *EncroChat* se vuelca gran parte de «su clientela» a otro software denominado *ANOM*, el cual comenzó a comercializarse en el año 2018 con el objetivo de brindar a sus usuarios un medio de comunicación seguro y por tanto protegido de posibles interceptaciones, el mismo se comercializaba sólo entre miembros del hampa, era requisito para poder acceder a uno de los dispositivos celulares con dicho software, ser recomendado por alguna persona con antecedentes criminales. Luego veremos que en realidad la puesta en funcionamiento de dicho software, fue parte de una operación encubierta denominada «operación trojan shield» llevada adelante por las fuerzas del orden y el FBI.

Además de los métodos de comunicación antes descriptos, existen otros más sencillos y económicos para realizar llamadas telefónicas y enviar mensajes con cierta seguridad, dado su grado de encriptación tales como las aplicaciones de mensajería WhatsApp y telegram. Ambas permiten realizar llamadas telefónicas y enviar mensajes de texto, voz y video. La primera es propiedad de Meta cuyos servidores se encuentran ubicados en Estados Unidos de América y la segunda fue desarrollada por dos hermanos de origen ruso Nikolái y Pável Durob. A través de cualquiera de dichas aplicaciones, se pueden realizar llamadas telefónicas que no pueden ser interceptadas por las fuerzas de seguridad, como las llamadas telefónicas comunes. Además, en el caso de telegram permite enviar mensajes de texto, voz o video que pueden ser borrados ya sea por el emisor o el receptor en su totalidad, no dejando rastros del mismo en el teléfono celular.

Existen otros medios por los cuales se pueden llevar adelante conversaciones tales como Facebook, Instagram, Tik-Tok y Snapchat, entre otros, si bien estas son redes sociales, tienen previstos servicios de mensajería a disposición de sus usuarios, aunque en estos casos la posibilidad de mantener un cierto grado de anonimidad y de seguridad frente a posibles interceptaciones, es muchísimo más bajo que en las precitadas.

También es posible llevar adelante charlas a través de las plataformas de juego on-line, ya que las mismas poseen un chat disponible para sus jugadores, lo cual muchas veces es usado por delincuentes para llevar adelante sus reuniones y mantener conversaciones sobre operaciones criminales de distinta índole.

Por último, no debemos olvidar el correo electrónico, el cual permite enviar archivos de texto, voz o video a través de cualquiera de las plataformas de mail disponibles en la actualidad. Si bien este último es menos seguro si, lo que se busca, es no dejar ningún tipo de rastro del material enviado.

2. Nuevas técnicas de investigación. El agente digital encubierto. Problemas legales y éticos de su implementación

La transnacionalidad de los delitos antes detallados trae aparejados distintos problemas, sea respecto a la legislación aplicable al procedimiento penal como también al derecho penal sustantivo, ya que la actividad criminal se produce afectando la normativa de distintos estados soberanos. Y ello impacta en el tipo de evidencia que se podrá recabar y también en el procedimiento para recabar la misma, de modo de que ella sea útil en un proceso penal posterior.

A los efectos de recabar pruebas se ha hecho necesario recurrir a nuevas técnicas de investigación, una de ellas es la del *agente digital encubierto***.** Se entiende por tal a: toda persona física que oculta su real identidad con la finalidad de entablar con otra persona física o jurídica una relación, y en virtud de ella obtener a través de ese vínculo, información de esta última o de terceros vinculados a ella. Este agente está autorizado judicialmente a participar de comunicaciones que se realizan en canales cerrados de comunicación, pudiendo enviar y recibir archivos de contenido ilícito, así como también analizar los algoritmos utilizados para identificar esos archivos ilícitos. También podrán ser autorizados a obtener imágenes o grabación de conversaciones que se realicen dentro del domicilio del investigado.

En la ley de enjuiciamiento criminal española esta figura no se encuentra definida expresamente, pero la misma surge de los incisos 6 y 7 del art. 282 bis.

a. Implicancias éticas y legales del agente digital encubierto.

Esta figura implica necesariamente la necesidad de entablar con el sujeto intervenido una relación de confianza, en muchos casos hasta de manipulación del mismo, con el objeto de que llegado el momento se pueda obtener la información o prueba buscada. Claramente existe una injerencia en la faz privada muy alta, lo cual puede comprometer el derecho de privacidad de los ciudadanos. Por ese motivo, esta medida debe ser utilizada sólo en supuestos en los que los delitos son graves, sea por su repercusión en la sociedad o por los bienes que resultan vulnerados por los mismos. De lo contrario, se caería en una sociedad hipervigilada, susceptible de ser manipulada por los agentes del estado, vulnerando de esa manera derechos individuales fundamentales como el derecho a la intimidad, la inviolabilidad de la correspondencia y papeles privados, la inviolabilidad del domicilio y de las comunicaciones y el derecho de libertad de expresión, poniendo en jaque la obligación del estado de cumplir con el principio de transparencia de las instituciones públicas, propio de todo estado republicano.

