UNCUYO
UNIVERSIDAD
NACIONAL DE CUYO

FACULTAD DE DERECHO

Tesis de Maestría

Las técnicas de investigación penal a la luz del Convenio sobre ciberdelito y su aplicación en Argentina

Maestría en Derecho Penal y Ciencias Penales

Alumno:
JUAN PABLO CHALES

Director:
DIEGO J. LAVADO

Mendoza, 2018

Índice

INTRODUCCIÓN

La irrupción de las nuevas tecnologías de la información, en el contexto de una sociedad cada vez más globalizada y conectada a través de los diversos medios electrónicos, sumado a la celeridad con que se producen los cambios, ha traído como consecuencia distintas conductas disvaliosas que se enfrentan con la rigidez del esquema legal penal que tenemos en Argentina.

La regla constitucional que no existe delito sin ley previa (art. 18 CN) y la prohibición de la interpretación analógica en materia penal, enfrentadas al dinamismo que conlleva el avance de las nuevas tecnologías, han tornado atípicos ciertos hechos claramente lesivos, impidiendo muchas veces la persecución y sanción de los mismos.

La ley 26.388, promulgada en junio de 2008[1], incorporó distintos delitos informáticos en el Código Penal Argentino, adecuando la ley penal argentina a las normas previstas en la Convención sobre *Cibercriminalidad*, firmada en la ciudad de Budapest en 2001.

Esta reforma significó no solo una actualización de nuestra legislación penal, sino que implica un cambio de concepción en muchos conceptos legales que el avance tecnológico había dejado obsoletos, así como también la incorporación de nuevos tipos penales y la actualización de algunos ya existentes.

Muestra de ello, es el alcance del término *documento* dada en el código penal, comprensivo del *documento electrónico*, al definirlo como "toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión"[2].

[1] https://www.boletinoficial.gob.ar/#!DetalleNormativa/408885/null
[2] Art. 77 Código Penal de la Argentina, actualizado por ley 26.388.

Ahora bien, no es solo el derecho penal sustantivo el que debe mantenerse actualizado a las nuevas tecnologías, sino también el derecho procesal penal y las técnicas de investigación, ya que el avance de estas ha permitido no solo nuevas conductas delictivas, sino también nuevas herramientas procesales, en razón de la mayor información que brinda un dato informático, una comunicación electrónica, etc.

En este sentido, ya en el contexto de una investigación penal, las nuevas tecnologías han permitido desarrollar modalidades de acreditación del hecho penal, no solo delitos informáticos propiamente dichos, sino también delitos cometidos a través de sistemas informáticos o delito comunes.

Es decir, hoy el uso de las tecnologías de la información permite obtener pruebas y avanzar en una investigación penal, tanto en *grooming*, en daño o estafa informática, como también en un homicidio o en un robo. Así, sin duda alguna, apenas sucedido un homicidio, por ejemplo, puede ser importante saber con quién se comunicó la víctima, si dijo algo o no a través de alguna red social, cuáles fueron sus últimas ubicaciones geográficas, etc., todo lo cual puede obtenerse, a través del acceso a los dispositivos electrónicos o informáticos utilizados.

En consecuencia, el avance de las nuevas tecnologías y el manejo de la evidencia digital, deviene trascendental en cualquier investigación penal, máxime si se reconoce la enorme influencia de la informática en la vida cotidiana de una persona, donde ya resulta cada vez más común que una persona tenga acceso a internet a través de un *Smartphone*, una *Tablet*, una computadora, etc. u otros elementos de la vida cotidiana como lavarropas, heladeras, luces del hogar, cámaras de seguridad, relojes inteligentes, etc., los que también brindan datos útiles a una investigación.

A ello, debe agregarse la enorme cantidad de información que se almacena en cada uno de dichos dispositivos, pudiendo uno tener en un *Smartphone,* no solo la agenda de contactos, sino también numerosas fotos, videos, archivos, etc., los cuales además se encuentran organizados con fechas, horas, extensión de estos, dispositivo que lo creó, la ruta de tráfico si hubo alguna transferencia o envío.

Así, las comunicaciones telefónicas, alguna vez una modalidad de avanzada frente a la correspondencia postal, deviene ahora una alternativa simple frente a las vías de comunicación actual, regidas por la informática, donde en menos de segundos pueden transmitirse no solo la voz sino también la palabra escrita, fotos, videos, archivos, en volúmenes mucho mayores.

Esta información resulta de suma utilidad en toda investigación, siendo, en la mayoría de los casos, aportes sustanciales en el avance de estas.

Más aún en los delitos informáticos propiamente dichos, donde la dificultad para identificar al autor y estimar la magnitud e impacto del acto dañoso en el entorno de las redes interconectadas, la volatilidad de los datos informáticos, la que impide muchas veces la conservación de la prueba necesaria para la acreditación del hecho delictivo, son algunos de los principales problemas que se enfrenta el proceso penal, ante el avance de estos nuevos modos de actuación delictiva.

La evidencia digital está representada por los datos e información que se almacena, transmite o recibe en un dispositivo electrónico, y pueden tener valor en una investigación criminal. Las características que presentan este tipo de pruebas son: que son volátiles al igual que las huellas digitales o las pruebas de ADN; que cruzan las fronteras jurisdiccionales de manera automática en cuestión de segundos; que pueden ser sensibles en su integridad al paso del tiempo dependiendo del soporte de almacenamiento; que pueden ser fácilmente alteradas, dañadas, destruidas o borradas[3]

Esta abarca prueba informática de carácter sonoro y visual, informes telefónicos, contactos telemáticos, correos electrónicos, entre otros, y exige al mismo tiempo cualidades y capacidades distintas a las que generalmente pueden encontrarse en la búsqueda de prueba en un delito ordinario.

Puede constar de elementos de software tales como documentos de texto, planillas de cálculo, imágenes y fotos, archivos de audio y de video, archivos adjuntos y bases de datos de diferentes tipos, entre otros. También puede incluir datos e información de navegación de internet tales como historial de sitios web visitados por un usuario, cookies almacenadas en una computadora, registros en salas de chat o foros de discusión, mensajes en blogs personales y redes sociales, registro de envío de archivos en programas de intercambio. En relación con el hardware, las unidades de procesamiento de las computadoras y los dispositivos de almacenamiento externos e internos representan unidades de análisis, en tanto que tienen la capacidad de almacenar datos e información digital[4].

[3] SAIN, Gustavo Raúl, "Delito y nuevas tecnologías: fraude, narcotráfico y lavado de dinero por internet", Editores del Puerto, 1ª Ed, Ciudad Autónoma de Buenos Aires, 2012

[4] SAIN, Gustavo Raúl, "Delito y nuevas tecnologías: fraude, narcotráfico y lavado de dinero por internet", Editores del Puerto, 1ª Ed, Ciudad Autónoma de Buenos Aires, 2012

Los rastros digitales de la comisión de delitos cibernéticos no siempre pueden conservarse, en especial debido al medio comisivo utilizado. La eliminación o borrado de esa evidencia digital suele ser más sencillo que ocultar el cuerpo del delito en otros casos[5].

En este sentido, la preservación rápida de los datos almacenados, sean de contenido, de tráfico o relativos al abonado, la obtención en tiempo real de datos informáticos o la interceptación de aquellos relativos al contenido, el acceso y observación de sistemas informáticos, son algunas de las técnicas de investigación que aparecen como necesarias en estos delitos.

En Argentina, si bien ha habido algunas reformas legislativas que prevén ciertas adaptaciones a las nuevas tecnologías de la información y comunicación, siguen siendo normas relativas a la interceptación de correspondencia o de llamadas telefónicas y al secuestro de documentación, las medidas de mayor aplicación en cuanto se requiere el acceso, la obtención o incorporación al proceso penal de un dato informático u otra evidencia digital, aun cuando sean de aplicación analógica.

En noviembre de 2017 se sancionó la ley 27.411, que dispuso la adhesión de la Argentina al Convenio sobre *ciberdelincuencia* celebrado por el Consejo de Europa en la ciudad de Budapest, en el año 2001.

Dicho convenio, si bien celebrado inicialmente en el marco europeo, está destinado desde un inicio a uniformar la legislación aplicable en cada estado parte respecto a la lucha contra la *ciberdelincuencia*, previendo no solo su aplicación por los estado europeos, sino también por todo aquel que así lo pretenda, previo los pasos de ingreso a este, que el propio convenio prevé[6].