Por todo ello cabe ante todo preguntarse: ¿cuáles son las condiciones necesarias para que, la información recabada por el agente digital encubierto, pueda ser utilizada en un proceso penal? La respuesta radica en el respeto a los principios de legalidad y debido proceso. Ello se logrará si la figura se encuentra específicamente prevista en el ordenamiento jurídico procesal del país en el que se pretende usar dicha técnica de investigación, no se puede aplicar por analogía la figura del agente encubierto común. Ya que la actividad que despliega el agente en el ámbito digital, es mucho más invasiva que la que puede desarrollar el agente encubierto en la realidad física y por tanto claramente puede violar el derecho de intimidad de las personas ajenas a la investigación penal de que se trate.

La otra condición que rige para la validez de la actuación del agente digital encubierto, es que exista autorización del juez competente previa a la misma. Para ello el magistrado debe ser notificado de cuáles son los indicios que existen sobre el delito a investigar, la necesidad de utilizar esta técnica de investigación por la gravedad del hecho delictivo o por su desarrollo fundamentalmente en la red, el plazo específico por el cual se va a habilitar el trabajo del agente encubierto, y la necesidad de que realicen reportes periódicos sobre el resultado de su trabajo. En los casos en los cuales el agente digital encubierto, deba a efectos de lograr recabar evidencia, proceder a realizar video grabaciones o grabación de conversaciones, tendrá que solicitar al magistrado específicamente dicha autorización, no puede muñirse para realizar dichas actividades de

la autorización judicial primigenia. Lo mismo debe aplicar, para los casos en los que, a efectos de proceder a realizar video grabaciones, deba ingresar a un domicilio particular.

En aquellos casos en los cuales el tipo de delito investigado o la dificultad para recabar evidencia, traiga aparejado la necesidad de extender la tarea del agente digital encubierto, será necesario que exista autorización judicial para ello.

Y aquí cabe cuestionarse lo siguiente: ¿puede el agente digital encubierto cometer hechos ilícitos en el marco de su investigación? Y de ser así, ¿podrá ser sancionado penalmente por ello?

Es claro que en el transcurso de una investigación penal de delitos complejos como puede ser el tráfico de drogas, armas, personas o terrorismo muchas veces el agente se verá en la necesidad de cometer algún hecho ilícito con el objetivo de continuar su actuación dentro de la red que se encuentra investigando, recordemos que esta figura se aplicará para delitos graves tales como los mencionados. De lo contrario, la tarea del investigador se verá frustrada, y el trabajo y esfuerzo desplegados en pos de la protección de bienes jurídicos sensibles, será en vano. Sin embargo, para que los actos delictivos que haya realizado el agente encubierto digital, no sean sancionados penalmente, será necesario que los mismos guarden proporción y razonabilidad con el delito investigado y en la medida en que no hayan sido provocados por el agente. Así lo ha previsto la ley de enjuiciamiento criminal española en su artículo 282 bis inciso 5 «el agente encubierto estará exento de responsabilidad criminal por aquellas actuaciones que sean consecuencia necesaria del desarrollo de la investigación, siempre que guarden la debida proporcionalidad con la finalidad de la misma y no constituyan una provocación al delito».

b. Caso *EncroChat* y operación *trojan shield*.

En virtud de las investigaciones que estaba llevando a cabo en el año 2017, el instituto de investigación criminal de la gendarmería nacional detectó el uso de teléfonos celulares con tecnología Android, que poseían un software que permitía realizar llamadas encriptadas, así como también enviar mensajes y crear notas encriptadas. El software de la empresa *EncroChat* además poseía un «botón de pánico» que permitía a sus usuarios una vez presionado, eliminar todo el contenido de los datos existentes en el teléfono, además tenía una función de autodestrucción. Este servicio, permitía mejorar la seguridad de la comunicación que brindaban los teléfonos desechables, sobre todo ante el avance de las fuerzas policiales en la ruptura de las encriptaciones. La aplicación funcionaba con una suscripción de pago de 3.000 euros al año.[5]

La investigación fue iniciada por la fiscalía de la jurisdicción interregional especializada de Lille (Francia), debido a que la ubicación de los servidores que ejecutaban *EncroChat*, se encontraban en su jurisdicción. Pero la investigación completa se llevó adelante en conjunto con la fiscalía de Holanda con el apoyo de Europol y Eurojust. Al tiempo de conclusión de la operación mencionada, existían 50.000 teléfonos celulares con ese software y el 90 % de los mismos era utilizado por criminales.

La operación de infiltración de la *red EncroChat* llevó aproximadamente más de dos meses. El malware enviado consistía en una actualización de los dispositivos *EncroChat* que realizaba el servidor comprometido, lo cual trajo aparejado que todos los dispositivos

[5] Zagaris, B. (2020, 30 de septiembre). EncroChat: la Policía europea desmantela una extendida red de mensajería encriptada para delincuentes. DelitosFinancieros.org. Enlace.

afectados, cargaran una imagen de todo el contenido del teléfono de vuelta a la policía francesa.

Tal es así que el 2 de julio de 2020, dichas autoridades anunciaron públicamente «la caída de *EncroChat*» lo que llevó a realizar más de 800 detenciones en países como Francia, Holanda, España, Reino Unido, Francia, Alemania, Suecia y Noruega.

La infiltración del servicio *EncroChat* por parte de las autoridades precitadas, tuvo aparejado detectar y desarticular operaciones de tráfico de drogas, armas, asesinatos, secuestros y lavado de dinero llevadas adelante en Europa por bandas del crimen organizado. Lo cual redundó en la incautación de más de 8.000 kilos de cocaína en Holanda, así como 1.2 toneladas de metanfetaminas, 25 millones de euros en efectivo, joyas, decenas de autos de lujo y el desmantelamiento de laboratorios de drogas sintéticas.

En tanto que, en el Reino Unido, la policía logró realizar más de 700 arrestos, confiscó 67 millones de libras esterlinas en efectivo, dos toneladas de drogas y numerosas armas de fuego.

Pero con la detención y arresto de tantos individuos surgieron las quejas planteadas por las defensas de los mismos en distintos países europeos, fundamentalmente en relación a la posibilidad del correcto ejercicio del derecho de defensa ante la legalidad de las pruebas obtenidas a través de la operación «*EncroChat*». Sus principales argumentos radican sobre:

- La falta de especificación de la medida de intervención de las comunicaciones, ya que no se encontraba determinado que tipo de comunicaciones se iban a intervenir; si eran llamados telefónicos, correos electrónicos o mensajes de texto;
- el desconocimiento sobre cómo se hicieron las interceptaciones, las defensas no pudieron acceder a conocer de qué manera se hicieron las mismas, ya que la policía francesa manifestó que el método utilizado, quedaba dentro de la ley de seguridad nacional y por tanto secretas;
- el uso de la encriptación como presunción de culpabilidad, sostienen que los tribunales han desarrollado una jurisprudencia basada en que la existencia de información encriptada en poder de los acusados, ya de por sí los hace parte de una organización criminal; y
- la falta de autorización judicial previa, ya que luego de cancelada la actividad de la empresa *EncroChat*, las autoridades francesas y holandesas remitieron al Reino Unido, Alemania y otros países europeos, la información que fue recabada en el curso de la investigación, ello a través de una orden de investigación europea, pero esto se hizo sin la autorización previa de un juez.

En el Reino Unido, se interpusieron recursos solicitando que se dejaran sin efecto, las condenas o arrestos que se habían realizado en virtud de la información brindada por los investigadores de *EncroChat*. En el precitado país existe una norma denominada «ley de poderes de investigación» del año 2016 que dispone que, interceptar comunicaciones a través de un «sistema de telecomunicaciones» es ilegal a menos que haya una orden adecuada vigente.

Existen distintos tipos de ordenes exigidas, dependiendo de si el mensaje interceptado estaba siendo transmitido o estaba almacenado en un lugar del sistema. Si está en reposo, la policía debe solicitar una orden de interferencia de equipos dirigida, pero si está en transmisión, se requiere una orden de intercepción dirigida. Teniendo en cuenta esta diferencia la justicia del Reino Unido en el año 2021 resolvió

> hemos concluido que la única pregunta sustancial que el juez estaba obligado a responder era si el material de *EncroChat* estaba almacenado por o en el sistema de telecomunicaciones cuando fue interceptado. Al igual que él, consideramos que estas comunicaciones no estaban siendo transmitidas sino almacenadas en ese momento.

Razón por lo cual, desestimó el pedido de las defensas sobre la nulidad de la información que fue obtenida a través del hackeo de *EncroChat*, que realizaran las fuerzas policiales francesas y holandesas.

Sin embargo, esta situación puede cambiar en un futuro cercano, ya que los tribunales franceses en el año 2022 resolvieron que los investigadores y fiscales, no proporcionaron un certificado para autenticar los datos telefónicos interceptados y los mensajes obtenidos de los teléfonos *EncroChat*; tal como lo exige la ley francesa. También se determinó que la policía francesa no reveló, por motivos de secreto de defensa, cómo las autoridades holandesas y francesas llevaron a cabo la operación de hacking en *EncroChat*.