Así, es en la actualidad, el único convenio multilateral y el de mayor alcance en cuanto a países suscriptos a nivel mundial, que incluye no solo los países del Consejo de Europa, sino también países como Estados Unidos, Canadá, Australia, Japón, Chile, Paraguay, y otros, siendo 61 países quienes a la actualidad han adherido al Convenio.[7]

Este convenio, más allá de establecer las pautas de definición de los *ciberdelitos*, a los fines de uniformar la legislación de cada Estado parte, prevé un

[5] ABOSO, Gustavo Eduardo, "Derecho penal cibernético", Ed. BdeF, Buenos Aires, 2017.
[6] Convenio sobre cibercrimen, Budapest, 2001, art. 37, www.coe.int
[7] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=l8xjrZOK

capítulo dedicado a los aspectos procesales de la lucha contra la *cibercriminalidad*, definiendo las reglas que ciertas medidas de investigación requieren.

Regula de esta manera, la preservación rápida de datos informáticos almacenados, la conservación y divulgación inmediata de los datos de tráfico, el mandato de comunicación u orden de presentación, el registro y decomiso de datos informáticos almacenados y la recopilación en tiempo real de estos.

Asimismo, prevé las medidas procesales que se puedan aplicar a los delitos informáticos que el propio convenio también define, a los delitos cometidos a través de un sistema informático o a la recopilación de pruebas electrónicas de cualquier delito, lo que exhibe el alcance amplio del mismo y las transversalidad de la evidencia digital en toda investigación penal.

La recepción de este Convenio en Argentina ha sido en mayor medida en los aspectos sustanciales, esto es la definición de aquellas conductas disvaliosas como delitos, siendo la base por la que se sancionó la reforma del código penal dispuesta por ley 26.388.

Sin embargo en lo procesal la adecuación de las reglamentaciones no ha tenido el mismo auge, manteniéndose aún, la aplicación analógica de ciertos institutos tradicionales, como el registro y allanamiento o la interceptación postal o de comunicaciones telefónicas.

Así, algunos códigos procesales, como el nuevo código procesal penal de la nación, sancionado por ley 27.063 (cuya entrada en vigencia se encuentra suspendida), o los ordenamientos neuquino o mendocino han incorporado ciertas adaptaciones a las nuevas tecnologías de la información y la comunicación que permiten la adopción de medidas necesarias para la obtención de evidencia digital.

Cabe reiterar que el avance de la cibernética ha permitido mayores injerencias en distintos ámbitos de privacidad e intimidad de las personas, quedando estas mucho más expuestas frente a accesos arbitrarios por parte de las autoridades. Ello implica que se deba analizar las distintas medidas a la luz de las garantías constitucionales, que marcan un límite a las posibilidades de intrusión del investigador.

La gran cantidad de información que puede almacenarse o desprenderse de la prueba digital, al accederse a ámbitos de privacidad e intimidad que la misma investigación puede no tener interés inicial, requiere que las reglas procesales

impongan a los operadores judiciales una mayor rigurosidad de los controles a fin de autorizar el acceso y/o registro y/o secuestro de las evidencias digitales.

En este sentido, los proveedores de servicio de internet adquieren un rol vital en razón de la información que manejan y que pueden o no guardar, atento que no se encuentran obligados a hacerlo. Téngase en cuenta que muchas veces una investigación se inicia con el conocimiento simplemente de una dirección IP desde la cual se produjo una conexión y por tanto, las posibilidades de referenciar dicha dirección con una persona, depende en gran medida de la colaboración de la empresa que proveyó la misma, a fin que aporte los datos relativos al abonado como también aquellos de tráfico, o quizás de contenido, que permitan identificar al usuario o la ruta de tráfico utilizada.

La preservación de dicha información, por demás útil en una investigación, depende en consecuencia de la colaboración de dicha empresa, por lo que es necesario la regulación de canales de comunicación entre investigador y sector privado que permitan alcanzar y acceder a estos datos.

Asimismo, el registro y conservación de datos informáticos puede implicar la colaboración de proveedores de servicios, que pueden ser públicos o privados, y que pueden tener asiento en el lugar donde transcurre la investigación o, en otro país, lo que implica la necesidad de aplicar mecanismos de cooperación expeditos, en razón de la volatilidad de la evidencia digital.[8]

Finalmente, cada vez más las organizaciones criminales utilizan herramientas tecnológicas que brindan grandes niveles de anonimato, usando conexiones a través de *TOR* y generación de espacios de intercambio en el *Deep Web*.

Estos casos suelen ser los de mayor dificultad de investigación, toda vez que las conexiones suelen cambiar cada pocos minutos, conectándose desde distintos *proxys* anónimos ubicados en distintos lugares del mundo, de difícil cooperación judicial.

Particularmente en estos casos es donde se justificaría la utilización del agente encubierto digital, toda vez que a través de la misma sería posible que los investigadores ingresaran en el ámbito de confianza de las bandas de *ciberdelincuentes*, pudiendo obtener información útil para identificar a los autores por un lado y para probar los delitos por otro.

[8] SAIN, Gustavo Raúl, "Delito y nuevas tecnologías: fraude, narcotráfico y lavado de dinero por internet", Editores del Puerto, 1ª Ed, Ciudad Autónoma de Buenos Aires, 2012.

El objeto del presente trabajo será analizar los distintos medios probatorios y técnicas de investigación que ofrece la legislación argentina, tomando como punto de partida los aspectos procesales previstos en el Convenio sobre *cibercriminalidad* celebrado en la ciudad de Budapest, al que Argentina adhirió mediante ley 27.411, y a fin de determinar la actualidad de nuestro proceso frente a la evidencia digital y las nuevas tecnologías de la información y la comunicación.

Así, luego de establecer el contexto histórico e internacional respecto a la *cibercriminalidad*, donde se buscará indagar los distintos ámbitos de discusión de la temática y cuáles son las herramientas existentes, se dividirá el trabajo en cuatro capítulos más.

El primero será relativo a la preservación y conservación de los datos informáticos, donde se buscará analizar la aplicabilidad de las medidas requeridas por el Convenio de Budapest, en sus artículos 16 a 18, que establecen la necesidad que las autoridades competentes puedan requerir a los empresas proveedoras de servicios de internet la conservación de los datos almacenados cuando haya riesgo de pérdida o de modificación, o la preservación y divulgación rápida de datos de tráfico suficientes para permitir la identificación de los prestadores de servicios y de la vía por la que la comunicación se ha transmitido, o que comunique aquellos almacenados que tenga en posesión o bajo su control.

Seguidamente, se analizará la actualidad y aplicabilidad de las normas procesales argentinas respecto al registro y decomiso de datos informáticos almacenados, tomando como base las pautas previstas en el artículo 19 del Convenio de Budapest.

Teniendo en cuenta las diferencias entre la evidencia digital y la evidencia física, se tratará de determinar las posibilidades que ofrece la legislación procesal argentina para registrar o acceder a un sistema informático y obtener, de cualquier modo, los datos que sean necesarios conforme la investigación llevada a cabo. Cabe resaltar, aquí se indagará las técnicas y medios probatorios para la búsqueda y obtención de la información ya existente y almacenada que obren en algún sistema informático o dispositivo electrónico.

La recopilación y obtención de datos informáticos en tiempo real, será objeto del siguiente capítulo, en el que se buscará determinar las facultades o no de las autoridades competentes argentinas para interceptar y obtener, durante su transmisión

o envío, las comunicaciones electrónicas o telemáticas. En este capítulo, vital será la distinción entre los distintos datos informáticos, de contenido, de tráfico o relativos al abonado, en razón del grado de intromisión que implica cada uno de ellos.

Por último, atento la importancia que presenta en una investigación actual sobre delitos cibernéticos, teniendo en cuenta el grado de desarrollo de las técnicas de anonimato en el manejo de internet, se buscará analizar la figura del agente encubierto digital y las posibilidades de su implementación, según la legislación vigente en Argentina.

CAPÍTULO I

I. Contexto histórico e internacional

En el inicio de las comunicaciones mediadas por computadoras durante los años 60, diferentes tipos de conductas indebidas o ilícitas comenzaron a aparecer entre los usuarios conectados a los centros académicos y laborales de investigación de ese entonces. Con el internet "comercial" y la expansión de la *Web* surgieron nuevos peligros y amenazas para la seguridad, personas y sistemas a partir de la multiplicidad de oportunidades tecnológicas que ofrece este medio. El fenómeno de la *cibercriminalidad* no solo es abordado por los diferentes organismos gubernamentales y fuerzas de seguridad sino también por organismos internacionales, con el objetivo de fortalecer la cooperación entre países y la armonización penal de los delitos informáticos.