Y siguiendo esa línea, es que el tribunal de justicia europeo el 30 abril del año 2024, resolvió en el caso C-670/22, M.N contra el Estado Alemán, que

> «[…] El artículo 31 de la Directiva 2014/41 debe interpretarse en el sentido de que una medida relacionada con la infiltración en aparatos terminales, con objeto de extraer datos de tráfico, de localización y de comunicación de un servicio de comunicación basado en Internet, constituye una «intervención de telecomunicaciones», en el sentido de dicho artículo, que debe notificarse a la autoridad designada a tal efecto por el Estado miembro en cuyo territorio se encuentre la persona que sea objeto de la intervención. En el supuesto de que el Estado miembro que realice la intervención no esté en condiciones de identificar a la autoridad competente del Estado miembro notificado, esta notificación podrá dirigirse a cualquier autoridad del Estado miembro notificado que el Estado miembro que realice la intervención considere idónea para ello».

En el considerando 5 dispone

> «[…] El artículo 14, apartado 7, de la Directiva 2014/41 debe interpretarse en el sentido de que obliga al juez penal nacional a excluir, en el marco de un procedimiento penal incoado contra una persona sospechosa de haber cometido hechos constitutivos de delito, determinada información y determinadas pruebas si dicha persona no está en condiciones de comentar eficazmente esa información y esas pruebas y si estas pueden influir destacadamente en la apreciación de los hechos».

Teniendo como antecedente la investigación del caso *EncroChat*, es que el FBI decidió llevar adelante lo que dio en llamar «operación Trojan Shield». El precitado órgano de investigación, había logrado con éxito acusar y encarcelar al titular de una empresa denominada *Phantom*, dedicada a brindar servicios de telefonía celular con un software de encriptación; a raíz de ello logran reclutar un «informante» el cual se encontraba desarrollando una «nueva generación» de aparatos de comunicación encriptados denominado *ANOM*. Este informante, con anterioridad había comercializado equipos de telefonía celular con software de encriptación, los mismos se vendían entre miembros del hampa exclusivamente, de manera que era conocido en el ambiente de la criminalidad organizada.

El funcionamiento del dispositivo *ANOM* implicaba un «backdoor» diseñado por el FBI, que permitía que cada mensaje enviado por los usuarios de *ANOM*, generara una copia cifrada adicional enviada a un servidor controlado por el FBI conocido como «*iBot*».

Este servidor descifraba el mensaje, extraía la información relevante (ubicación GPS, texto, nombre de usuario, etc.), y luego reenviaba la información a otro servidor, propiedad del FBI (*iBot2*). En virtud de restricciones legales de Estados Unidos, el servidor se ubicó primigeniamente en Australia, con intervención de la policía australiana y luego en Lituania.

Durante la etapa de versión beta de *ANOM*, la policía australiana solicitó órdenes judiciales a efectos de monitorear legalmente, a aquellos ciudadanos australianos que se encontraban utilizando dicho dispositivo o bien a individuos con claros nexos con Australia.

Durante el transcurso del año 2019, el FBI comenzó tratativas con un tercer país a efectos de que se instale un servidor «*iBot*» en este último, de manera que una vez que este, obtuvo la orden judicial correspondiente de acuerdo a su legislación, procedió a copiar toda la información del «*iBot*» y en virtud de un tratado existente entre Estados Unidos y el precitado país, a través de un *mutual legal assistance treaty* (*MLAT*) el FBI pudo acceder a la copia del servidor.

Con posterioridad el tercer país obtuvo una orden judicial para acceder a las copias del «*iBot*» cada tres días. Dicha información fue remitida al FBI hasta junio del año 2021. Esa información comprendía los mensajes encriptados de todos los usuarios de *ANOM*. Y trajo aparejado la traducción de 20 millones de mensajes correspondientes a 11.800 dispositivos, que eran utilizados en 90 países.

La mayor cantidad de usuarios se encontraban en Alemania, España, Australia, Holanda y Serbia. Del análisis de los mensajes, el FBI pudo determinar que los dispositivos eran utilizados exclusivamente por miembros de organizaciones criminales transnacionales, dedicadas al tráfico de droga y lavado de dinero, sin embargo, también detectaron otras actividades ilícitas.

Con el acceso a esta información, detectives del FBI solicitan autorización judicial al tribunal de distrito de California, a efectos de que le otorguen autorización para que la *Empresa Google LLC*, entregue copia digital de toda la información correspondiente a la cuenta expliam@gmail.com desde el 1 de enero de 2021 al 15 de mayo del 2021 a funcionarios del FBI. La información requerida consistía en el contenido de los correos electrónicos, sus adjuntos, mensajes de texto guardados, mensajes de voz, fotografías, logs de acceso, perfiles, lista de amigos, información de pagos, detalles de facturas y documentación de embarques.