Altmark y Molina Quiroga[9] destacan cuatro etapas en materia de legislación penal informática. La primera a comienzos de la década del ´70, con las normas de protección de datos personales. La segunda, a comienzos de la década del ´80, vinculada a la represión de delitos económicos cometidos mediante computadoras. La tercera se ocupó de la propiedad intelectual. Y la cuarta, ya en la década de los ´90, abarcó las reformas procesales relacionadas con la adquisición, preservación y validación en juicio de la prueba en entorno digital.

En Argentina, el Código Penal data de comienzos del siglo XX, cuando esta era de la información no se iniciaba aún. Sin embargo, a partir de la década del ´90, se sancionaron leyes que ya incluían figuras penales informáticas. Tal es el caso de la Ley 24.766 de secretos comerciales (1996), la Ley 24.769 Régimen penal Tributario (1997), la Ley 25.036 de Derechos de Autor (1998), la Ley 25.326 de Protección de Datos

[9] ALTMARK, Daniel Ricardo- MOLINA QUIROGA, Eduardo "Tratado de Derecho Informático", 1ª ed., Buenos Aires, La Ley, 2012, T. III, p. 219

Personales (2000), la Ley 25.506 de Firma digital (2001), la Ley 25.520 de Inteligencia (2001), la Ley 25.930 que reformó el concepto tradicional de defraudación (2004), o finalmente la Ley 25.891 de celulares (2005).

En noviembre del año 2001 se firmó el Convenio sobre *ciberdelincuencia* en la ciudad de Budapest por los miembros del Consejo de Europa (C.O.E.- *Council of Europe*) con el objeto de llevar a cabo una política penal común destinada a prevenir la criminalidad en el *ciberespacio* y, en particular, mediante la adopción de una legislación apropiada, es decir, acorde al derecho interno de cada Estado, y la mejora de la cooperación internacional. Dicho Convenio constituye el piso mínimo a fin de estar al día en materia de delitos informáticos y de armonización legislativa al respecto.

Este Convenio ha tenido incidencia en la legislación argentina, motivando la sanción de la ley 26.388, y posteriores reformas, que incorporaron distintos tipos penales y actualizaron algunos conceptos jurídicos, en consonancia con el primero.

Ha quedado de lado, a diferencia del Convenio, una reforma en el ámbito procesal, que contenga los distintos avances tecnológicos que surgen continuamente y que permiten una mayor eficiencia en la investigación no solo de delitos informáticos propiamente dichos, sino también de delitos comunes.

En la actualidad, y por acción del uso de dispositivos electrónicos, la posibilidad de que nuestras acciones generen un registro que pueda ser recolectado y compulsado, en el momento y mucho tiempo después, es muy alta, impactando tal circunstancia en el proceso penal, encaminado a la reconstrucción de hechos históricos.

La recolección de dicha información se produce mediante los mecanismos legales que habilitan a los organismos judiciales o de investigación a entrometerse en la esfera de los datos de las personas, en pos de la búsqueda de la verdad.

El principio de libertad probatoria, que rige el proceso penal, es una expresión clara de esta finalidad, al permitir que todo hecho, circunstancia o elemento contenido en el objeto del procedimiento y, por lo tanto, importante para la decisión final, pueda ser probado y, por cualquier medio.

Sin embargo, este principio está sujeto a ciertos límites, entre ellos, los relativos a la protección de la intimidad, que permiten ciertas injerencias únicamente si cumplen con algunas condiciones formales[10].

Todos los principios limitadores del poder penal del Estado que contiene la Constitución Nacional son desarrollados y reglamentados (art 28, Constitución Nacional) en los códigos de procedimientos y leyes orgánicas judiciales. Al menos, así debe ser, por la supremacía constitucional (art. 31, Constitución Nacional) que determina la vigencia de la ley[11].

En su marco contextual, el propio Convenio sobre *ciberdelincuencia* de Budapest 2001, establece en su art. 15 que las normas de orden procesal deberán respetar las garantías constitucionales, tanto las del derecho interno de cada país, como las previstas en normas internacionales.

La referencia al respeto de las garantías individuales en el proceso penal no es casual. Las medidas que pueden adoptarse legalmente para obtener y preservar prueba digital son intromisiones graduales que hace el Estado en la esfera de la intimidad de las personas. Por tanto, a mayor intromisión en la misma, mayores deberán ser los recaudos que deberán tomarse en forma previa a su autorización, no pudiendo ser cualquier autoridad la que pueda disponer la realización de aquellas más invasivas.

En el caso de la Argentina, tal como hemos referido previamente, no ha habido una receptación de aquellas reglas procesales necesarias, conforme el avance de las nuevas tecnologías de la información y, por tanto, en la práctica, la aplicación analógica de institutos procesales ya existentes ha ganado terreno.

Sin embargo, y a pesar de la validez de dicha técnica, ella deviene peligrosa, en tanto amplía, a criterio de los operadores judiciales, los casos que el Estado puede autorizar el acceso a ámbitos de privacidad, a riesgo de vulnerar la naturaleza restrictiva y excepcional de cualquier injerencia a los mismos.

Aquí, es importante distinguir entre medidas probatorias y de coerción desarrolladas como parte de la actividad probatoria en el proceso penal, por cuanto, si bien existe un número abierto en la primera, ello no es así respecto de las segundas. Esta cuestión es importante para poder diferenciar aquellas injerencias que

[10] PETRONE, Daniel, "Prueba informática", Ediciones Didot, 1ª Ed., Ciudad Autónoma de Buenos Aires, 2014

[11] MAIER, Julio, citado en ALTMARK, Daniel Ricardo- MOLINA QUIROGA, Eduardo "Tratado de Derecho Informático", 1ª ed., Buenos Aires, La Ley, 2012, T. III, p. 468.

suponen la incorporación de pruebas, de aquellas que solo tienden a la obtención de los fines procesales y que, solo en forma mediata, responden a una finalidad probatoria[12].

Toda medida que restringe derechos está sujeta al cumplimiento de estándares de judicialidad, motivación, proporcionalidad y legalidad. Este último principio impone que cualquier intromisión en los derechos y libertades de un imputado debe estar autorizada y regulada por una ley previa, lo que implica que no pueda ser retroactiva salvo que sea más benigna.

Por tanto, la aplicación analógica de institutos procesales existentes a nuevos elementos probatorios, surgidos de las nuevas tecnologías de la información, requiere que estas fueren menos gravosas, es decir solo se permite la analogía procesal *in bonam partem*[13].

Así, mientras que la prohibición de la analogía en materia de derecho penal material se basa en que no puede haber delito ni pena sin una ley previa que los defina y prevea (principio de legalidad), lo que implica que el juez debe aplicar la ley de fondo (centralmente los tipos penales) de manera estricta (lex stricta) y no está autorizado a realizar razonamientos analógicos, en materia procesal penal, la prohibición de analogía surge del hecho de que existe un principio justamente análogo que impide aplicar una medida de coerción si no se da el tipo de coerción establecido por las normas procesales respectivas[14].

Al respecto, la Cámara Nacional de Apelaciones en lo Criminal y Correccional, ha dicho en el caso "Czarneski, Fabricio Jesús de Nazareth"[15]: "Todas esas consideraciones, y las valoradas por la Fiscal con referencias al derecho local y comparado, no pueden alterar el catálogo de disposiciones en materia de medidas de coerción que, taxativamente, establece la ley procesal. Y ello se debe a que, así como en el ámbito del Derecho Penal material existe el principio del "*nullum crimen nulla poena*

[12] BRUZZONE, Gustavo, citado en LERMAN Marcelo, "La prohibición de analogía en materia procesal penal: Nulla coactio y teoría del fruto del árbol envenenado", https://informacionlegal.com.ar, AR/DOC/812/2004

[13] PETRONE, Daniel, "Prueba informática", Ediciones Didot, 1ª Ed., Ciudad Autónoma de Buenos Aires, 2014

[14] LERMAN Marcelo, "La prohibición de analogía en materia procesal penal: Nulla coactio y teoría del fruto del árbol envenenado", https://informacionlegal.com.ar, AR/DOC/812/2004

[15] Cámara Nacional de Apelaciones en lo Criminal y Correccional, causa N° 22145 "Czarneski Fabricio Jesús de Nazareth", https://informacionlegal.com.ar, AR/JUR/4441/2003. En dicho fallo el resolutivo dijo: "I) Declarar la nulidad de la reserva de identidad de los testigos identificados como 1, 2 y 3 y, en consecuencia, declarar la nulidad parcial del auto de fs. 132, por medio del cual se citó a prestar declaración indagatoria a Fabricio Jesús de Nazareth Czarneski; de la declaración indagatoria del nombrado de fs. 178/179; y del auto de procesamiento con prisión preventiva de fs. 133/135, con los alcances indicados (arts. 167 y sigtes. del CPPN)"

sine lege", en el ámbito procesal penal existe su correlato en la "*nulla coactio sine lege*". Esto significa que, para la aplicación de medidas de coerción o de injerencia, las pautas que utilizamos de tipicidad material son, *mutatis mutandi*, de aplicación a esas medidas procesales".

En definitiva, más allá del caso concreto, en cuanto habla de un testigo de identidad reservada, lo importante de ello, es la prohibición de analogía procesal en cuanto las mismas implican una medida de coerción.

Clara relevancia tiene en la temática desarrollada en este trabajo, toda vez que los institutos procesales regulados, tienen un alcance distinto o menor al que por las nuevas tecnologías se puede acceder.

La eficacia de una investigación criminal, no puede justificar, en desmedro de las garantías constitucionales, diversas injerencias al ámbito privado fundadas en reglas procesales que no regulan la misma.

El art. 18 de la Constitución Nacional argentina dispone expresamente que "el domicilio es inviolable, como también la correspondencia epistolar y los papeles privados; y una ley determinará en qué casos y con qué justificativos podrá procederse a su allanamiento y ocupación", lo que necesariamente debe correlacionarse con el art. 19, donde se garantiza la posibilidad de desenvolver libremente una esfera de intimidad individual.

Estas normas de nuestra Carta Magna, tienen sus correlatos en Declaración Universal de Derechos Humanos[16], Pacto Internacional de Derechos civiles y políticos[17] y Convención Americana sobre Derechos Humanos[18], pactos internacionales de jerarquía constitucional en la Argentina.

Esta protección de la intimidad se extiende no solo a los ámbitos físicos referidos, sino también a otros en que la persona desarrolle concretamente su existencia, sea de modo permanente o accidental. Por ello, se extiende a todas las comunicaciones que el propio individuo muestra su voluntad de sustraerlas del

[16] Art. 12: "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".
[17] Art. 17.1: "Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación"
[18] Art. 11.2: "Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia en su domicilio o en su correspondencia…"

conocimiento de terceros o, a los documentos privados, sean estos materiales o informáticos o, a la propia vestimenta o el cuerpo.

Es de esperar que en la regulación normativa del derecho, se vire en el sentido apuntado, dislocando la protección y, en su remplazo, se creen normas que definan el contenido nuclear de la intimidad, tanto en la tipología penal sustantiva, penalizando determinados ataques a la intimidad, cualquiera sea el sitio, medio o registro donde ésta se exprese, como también definiendo con el mismo enfoque las normas procesales relativas a la invasión, adquisición y utilización de pruebas obtenidas de ese espacio ambiental[19]

El desarrollo tecnológico, unido a los nuevos desafíos del control y del mercado, en *megaurbes*, presenta un panorama mucho más complejo. La invasión sutil a la intimidad, poco perceptible para el afectado, resulta al final, más brutal con la ilimitada capacidad de almacenamiento e interrelación de datos logrados en sistemas computarizados y en el espacio virtual. Los sistemas de captación de señal de la telefonía celular y los sistemas de búsquedas por programas computarizados permiten reconstruir no sólo la red de contactos de personas, sino los sitios en que estuvo y sus desplazamientos, con indicación de días y horarios. También se afirma que es posible reconstruir comunicaciones pasadas mediante examen de mensajes de texto. Y así es de esperar que los modos de invasión de la intimidad se sigan desarrollando en un espiral de aceleración en relación directamente proporcional al avance tecnológico. Por esta razón el orden normativo tiene que desplazar la atención, desde la actual regulación proteccionista centrada en los medios y sitios donde se expresa la intimidad, hacia una punitiva que atienda a la intimidad misma[20].

A. El rol de la Organización de Naciones Unidas en la lucha contra el delito informático

La Organización de Naciones Unidas, como foro político de discusión, se ha ocupado de uno de los problemas de mayor importancia en la agenda internacional, cual es, los delitos de alta tecnología y aquellos relacionados con las redes informáticas.

La Comisión de Prevención del Delito y Justicia Penal es el órgano principal del sistema de las Naciones Unidas para formular políticas y

[19] FLEMING Abel y LOPEZ VIÑALS Pablo, "Garantías del imputado", Rubinzal-Culzoni, 1ª ed, 2007
[20] FLEMING Abel y LOPEZ VIÑALS Pablo, ob. cit.

recomendaciones sobre cuestiones de la justicia penal, incluida la trata de seres humanos, los crímenes transnacionales y los aspectos de la prevención del terrorismo. La Comisión supervisa el uso y la aplicación de las normas de las Naciones Unidas relativas a estas cuestiones y guía el desarrollo de políticas para abordar nuevas cuestiones.

La Comisión ofrece a los Estados miembros un foro para el intercambio de conocimientos, experiencias e información para el desarrollo de estrategias nacionales e internacionales. También coordina esfuerzos con otros organismos de las Naciones Unidas con mandatos en materia de prevención del delito y justicia penal, como el Consejo de Seguridad, la Conferencia de Estados Partes en la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y la Conferencia los Estados Partes en la Convención de las Naciones Unidas contra la Corrupción.

Cada cinco años, la Comisión coordina la ejecución del Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal[21].

- En el año 2010, en el 12º Congreso de Naciones Unidas sobre Prevención del Delito y Justicia Penal**,** se trabajó un documento, titulado "Novedades recientes en el uso de la ciencia y la tecnología por los delincuentes y las autoridades competentes en la lucha contra la delincuencia, incluido el delito cibernético"[22].

Este trabajo comienza planteando los retos que enfrentan la investigación, determinación y sanción del delito cibernético.

En primer lugar menciona, la incertidumbre sobre el alcance del problema, en razón de la falta de información fidedigna sobre el mismo, debido a las características propias del delito.

Las estadísticas relativas a la delincuencia no suelen mencionar los delitos por separado, y las pocas estadísticas que existen sobre el impacto del delito cibernético no son, por lo general, lo suficientemente detalladas como para proporcionar a los responsables de la formulación de políticas información fidedigna sobre la escala o el alcance de los delitos. Sin esos datos, es difícil cuantificar el impacto del delito cibernético en la sociedad y elaborar estrategias para combatirlo

[21] https://www.unodc.org/lpo-brazil/es/crime/index.html
[22] http://www.un.org/es/comun/docs/?symbol=A/CONF.213/9

A continuación, destaca el informe el carácter transnacional del delito cibernético. Es fácil enviar correos electrónicos con un contenido ilegal a destinatarios de una serie de países, incluso cuando el remitente inicial y el destinatario final se encuentran en el mismo país o cuando ya sea el remitente o el destinatario utilizan un servicio de correo electrónico prestado por un proveedor situado fuera del país.

Como consecuencia del principio fundamental de la soberanía nacional, según el cual no pueden realizarse investigaciones en territorios extranjeros sin el permiso de las autoridades locales, la cooperación estrecha entre los Estados involucrados es crucial para la investigación de los delitos cibernéticos.

Otra dificultad importante se relaciona con el poco tiempo disponible para llevar a cabo las investigaciones de esos delitos, ya que las pruebas suelen suprimirse automáticamente y/o en pocos segundos, por lo que procedimientos oficiales prolongados pueden obstaculizar seriamente las investigaciones.

Otro desafío planteado deviene de las diferencias de enfoques nacionales, ya que un efecto práctico de la arquitectura en la red de Internet es que los autores de los delitos cibernéticos no necesitan estar presentes en el lugar del delito. Por ello, impedir la existencia de refugios seguros para los delincuentes se ha convertido en un aspecto clave de la prevención de esta delincuencia.

Dos criterios diferentes para hacer frente a la dimensión transnacional del delito cibernético y a las diferencias en las normas jurídicas que destaca el informe.

Una, es desarrollar y normalizar la legislación pertinente. El "Documento" destaca varias iniciativas, entre ellas una ley modelo elaborada por el Commonwealth en 2002 o el Convenio sobre *ciberdelincuencia* elaborado por el Consejo de Europa en el año 2001.

Y la otra, es mediante la territorialización de internet, es decir, a través de la restricción al acceso a determinada información. Desde el punto de vista técnico, los proveedores de acceso pueden en general controlar si el sitio *web* al que el usuario desea entrar está en una lista negra y bloquear esa entrada.

El último reto planteado por el Informe, surge del hecho que los delitos cibernéticos son obra de personas aisladas, sino también, de grupos delictivos organizados, distinguiendo dos categorías de actuación de estos grupos: la utilización de

la tecnología de la información por los grupos delictivos organizados tradicionales, y la comisión de delitos cibernéticos por grupos delictivos organizados.