El juez autorizó la misma y ello llevó a que las autoridades norteamericanas, pudieran realizar más de 500 arrestos en distintos países, secuestraron 8 toneladas de cocaína, 22 toneladas de marihuana, 48.000.000 de dólares en efectivo y criptomonedas, armas de fuego, vehículos de lujo y además lograron desmantelar 50 laboratorios clandestinos de drogas.

Si bien los abogados defensores de los acusados, han intentado lograr la exclusión de la evidencia recabada en esta investigación, argumentando que se habían violado el derecho al debido proceso y el derecho a la privacidad, hasta el momento ningún Tribunal ha receptado tales posturas, y no han rechazado la evidencia recabada.

En la *operación Trojan Shield*, se tiene certeza de que toda la información a la que se estaba «accediendo» a través de la infiltración de los aparatos de comunicación encriptados, correspondían a criminales. Esto es lo que marca la diferencia con el caso

EncroChat, cuyo dispositivo era utilizado por criminales, pero también por ciudadanos comunes y corrientes, si bien en un número ínfimo en relación a aquellos.

3. Acceso transfronterizo de datos

La evolución de la tecnología de la comunicación y en especial de internet siendo esta, una super autopista de información, que implica que cualquier persona pueda tener acceso a todo tipo de servicio de información electrónica, con indiferencia del lugar el mundo en el que se encuentre; trajo aparejado problemas relacionados a los delitos cometidos en el «ciberespacio», pero también en relación a los delitos tradicionales, cuyos autores se valen de las nuevas técnicas de comunicación para llevarlos adelante. Los delitos cometidos en el ciberespacio comprenden los ataques contra la integridad, disponibilidad y confidencialidad de los sistemas informáticos y de las redes de comunicación. Hablamos de situaciones en las que un individuo radicado en un país «X», puede acceder ilegítimamente al servidor que contiene la información de todos los residentes argentinos que poseen licencia de conducir[6]; o el hecho de que un grupo de personas de nacionalidad rusa realice un «ataque» «a una empresa aseguradora Argentina», enviándoles un virus a través de un inocente correo, que traiga aparejado el «secuestro» de toda la base de datos de la misma; la cual posteriormente es encriptada y a cambio de su devolución, se le exigen a los directivos una determinada suma de dinero[7]. Estas son situaciones, que eran impensables para los legisladores de comienzos del siglo pasado.

Como se puede observar, se pone en juego la territorialidad de las autoridades encargadas de exigir el cumplimiento de las leyes, ya que estamos frente a conductas delictivas transfronterizas.

Teniendo en cuenta, que la información generalmente se encuentra almacenada en servidores de distintos países, el acceso a dicha información importa poner en juego la legislación penal y procesal penal de dichos estados.

Sin olvidarnos que la evidencia electrónica es volátil, por lo cual esta situación coloca un escollo más en las investigaciones transnacionales, sin olvidar que existen distintos marcos normativos en materia de protección de datos personales, que dificulta el acceso a la misma, además de falta de capacitación de las autoridades que existen en algunos países. Para ello debemos tener como norte, el respeto a la privacidad de los datos personales y la cooperación de los estados nacionales.

Por ello se hace necesario, ante una sociedad globalizada e hiperconectada crear mecanismos de cooperación internacional, que faciliten el acceso a evidencia clave en la comisión de delitos. Esto debe producirse, de manera que la misma pueda ser recabada tomando los recaudos necesarios, que permitan luego incorporar la misma al proceso penal. Lo cual trae aparejado, el respeto al debido proceso, y el acceso de la defensa a conocer la metodología que se utilizó para recabar la prueba. Recordemos que la misma, se encuentra alojada en servidores de un país distinto de aquél en el que vive su defendido.

[6] Infobae. (2024, 16 de abril). *Hackearon la base de datos de licencias de conducir: contiene casi 6 millones de registros y piden USD 3000 para devolverlas*. Infobae. Enlace.
[7] Ámbito. (2024). *Ciberseguridad: una aseguradora argentina sufrió un importante ataque hackers rusos*. Ámbito. Enlace.

Estas son las cuestiones que ya a finales de los años 90, se estaban discutiendo en el marco del comité europeo para los problemas criminales y el cual tomó en cuenta el informe del profesor Dr. H. W. K. Kaspersen el cual sostuvo lo siguiente

> «[…] habría que buscar otro instrumento jurídico más obligatorio que una recomendación, tal como un convenio. Dicho convenio no debería abordar tanto las cuestiones de derecho penal sustantivo como las cuestiones de derecho procesal penal, así también como los acuerdos y procedimientos del derecho penal internacional»[8].