En el caso de los primeros, están utilizando la tecnología de la información para coordinar sus actividades y aumentar su eficacia en la comisión de delitos, es decir, se utiliza para mejorar la eficiencia del grupo delictivo organizado en su campo de actividad tradicional.

En relación al segundo grupo, debe tenerse en cuenta ciertas características: suelen tener una estructura más flexible y abierta, permitiendo nuevos miembros por periodos limitados; son frecuentemente grupos más pequeños; y los miembros se comunican exclusivamente de modo electrónico.

Finalmente, el Informe refiere que las organizaciones internacionales y regionales, los gobiernos nacionales, los organismos encargados de hacer cumplir la ley y las organizaciones no gubernamentales están abordando el delito cibernético de diferentes formas, que incluyen medios legislativos, de aplicación de la ley y de fomento de la capacidad.

Sobre la elaboración de leyes, cabe decir que ellas han tenido auge a nivel nacional o regional, pero no se ha hecho nada para armonizar la legislación a nivel mundial. El Convenio sobre Ciberdelincuencia, celebrado en el marco del Consejo de Europa, es el instrumento de mayor alcance, ya que no solo tiene validez para los Estado miembros, sino que aquellos Estado que no son miembros también puede adherir y ratificar el mismo.

Además de necesitar instrumentos jurídicos, la aplicación de la ley depende en gran medida de la disponibilidad de instrumentos de investigación tales como programas informáticos forenses (para reunir pruebas, registrar las pulsaciones de teclado y descifrar o recuperar ficheros suprimidos) y programas informáticos o bases de datos de gestión de la investigación (por ejemplo, con valores *hash* para imágenes de pornografía infantil conocidas). En los últimos años se han desarrollado varios instrumentos de ese tipo y se sigue trabajando en ello.

Por último, puesto que investigar los delitos cibernéticos y enjuiciar a las personas involucradas en ellos plantea dificultades especiales, es importante impartir capacitación a los funcionarios encargados de hacer cumplir la ley, los fiscales y los jueces.

- En el año 2015, en el 13º Congreso de Naciones Unidas sobre Prevención del Delito y Justicia Penal, celebrado en Doha, Qatar, se trabajó un documento, titulado "El fortalecimiento de las respuestas de prevención del delito y justicia penal frente a las formas de delincuencia en evolución, como la *ciberdelincuencia* y el tráfico de bienes culturales, incluidas las lecciones aprendidas y la cooperación internacional"[23].

En este informe de antecedentes se describen a grandes rasgos los aspectos comunes y específicos de las respuestas en materia de prevención del delito y justicia penal frente a la *ciberdelincuencia* y el tráfico de bienes culturales, dos ejemplos destacados de delincuencia en evolución que han adquirido cada vez más relevancia como consecuencia de la globalización y el desarrollo de la tecnología de la información. Si bien los grupos de delincuencia organizada han sabido aprovechar las oportunidades que ofrecen estos fenómenos, es preciso adoptar medidas eficaces para conocer mejor la escala, las raíces y el *modus operandi* en la comisión de delitos conexos, elaborar estrategias eficaces de prevención, mejorar el intercambio de información, y reforzar los marcos nacionales y la cooperación internacional entre Estados Miembros.

Uno de los principales aportes hechos por este documento, es la definición de *ciberdelito*, que son aquellos en los que los datos o sistemas informáticos son el objeto contra el que se dirige, así como los actos en que los sistemas informáticos o de información forman parte del *modus operandi* del delito.

Sin embargo, en términos generales, la frontera entre la *ciberdelincuencia* y la delincuencia convencional resulta cada vez más difusa. Con el uso cada vez más generalizado de dispositivos electrónicos y de la conectividad global en la vida cotidiana, las pruebas, como los mensajes de texto, los mensajes electrónicos, los datos de navegación por Internet o de redes sociales, son cada vez más habituales en muchas investigaciones penales tradicionales.

Los instrumentos forenses digitales y los requerimientos a proveedores de servicios electrónicos a que se recurre en estos casos, así como muchos de los problemas y buenas prácticas de investigación, son a menudo los mismos que en los casos de *ciberdelincuencia*. En ese sentido, si bien este documento de antecedentes se centra en actos que habitualmente se consideran casos de ciberdelincuencia, muchas de

[23]https://www.unodc.org/documents/congress/Documentation/A-CONF.222-12_Workshop3/ACONF222_12_s_V1500666.pdf

sus observaciones y conclusiones se aplican de manera más amplia a las pruebas electrónicas en general.

Uno de los principales elementos impulsores de la delincuencia contemporánea y del uso creciente de pruebas digitales es el desarrollo de la conectividad electrónica global. Hoy existen casi 3.000 millones de usuarios de *Internet*, cerca del 40% de la población mundial. El acceso mayoritario a *Internet* es por medio de banda ancha móvil, que llega aproximadamente al 32% de la población mundial, casi cuatro veces la cifra de 2009[24].

La tecnología no deja de progresar, y los instrumentos forenses y las técnicas actuales de investigación de la ciberdelincuencia afrontan retos inimaginables hace apenas una década. Las nuevas redes descentralizadas y anónimas, a menudo conocidas como la "*Internet* profunda", funcionan junto con la convencional. Algunos servicios como *The Onion Router ("Tor")* hacen que resulte muy difícil para las autoridades encargadas de hacer cumplir la ley determinar el origen de las comunicaciones electrónicas o la identidad de las páginas web de "servicios ocultos". Estos pueden usarse para albergar anónimamente mercados ilícitos de drogas, armas o pornografía infantil. Algunas de esas redes ofrecen también la posibilidad de almacenar datos de forma descentralizada y encriptada entre los distintos "nodos" participantes. Los documentos o imágenes electrónicos así almacenados son también prácticamente inaccesibles para las autoridades encargadas de hacer cumplir la ley. Las implicaciones de esas tecnologías son profundas y plantean la cuestión de cómo lograr que las respuestas de las autoridades se mantengan a la par con el ritmo de innovación de la ciberdelincuencia.

Una de las formas de prevenir y afrontar la *ciberdelincuencia*, además de la capacidad de medir la misma, también deben adoptarse respuestas nacionales a la ciberdelincuencia de carácter legislativo y normativo, en ámbitos como la tipificación de delitos y las competencias procesales; la capacidad de las autoridades encargadas de hacer cumplir la ley y de la justicia penal para investigar la *ciberdelincuencia*, las técnicas forenses digitales y el manejo de pruebas electrónicas; los mecanismos judiciales de cooperación internacional en asuntos penales; y la prevención de la misma

[24] https://www.unodc.org/documents/congress/Documentation/A-CONF.222-12_Workshop3/ACONF222_12_s_V1500666.pdf

Las políticas, estrategias y leyes nacionales relativas a la ciberdelincuencia son un punto de partida importante para establecer el marco general y las prioridades de las respuestas a ese delito. El archivo de datos en línea sobre *ciberdelincuencia* de la UNODC (que entrará en funcionamiento en 2015) contendrá detalles acerca de las estrategias nacionales de unos 50 países, y abarcará ámbitos como la sensibilización acerca de la delincuencia informática, la cooperación internacional, la capacidad de aplicación de la ley, la legislación, la prevención y las alianzas público-privadas.

Pero además de disposiciones relativas a la tipificación de delitos y a las competencias procesales, los instrumentos existentes también pueden contener mecanismos de cooperación internacional para la investigación y la persecución transfronteriza de la ciberdelincuencia. Este es un ámbito que plantea cada vez más dificultades a las autoridades encargadas de hacer cumplir la ley. La llegada de la computación en la nube y del intercambio y almacenamiento de datos entre pares significa que, aun cuando en teoría sea posible localizar unos datos informáticos concretos en un momento determinado, dichos datos pueden existir en múltiples copias, pueden ser distribuidos entre múltiples dispositivos y lugares, y pueden ser trasladados a otra localización geográfica en cuestión de segundos

Algunos proveedores de servicios de almacenamiento de datos, como los de servicios electrónicos o de computación en la nube del sector privado, pueden estar obligados por ley a conservar copias de los datos durante cierto tiempo, y por regla general entregarán los datos a las autoridades responsables de la aplicación de la ley en cumplimiento de una orden judicial o de otro proceso legal establecido a tal efecto. No obstante, cuando el prestador o los datos se encuentran fuera de la jurisdicción encargada de la investigación, dicho proceso legal implica a menudo el uso de procedimientos oficiales y lentos de asistencia judicial recíproca entre Estados.