En tanto que, en la conferencia del G-8 sobre crimen organizado transnacional, que se realizó en Moscú el 19 y 20 de octubre de 1999, se establecieron lineamientos claves, para combatir el crimen organizado transnacional y los delitos de alta tecnología. Entre ellos se encontraban los siguientes: (a) Permitir la conservación de datos contenidos en los sistemas informáticos de otro Estado de forma expedita en conformidad con la legislación nacional; (b) Autorizar el acceso, búsqueda, copiado o incautación de datos almacenados en sistemas informáticos ubicados en otro Estado; cuando se ha otorgado el consentimiento voluntario de una persona que tiene la autoridad legal para divulgar los datos; (c)Disponer que el acceso transfronterizo a datos almacenados, no requieren la asistencia jurídica cuando se encuentren en fuentes públicas (fuentes abiertas), con independencia de su ubicación geográfica; (d) Establecer que cuando un Estado requiera acceso a datos en otro Estado, y esos datos revelen una violación del derecho penal, se debe notificar al Estado donde se llevará a cabo el acceso.

En el año 2010 la *unión internacional de telecomunicaciones* (UIT) elaboró un conjunto de herramientas legislativas sobre ciberdelito; con el objetivo de facilitar y proporcionar a los distintos países materiales de referencia y apoyo, para armonizar la legislación y normas de procedimiento en materia de ciberdelito. Otra meta era que la misma pueda ser utilizada como guía, para los estados que deseen desarrollar o modificar la legislación sobre el tema.

La sección 30 de ese conjunto de herramientas, posee un artículo muy similar al artículo 32 del convenio de Budapest del año 2001[9], el primero dispone que la autoridad competente podrá acceder a los datos informáticos almacenados (de fuente abierta) y son de acceso público, ya sean estos de contenido o de tráfico con independencia de la ubicación geográfica de los mismos.

Así también prevé que

> […]una autoridad competente de otro país puede, sin autorización de las autoridades de ese país, tener acceso y recibir, por medio de una computadora o sistema informático ubicado en su territorio, datos informáticos especificados, datos de contenido o datos de tráfico almacenados en ese país si la autoridad competente del otro país obtiene el consentimiento legal y voluntario de la persona que tiene la autoridad legal para divulgar los datos a dicha autoridad competente a través de esa computadora o sistema informático»[10].

Tal como había expresado el profesor Kaspersen, se hacía necesario tener un Convenio que permitiera abordar temas de derecho procesal internacional en materia de

[8] Consejo de Europa. (1997). *Aplicación de la Recomendación núm. R (89) 9 sobre delitos informáticos* (Informe preparado por el Prof. Dr. H. W. K. Kaspersen, Doc. CDPC (97) 5 y PC-CY (97) 5, p. 106).
[9] Consejo de Europa. (2001*). Convenio sobre Ciberdelincuencia* (Budapest, 23 de noviembre de 2001), art. 32: Acceso transfronterizo a datos almacenados con consentimiento o cuando estén disponibles públicamente.
[10] Unión internacional de telecomunicaciones. (2010). *Conjunto de herramientas para la legislación sobre ciberdelito* (Sección 30).

ciberdelitos, y es así como surgió el convenio de Budapest en el año 2001, suscripto por Estados Unidos y gran parte de los países que conforman la Unión Europea. El mismo quedó abierto para su adhesión por parte de otros Estados, con el objetivo de tener una herramienta internacional que favoreciera el intercambio de información ubicada en bases de datos informáticas o sistemas informáticos transnacionales, a través de procesos ágiles y no engorrosos que favorezcan la persecución de los delitos cometidos en el ciberespacio o a través de él. Ello respetando los derechos fundamentales previstos en el *convenio del consejo de Europa para la protección de derecho humanos y de las libertades fundamentales* (1950), *pacto internacional de derechos civiles y políticos de naciones unidas* (1966), el *convenio del consejo de Europa para la protección de los datos informatizados de datos personales* (1981) y otros convenios que tienen por objeto el resguardo a la libertad de expresión y el respeto al derecho de privacidad.

El precitado convenio posee un protocolo adicional que penaliza la comisión de actos xenófobos o racistas cometidos a través de internet.

El segundo protocolo adicional al convenio sobre ciberdelincuencia, relativo a la cooperación reforzada y la revelación de pruebas electrónicas se sancionó el 12 de mayo del año 2022 y entró en vigencia a finales del año 2023.

Este último ha previsto entre otras medidas tendientes a reforzar la cooperación internacional, en su artículo 12, la conformación de equipos conjuntos de investigación entre los Estados partes del mismo. Dichos equipos actuarán en sus territorios en aquellos casos que sean convenientes por la naturaleza de la investigación y proceso penal, ello a efectos de favorecer las mismas.