Innovaciones como la inclusión de un módulo de pruebas digitales en la nueva versión del Programa para Redactar Solicitudes de Asistencia Judicial Recíproca de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) pueden contribuir a agilizar los procedimientos de asistencia judicial recíproca relacionados con pruebas electrónicas. La implicación de entidades como el Complejo Mundial para la Innovación de la INTERPOL y el Centro Europeo contra la Delincuencia Informática (EC3) de la Oficina Europea de Policía (Europol) en tareas de coordinación

y apoyo de las investigaciones transnacionales, por ejemplo, facilitando el intercambio de información entre fuerzas del orden de distintas nacionalidades, podría resultar especialmente importante.

Por último, es fundamental el desarrollo de la capacidad de los sistemas nacionales de aplicación de la ley y de la justicia penal, ya que muchos de los países aun no disponen de recursos suficientes o tienen problemas de capacidad. No cabe duda que el desarrollo de la capacidad de los encargados de hacer cumplir la ley y de la justicia penal frente a la ciberdelincuencia será un proceso continuo, en vista al ritmo que siguen evolucionando las innovaciones técnicas y delictivas.

B. Convenio sobre la Ciberdelincuencia

En noviembre del año 2001 se firmó el Convenio sobre *ciberdelincuencia* en la ciudad de Budapest por los miembros del Consejo de Europa (C.O.E.- Council of Europe) con el objeto de llevar a cabo una política penal común destinada a prevenir la criminalidad en el ciberespacio y, en particular, mediante la adopción de una legislación apropiada, es decir, acorde al derecho interno de cada Estado y la mejora de la cooperación internacional.

Si bien se suscribe en el marco del Consejo de Europa, el Convenio establece a través de sus arts. 36 y 37[25] la posibilidad a estados no miembros a ser invitados a participar, siendo vital para el éxito de los objetivos de la Convención, la inclusión de todos los países, aun cuando no hayan suscrito inicialmente el mismo.

La República Argentina recibió la invitación a participar en la 5ta Conferencia Anual sobre *Ciberdelitos* del Consejo de Europa en marzo de 2010.

Esto vino como consecuencia de la Ley 26.388 (2008) que incorporó distintos delitos informáticos en el Código Penal Argentino, de conformidad a las disposiciones del Convenio.

Esta reforma significó no solo una actualización de nuestra legislación penal sustantiva, sino que implica un cambio de concepción en muchos

[25] Art. 37 del Convenio sobre Ciberdelincuencia, Budapest 2001: "*A partir de la entrada en vigor del presente Convenio, el Comité de Ministros del Consejo de Europa podrá, previa consulta con los Estados contratantes del Convenio, y habiendo obtenido su consentimiento unánime, invitar a adherirse al presente Convenio a cualquier Estado que no sea miembro del Consejo de Europa y que no haya participado de su elaboración. La decisión se adoptará respetando la mayoría establecida en el art. 20.d del Estatuto del Consejo de Europa y con el voto unánime de los representantes de los Estados contratantes con derecho a formar parte del Comité de los Ministros. (...)*"

conceptos legales que el avance tecnológico había dejado obsoletos, así como también la incorporación de nuevos tipos penales y la actualización de algunos ya existentes.

En este camino trazado por la Argentina, se creó, mediante resolución conjunta de la Jefatura de Gabinete de Ministros (866/2011) y del Ministerio de Justicia y Derechos Humanos (1500/2011), una comisión Técnica Asesora en materia de *Cibercrimen*, en razón de la necesidad de revisar también las reglas procesales en relación a la investigación de los delitos informáticos, y con el objeto de armonizar las mismas con el Convenio de Budapest.

A tal fin, elaboró un anteproyecto de reforma del código procesal penal de la nación, realizando las adaptaciones conforme las garantías individuales consagradas en nuestra Constitución Nacional e invitando a la Ciudad Autónoma de Buenos Aires y a las Provincias a que revisen sus legislaciones provinciales.

En diciembre de 2017, a través de la ley 27.411[26] se aprobó el Convenio sobre Ciberdelito del Consejo de Europa, aunque con algunas reservas puntuales que se detallan en el artículo 2 de dicha ley.

En lo que hace objeto de este trabajo, la República Argentina hizo reserva respecto el art. 22.1.d[27], manifestando que no regirá en su jurisdicción por

---

[26] https://www.boletinoficial.gob.ar/#!DetalleNormaBusquedaAvanzada/176168/20171215
Ley 27411 "artículo 1°.- Apruébase el Convenio sobre ciberdelito del Consejo de Europa, adoptado en la ciudad de Budapest, Hungría, el 23 de noviembre de 2001, que consta de cuarenta y ocho (48) artículos cuya copia auténtica de su traducción al español así como de su versión en idioma inglés, como anexo i, forma parte de la presente. artículo 2°.- al depositarse el instrumento de adhesión deberán efectuarse las siguientes reservas:
a) La república Argentina hace reserva del artículo 6.1.b. del Convenio sobre ciberdelito y manifiesta que no regirá en su jurisdicción por entender que prevé un supuesto de anticipación de la pena mediante la tipificación de actos preparatorios, ajeno a su tradición legislativa en materia jurídico penal.
b) La república Argentina hace reserva de los artículos 9.1.d., 9.2.b. y 9.2.c. del Convenio sobre ciberdelito y manifiesta que estos no regirán en su jurisdicción por entender que son supuestos que resultan incompatibles con el código penal vigente, conforme a la reforma introducida por la ley 26.388.
c) La república Argentina hace reserva parcial del artículo 9.1.e. del Convenio sobre ciberdelito y manifiesta que no regirá en su jurisdicción por entender que el mismo sólo es aplicable de acuerdo a legislación penal vigente hasta la fecha, cuando la posesión allí referida fuera cometida con inequívocos fines de distribución o comercialización (artículo 128, segundo párrafo, del código penal).
d) La república Argentina hace reserva del artículo 22.1.d. del Convenio sobre ciberdelito y manifiesta que no regirá en su jurisdicción por entender que su contenido difiere de las reglas que rigen la definición de la competencia penal nacional.
e) La república Argentina hace reserva del artículo 29.4 del Convenio sobre ciberdelito y manifiesta que no regirá en su jurisdicción por entender que el requisito de la doble incriminación es una de las bases fundamentales de la ley de cooperación internacional en materia penal n° 24.767 para el tipo de medidas de cooperación previstas en artículo y numeral citados."

[27] file:///C:/Users/Juan%20Pablo/Downloads/5446875A01%20(1).pdf; Ley 27.411- Anexo 1 "Convenio sobre ciberdelito": "Artículo 22 - Competencia 1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para atribuirse la competencia respecto a cualquier infracción penal establecida en los artículos 2 a 11 del presente Convenio, cuando la infracción se haya cometido: a.- en su territorio;b.- a bordo de una nave que enarbole el pabellón de ese Estado; c.- a bordo de una aeronave

entender que su contenido difiere de las reglas que rigen la competencia penal nacional. Es decir, no rige la regla de competencia establecida en el Convenio, que refiere que cuando el delito haya sido cometido por uno de sus súbditos, si la infracción es punible penalmente en el lugar donde se ha cometido o si la infracción no pertenece a la competencia territorial de ningún Estado.

Finalmente, Argentina fue ratificada el 05 de junio de 2018 y por tanto el Convenio entra en vigencia el 01 de octubre de 2018[28].

a. Sobre los aspectos procesales del Convenio sobre Ciberdelincuencia

Analizando el mencionado Convenio, este se divide en tres capítulos:

I.- Relativo a la terminología, en el cual desarrolla los conceptos de sistema informático, "datos informáticos", "proveedor de servicios", y "datos relativos al tráfico".

II.- Relativo a las medidas que deben adoptar los estados nacionales, distinguiendo asimismo tres secciones:

1.- Derecho penal sustantivo, en el cual adopta distintas definiciones, entre ellas la de "sistema informático" (todo dispositivo aislado o conjunto de dispositivos interconectados o unidos, que aseguran, en ejecución de un programa el tratamiento automatizado de datos) y establece distintos tipos penales que deben ser incorporados a las legislaciones nacionales (infracciones contra la confidencialidad, la integridad y la disponibilidad de datos y sistemas informáticos, infracciones informáticas, e infracciones relativas a la pornografía infantil y a la propiedad intelectual).

2.- procesal, en el cual establece distintos procedimientos que los Estados deben adoptar, tales como la conservación de datos informáticos almacenados o el secuestro y decomiso de los mismos o la recolección en tiempo real de datos informáticos

3.-jurisdicción.