Para ello, las autoridades competentes acordarán los procedimientos y condiciones que van a regir el funcionamiento de los equipos conjuntos de investigación; en particular lo atinente a su composición, funciones, duración, organización, requisitos correspondientes a la recopilación, transmisión y utilización de pruebas que realicen las autoridades de una parte en la investigación que tenga lugar en el territorio de la otra parte.

Así también dispone que, cuando sea necesario tomar medidas de investigación en el territorio de una de las partes en cuestión, las autoridades participantes de dicha parte podrán solicitar a sus propias autoridades, tomar esas medidas sin que sea necesario presentar una solicitud de asistencia mutua.

El uso de la información podrá ser denegado o restringido según lo pactado en el acuerdo. Si el mismo no regula las condiciones para denegar o restringir su uso, las partes podrán utilizar esa información para los casos previstos en el Convenio, ante situaciones de emergencia, y para la detección, investigación, enjuiciamiento de delitos distintos de los contemplados en el acuerdo, siempre que exista la autorización previa, de las autoridades que proporcionen la información o las pruebas.

Es altamente probable, que el resultado de la operación denominada *EncroChat* llevada adelante en un principio por Francia y Holanda en el año 2017, haya servido como antecedente para la incorporación del artículo 12 del segundo protocolo de Budapest. Mas aún si tenemos en cuenta que hasta el día de hoy, se está debatiendo en los Tribunales Europeos la validez de la evidencia recabada en la operación precitada.

La república argentina adhirió al convenio de Budapest sobre ciberdelincuencia del año 2001, el cual entró en vigencia en virtud de la ley 27.411, de fecha 15 de diciembre

del año 2017. En tanto que, a mediados de febrero del año 2023, la república argentina adhirió al segundo protocolo adicional de Budapest.[11]

4. El agente digital encubierto y la legislación argentina

En la actualidad la figura del *agente digital encubierto* sólo está previsto en la provincia de Mendoza. En otras jurisdicciones existe la figura del agente encubierto y del agente revelador, tal como ocurre en la ciudad autónoma de buenos aires o en la provincia de santa fe, pero no específicamente la del agente digital encubierto.

El código de procedimiento penal de Mendoza, receptó a comienzos del 2024 esta figura especial en el artículo 29 bis, y lo define en su último párrafo de la siguiente manera

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

La normativa procesal dispone que, en aquellos casos en los que sea necesario investigar delitos en plataformas o entornos digitales, el fiscal podrá solicitar autorización al juez penal colegiado; pero para ello deberá haber fundado expresamente los motivos por los cuales se hace necesario recurrir a tal medida de investigación. Así también deberá acreditar que la misma es imperiosa ya que se encuentra ante la posible existencia de delitos de producción, comercialización y distribución de material de abuso sexual infantil; es decir toda la gama de hechos tipificados en el artículo 128 del código penal, también para el caso del delito de grooming, receptado en nuestro ordenamiento jurídico penal en el artículo 131. El código procesal penal de Mendoza agrega, que se podrá recurrir a la utilización del agente digital encubierto, cuando se trate de delitos cometidos a través de medios informáticos, que no pueden ser investigados por otros medios; como todo otro delito que por su especial gravedad o por la complejidad de su investigación, justifique utilizar esta figura.

El agente deberá realizar su tarea en un plazo de 180 días, contados a partir de la fecha en que el juez lo autorizó. No se encuentra prevista en forma expresa la posibilidad de prorrogar dicho plazo, de manera tal que sólo será legal la actuación del agente, siempre que se haya realizado dentro de ese marco de tiempo.

Los perfiles que hayan sido creados para la actuación del agente, no podrán corresponder a imágenes que pertenezcan a personas reales, y serán manejados por personal idóneo de la fiscalía o de la fuerza de seguridad habilitada para ello. Todo el trabajo que lleve adelante dicho agente deberá ser puesto en conocimiento de la fiscalía que solicitó la medida, la cual será la encargada de resguardar (en caja de seguridad) toda la información relativa a los perfiles usados, las plataformas en las que haya intervenido, las claves de acceso a las mismas y la actividad concreta desarrollada por el mismo.

A efectos de proteger al agente digital encubierto, de la responsabilidad penal que pueda surgir como consecuencia de su tarea, la normativa dispone que el mismo podrá

[11] Presidencia de la Nación. (2025). *Argentina y la Unión Europea unen esfuerzos para combatir el ciberdelito*. Argentina.gob.ar. Enlace.

enviar o intercambiar archivos ilícitos relacionados a la investigación en curso, siempre que esté autorizado para ello. Así también se establece que quedará exento de responsabilidad criminal en la medida que los actos realizados guarden proporción con la tarea desarrollada y siempre que no hayan sido provocados. De hecho, el párrafo que trata dicho tema tiene una redacción muy similar al artículo 282 bis inciso 5 de la ley de enjuiciamiento criminal española; siendo que el art. 29 bis código procesal penal de Mendoza dispone