---

inmatriculada en ese Estado; d.- por uno de sus súbditos, si la infracción es punible penalmente en el lugar donde se ha cometido o si la infracción no pertenece a la competencia territorial de ningún Estado"

[28] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=yozk7qyT

III.- Relativo a la cooperación internacional, en el cual el Convenio establece los principios generales relativos a la cooperación internacional, a la extradición, a la colaboración y a las medidas cautelares.

Es interés de este trabajo analizar la sección 2 ("Derecho Procesal") del Capítulo II ("Medidas que deben adoptar los Estados nacionales") de este Convenio, destinado a las adecuaciones que cada Estado debe realizar respecto de sus propias legislaciones.

- En esta sección, más allá de los parámetros que establece para que cada parte modifique su legislación, el Convenio destaca dos cuestiones fundamentales:

Por un lado, estas modificaciones procesales se deben aplicar no solo a los delitos informáticos, sino también a cualquier otro delito cometido a través de un sistema informático y a la obtención de prueba electrónica de cualquier delito (art. 14 del Convenio sobre la Ciberdelincuencia, Budapest 2001).

El Convenio dispone dos excepciones que limitan el amplio ámbito de aplicación referido. En primer lugar, la facultad de interceptar los datos relativos al contenido deberá estar limitada a una serie de delitos graves que serán determinados por la legislación nacional (art. 21 del Convenio sobre la Ciberdelincuencia, Budapest 2001). Y en segundo lugar, la facultad de obtener en tiempo real datos relativos al tráfico, debe ser aplicada solo a aquellos delitos previstos en la reserva, siempre que esta no sea más restringida que la serie prevista en el art. 21 (art. 20 del Convenio sobre la Ciberdelincuencia, Budapest 2001)[29]

Y por el otro, establece como salvaguardia el marco legal que las legislaciones procesales no deben trasponer, cual es una protección adecuada de los derechos humanos y las libertades individuales, el respeto de los Pactos suscriptos en la materia y principalmente el principio de proporcionalidad (art. 15 del Convenio sobre la Ciberdelincuencia, Budapest 2001).

Es decir, si bien cada Estado Parte debe introducir normas de derecho procesal, sujetas al plexo normativo de cada Parte, estas deben incluir ciertas condiciones y salvaguardias que el Convenio fija, en razón de la diversidad de culturas y sistemas jurídicos, a fin que haya un equilibrio entre las mismas.

[29] ALTMARK, Daniel Ricardo- MOLINA QUIROGA, Eduardo "Tratado de Derecho Informático", 1ª ed., Buenos Aires, La Ley, 2012, T. III, p. 214/490.

La República Argentina ha suscripto sobre la materia la Declaración Americana sobre los Derechos y Deberes del Hombre, la Declaración Universal de Derechos Humanos, la Convención Americana sobre Derechos Humanos, el Pacto Internacional de Derechos económicos, sociales y culturales, todos los cuales tienen jerarquía constitucional. El respeto de dichas normas debe guiar las modificaciones procesales conforme establece el Convenio como salvaguardia.

Sobre el principio de proporcionalidad, cada Parte deberá aplicarlo conforme su derecho interno. Sin perjuicio de ello, lo mencionado previamente respecto de los artículos 20 y 21 son ejemplos de dicho principio.

En este sentido, muchas de las medidas procesales que el Convenio establece, implican una injerencia sobre la privacidad o intimidad de las personas, motivo por el cual resulta vital que el principio de proporcionalidad guíe las mismas, en función de la naturaleza de delito y el grado de intromisión de estas.

CAPÍTULO II

II. Conservación y revelación de datos informáticos

El avance de las tecnologías y el uso de internet han generado que en la actualidad cualquier delito que se encuentre legislado pueda involucrar evidencia digital, no ya por tratarse de delitos informáticos propiamente dichos, sino porque esta también ganó protagonismo en cualquier tipo de delito. Hoy se puede estar investigando un homicidio y lo primero que querrá saberse es con quien conversó por última vez la víctima, si se conectó a alguna red social, o si se tomó alguna fotografía con su teléfono móvil.

De nada servirá en la actualidad contar con regulación específica de técnicas avanzadísimas de investigación si no contamos con la información necesaria para iniciar un caso, identificar a quien infringe la norma y eventualmente atribuir responsabilidad penal en el ciberespacio: los datos de tráfico del usuario.

El Convenio de Budapest define a los datos de tráfico como los relativos a una comunicación realizada por medio de un sistema informático, generados por este último, en tanto que elementos de la cadena de comunicación y que indique el origen, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente[30].

Estos difieren de los datos de contenido que se refieren al contenido comunicativo, es decir al mensaje o información transmitido por ella.

Como también difieren de los datos relativos a los abonados que consisten en cualquier información, que posea un proveedor de servicios y que se refiere a sus clientes y que permitan determinar, entre otras cosas, el tipo de servicio de

[30] Art. 1. d del Convenio sobre ciberdelincuencia, Budapest, 2001

comunicación utilizado; la identidad, dirección postal o ubicación geográfica y el número de teléfono del abonado; los datos relativos a la facturación y el pago y cualquier otra información que se encuentre disponible en virtud de un contrato de prestación de servicio[31].

La facultad de exigir la conservación de datos informáticos almacenados, quedando pendiente la posterior revelación en relación a procedimientos penales específicos, es una nueva e importante herramienta de investigación para hacer frente a los delitos informáticos y delitos cometidos a través de medios informáticos, especialmente internet.

En este sentido, Altmark y Molina Quiroga[32] destacan tres factores respecto a la importancia de esta medida.

En primer lugar, debido a la volatilidad de los datos informáticos, éstos son fácilmente objeto de manipulaciones y modificaciones, por lo que valiosas pruebas de un delito pueden desaparecer fácilmente debido a negligencias en el manejo o las prácticas de almacenamiento; a la manipulación borrado deliberado de datos con el fin de destruir pruebas, o a la eliminación sistemática de datos cuya conservación no se requiere por más tiempo.

En segundo lugar, los *ciberdelitos* y los cometidos a través de medios cibernéticos son cometidos en gran medida como resultado de la transmisión de comunicaciones a través de un sistema informático. Por ello, determinar el origen o destino de esas comunicaciones pasadas puede contribuir a dilucidar la identidad de los autores. Con el fin de rastrear esas conversaciones es necesario obtener datos relativos al tráfico de las mismas en relación con aquellas.

En tercer lugar, cuando estas comunicaciones vehiculan contenidos ilícitos o pruebas de una actividad delictiva y los proveedores de servicios conservan copias de dichas comunicaciones, como, por ejemplo, los mensajes de correo electrónico, es importante proceder a la conservación de estas, a fin de asegurar que no desaparezcan pruebas esenciales.

Un fallo de la Justicia de la Ciudad de Buenos Aires determinó que no puede entenderse a una dirección IP como un elemento integrativo de la personalidad, susceptible de ser abarcado por el derecho a la intimidad: "…una dirección

[31] Art. 18. 3 Convenio sobre Ciberdelincuencia, Budapest, 2001

[32] ALTMARK, Daniel Ricardo y MOLINA QUIROGA, Eduardo, "Tratado de derecho informático", Ed. La Ley, 1ª edición, Buenos Aires, 2012, T-III

IP que resulta ser simplemente una etiqueta numérica que identifica… una interfaz… de un dispositivo… dentro de una red que utiliza el protocolo IP… la dirección IP no resulta una característica inherente al sujeto humano que maneja una determinada computadora, ni siquiera resulta una característica fija de esa misma computadora, sino que es un elemento de conexión altamente volátil…"[33].

En similar sentido, un fallo de la Justicia mendocina, confirmado por la Suprema Corte Provincial, dijo "que la dirección IP no es un dato privado, puesto que en definitiva no es más que la identificación que la prestadora de servicio de internet le asigna a un usuario dentro de la red en un momento determinado. Es un dato que (por analogía) podría válidamente asemejarse al número telefónico que las prestadoras de servicios telefónicos les asignan a sus clientes. Dicho número, en sí mismo, no nos dice nada acerca de quién es el titular de la línea. Para poder determinarlo se impone que la información sea aportada por la empresa proveedora, o en su defecto si la guía se encuentra digitalizada se puede efectuar la búsqueda en forma directa, sin necesidad de que la empresa informe. Pero incluso, en el caso de los números telefónicos, es posible buscar a través de portales de internet de las empresas, quienes informan a quién pertenece una línea colocando solo el número telefónico"[34].