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

5. Conclusión

Teniendo en cuenta el gran impacto que tienen las tecnologías informáticas de la comunicación en el desenvolvimiento de la vida actual, y observando que las mismas son utilizadas para cometer ilícitos, debido a que brindan celeridad, seguridad y anonimidad a las organizaciones criminales; se hace necesario que la normativa procesal nacional e internacional prevea normas que recepten técnicas especiales de investigación. Tal es el caso de la figura del agente digital encubierto, la cual deberá encontrarse específicamente regulada en los códigos de procedimiento. Ello con el ánimo de proteger los derechos a la privacidad de los datos personales, a la intimidad, a la libertad de expresión, al debido proceso y la igualdad de armas en el mismo; logrando un equilibrio con la necesidad de proteger y castigar delitos que debe perseguir todo estado, para brindar seguridad a sus ciudadanos.

6. Bibliografía

Barberá, G. (s.f.). *Nuevas tecnologías y libertad probatoria en el proceso penal*.

Bitcoin Project. (s.f.). *Bitcoin*. Recuperado de https://bitcoin.org/

Chambers. (2022, noviembre 22). *What France's Supreme Court Decision Re Encrochat Evidence Means for the UK* (M. S. Khan). https://chambers.com/articles/what-frances-supreme-court-decision-re-encrochat-evidence-means-for-the-uk

Consejo de Europa. (2001). *Convenio de Budapest sobre Ciberdelincuencia*.

Consejo de Europa. (s.f.). *Protocolo adicional que penaliza la criminalización de actos de naturaleza racista y xenófoba cometidos a través de sistemas informáticos (CETS 189)*.

Consejo de Europa. (s.f.). *Protocolo adicional al Convenio sobre Ciberdelincuencia relativo al refuerzo de la cooperación y la divulgación de las pruebas electrónicas*.

Eurojust. (s.f.). *Eurojust*. https://www.eurojust.europa.eu

Euronews. (s.f.). *Euronews*. https://es.euronews.com

Infobae. (2024, 16 de abril). *Hackearon la base de datos de licencias de conducir: contiene casi 6 millones de registros y piden USD 3000 para devolverlas*.

https://www.infobae.com/politica/2024/04/16/hackearon-la-base-de-datos-de-licencias-de-conducir-contiene-casi-6-millones-de-registros-y-piden-usd-2000-para-devolverlas/

Instituto de Investigación Criminal de la Gendarmería Nacional. (2020). *Search Warrant Operation Trojan Shield, AO 106A (08118) Application for a Warrant by Telephone or Other Reliable Electronic Means Case*.

Kademlia Project. (s.f.). *Kad network*. http://www.kademlia.com/

Ley de Enjuiciamiento Criminal Española. (s.f.). España.

Ley No. 9510 de la Provincia de Mendoza. (s.f.). Argentina.

Monastersky, D. (2018). *Cibercrimen: La nueva amenaza de la delincuencia en la era digital*. Ediciones Jurídicas.

Montserrat de Hoyos, M. (2022, 14 de junio). *La investigación penal a través del agente encubierto* [Trabajo de grado, Universidad de Valladolid].

Presidencia de la Nación. (2025). *Argentina y la Unión Europea unen esfuerzos para combatir el ciberdelito*. https://www.argentina.gob.ar/noticias/argentina-y-la-union-europea-unen-esfuerzos-para-combatir-el-ciberdelito

Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala) de 30 de abril de 2024, asunto C-670/22.

Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala) de 16 de julio de 2020, asunto C-311/18.

The Register. (2020, 13 de noviembre). *EncroChat Judicial Review Judgement*. https://www.theregister.com/2020/11/13/encrochat_judicia_review_judgement

Unión Internacional de Telecomunicaciones. (2010). *Recomendaciones legislativas sobre ciberdelito*.

United States Attorney's Office, Southern District of California. (2021, 28 de mayo). *Indictment: Operation Trojan Shield, Case 3:21-cr-01623-JLS, Document 1*. https://www.justice.gov/usao-sdca/pr/fbi-s-encrypted-phone-platform-infiltrated-hundreds-criminal-syndicates-result-massive

Zagaris, B. (2020, 30 de septiembre). *EncroChat: la Policía europea desmantela una extendida red de mensajería encriptada para delincuentes*. DelitosFinancieros.org. https://www.delitosfinancieros.org/encrochat-la-policia-europea-desmantela-una-extendida-red-de-mensajeria-encriptada-para-delincuentes/

Ámbito. (2024). *Ciberseguridad: una aseguradora argentina sufrió un importante ataque de hackers rusos*. https://www.ambito.com/informacion-general/ciberseguridad-una-aseguradora-argentina-sufrio-un-impotante-ataque-hackers-rusos-n5665636