Estos fallos son importantes en relación a la distinta protección que tienen los datos informáticos al amparo de garantías fundamentales como el derecho a la intimidad y privacidad, protegidos no solo por los arts. 18 y 19 de la Constitución Nacional, sino también por tratados internacionales como la Declaración universal de los derechos humanos, la Convención americana de derechos humanos, el Pacto internacional de derechos civiles y políticos y el Convenio europeo para la protección de los derechos humanos y las libertades fundamentales.

Nadie duda respecto a la necesidad de una orden judicial fundada en el marco de una investigación determinada para obtener los datos de contenido de una comunicación. Sin embargo, este no parece ser el mismo análisis que merece la

[33] Juzgado Penal, Contravencional y de Faltas n° 14, "C., O. E. s/inf art. 128 CP", rta 30/12/14 y confirmada por Cámara PCyF de la CABA Sala II, rta. 23/4/15, citado en NEME, Catalina F., "Una mirada actual en materia de regulación de retención de datos de tráfico y conservación rápida de datos informáticos" en DUPUY Daniela y KIEFER Mariana, "Cibercrimen" Editorial BdeF, Buenos Aires, 2017.

[34] Cámara del Crimen N° 3 de 1° circunscripción judicial de Mendoza "F. c/ Flores Muñoz C. p/…", 09/06/17, con voto preopinante del Dr. Diego Lusverti; y confirmada por Suprema Corte de Justicia de Mendoza, sala II, 16/5/2018

posibilidad de retener o de conservar los datos de tráfico, o la solicitud a los proveedores de servicios de aquellos datos relativos a los abonados.

Es necesario distinguir el término conservación de la retención de datos. Si bien ambas expresiones significan de modo similar en el lenguaje común, se diferencian respecto al uso de los ordenadores. Conservar los datos significa guardar los que ya están almacenados de algún modo, protegiéndolos contra cualquier cosa que pudiera causar una modificación o deterioro de su calidad o condición actual. Retener significa guardar a partir de este momento los que están siendo generados en este momento. La retención implica acumular datos en el presente y guardarlos o mantener su posesión en el futuro. La retención es el proceso de almacenar. Por el contrario, la conservación es la actividad destinada a guardar aquella información almacenada de manera segura[35].

La principal diferencia recae en que, mientras la retención de datos relativos al tráfico se realiza previo al inicio de una investigación penal, la conservación rápida de estos exige que se efectúe en el marco de una investigación penal en curso y respecto de aquellos que ya se encuentran almacenados en algún soporte electrónico o digital, pudiendo tratarse en este caso tanto de tráfico como de contenido[36].

A. Conservación y divulgación de datos informáticos en el Convenio de Budapest y en la ley de enjuiciamiento criminal española

Una de las medidas que, el Convenio sobre *ciberdelincuencia* celebrado en Budapest en 2001 y que Argentina adhirió mediante ley 27411 del año 2017 dispone para que cada Estado Parte adopte en sus legislaciones internas, es la relativa a la conservación inmediata de datos electrónicos almacenados mediante un sistema informático, lo que incluye los de tráfico[37].

---

[35] Informe explicativo del Convenio sobre ciberdelincuencia, Budapest, 2001, punto 151, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa403

[36] NEME, Catalina F., "Una mirada actual en materia de regulación de retención de datos de tráfico y conservación rápida de datos informáticos" en DUPUY Daniela y KIEFER Mariana, "Cibercrimen" Editorial BdeF, Buenos Aires, 2017.

[37] Art. 16 del Convenio sobre Ciberdelincuencia, Budapest 2001 establece: "*1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para permitir a sus autoridades competentes ordenar o imponer de otro modo la conservación rápida de datos electrónicos específicos, incluidos los datos relativos al tráfico, almacenados por medio de un sistema informático, en particular cuando existan*

Los artículos 16 y 17 del Convenio, se refieren únicamente a la conservación de datos y no a la retención de datos. No imponen la obtención y retención de todos, incluso de algunos, de los datos recopilados por un proveedor de servicios u otra entidad en el curso de sus actividades. Las medidas referentes a la conservación se aplican a los datos informáticos que han sido almacenados por medio de un sistema informático, lo que supone que los datos ya existen han sido obtenidos y están almacenados.

La medida prevista por el artículo 16 tiene por fin preservar todos aquellos datos, que hubiere motivos para creer que son susceptibles de pérdida o modificación, hasta que la autoridad competente pueda revelarlo o transcurran noventa días, límite temporal que puede ser prorrogado por cada Estado Parte.

La conservación implica que los datos sean guardados o protegidos por quien sea destinatario de tal orden. No significa que deban congelarlos o bloquearlos, pudiendo los usuarios seguir accediendo a ellos.

Tampoco especifica el modo que han de ser conservados, quedando a criterio de cada Parte determinar la manera de conservación apropiada.

Asimismo, establece los parámetros por los cuales puede ordenarse tal medida, debiendo justificarse siempre la existencia de un riesgo que los datos existentes puedan borrarse o modificarse. Por tanto, si el periodo de peligro que ello suceda es determinado, la orden deberá incluir ese lapso temporal.

El Convenio prevé que cada Parte adopte las medidas necesarias para obligar a la persona encargada de la custodia de los datos informáticos a mantener el secreto de los procedimientos de conservación, lo que tiene una doble finalidad, por un lado, que no se alteren o borren la información objeto de conservación y, por el otro, proteger la vida privada del sujeto de la medida.

---

motivos para creer que dichos datos son particularmente susceptibles de pérdida o de modificación. 2. Cuando una Parte aplique lo dispuesto en el párrafo 1 anterior por medio de una orden impartida a una persona de que conserve determinados datos almacenados que se encuentran en poder o bajo el control de esa persona, la Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a dicha persona a conservar y proteger la integridad de los datos durante el tiempo necesario hasta un máximo de noventa días, con el fin de que las autoridades competentes puedan obtener su revelación. Las Partes podrán prever la renovación de dicha orden. 3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a la persona que custodia los datos o a otra persona encargada de su conservación a mantener en secreto la ejecución de dichos procedimientos durante el tiempo previsto en su derecho interno. 4. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en el art. 14 y 15."

Dicha confidencialidad que hace referencia el Convenio no es un tema menor, ya que muchas empresas tienen como política hacer lugar a estos requerimientos judiciales, pero al mismo tiempo dan aviso al usuario de la investigación en curso, lo que puede llegar a frustrar en ciertas ocasiones una investigación en su fase inicial, faltando el elemento sorpresa, que obstaculizaría cualquier intento del usuario de deshacerse de toda la información.

En caso de que un Estado parte necesite la conservación rápida de datos almacenados en un sistema informático que se encuentren en el territorio de otro Estado Parte, podrá requerirlo presentando una solicitud de asistencia mutua[38].

Si del cumplimiento de dicha medida, el Estado Parte requerido descubriera la participación de un proveedor de servicios de otro Estado parte, revelará rápidamente al Estado requirente los datos de tráficos suficientes para que pueda identificarse al proveedor de servicios[39]

- Seguidamente, el art. 17[40] de este Convenio establece que cada Estado Parte deberá llevar a cabo las medidas legislativas, o de otro tipo, para garantizar la conservación rápida de los datos de tráfico y asegurar la revelación rápida de estos que permitan al Estado competente identificar el proveedor de servicio, así como la vía por la que la comunicación se ha realizado.

Muchas veces la transmisión de una comunicación ha requerido la participación de más de un proveedor de servicios. Por ello, una medida de conservación para su posterior revelación por la autoridad competente puede tener por

---

[38] Art. 29 del Convenio sobre Ciberdelincuencia, Budapest 2001. El párrafo 2 establece los datos que deberán precisarse en la solicitud de conservación: "*a. autoridad que solicita la intervención; b. el delito objeto de la investigación o de procedimientos penales y una breve exposición de los hechos relacionados con el mismo; c. los datos informáticos almacenados que deben conservarse y su relación con el delito; d. toda información disponible que permita identificar al responsable de la custodia de los datos informáticos almacenados el emplazamiento del sistema informático; e. la necesidad de la medida de conservación; f. que la Parte tiene intención de presentar una solicitud de asistencia mutua con vistas al registro o al acceso por un medio similar, a la confiscación o a la obtención por un medio similar, o a la revelación de los datos informáticos almacenados.*"

[39] Art. 30 del Convenio sobre Ciberdelincuencia, Budapest 2001.

[40] Art. 17 del Convenio sobre Ciberdelincuencia, Budapest 2001 establece: "*1. Con el fin de garantizar la conservación de los datos relativos al tráfico, en aplicación del artículo 16, cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para: a. garantizar la conservación rápida de los datos relativos al tráfico, ya sean uno o varios los proveedores de servicios que hayan participado en la transmisión de dicha comunicación; y b. asegurar la revelación rápida a la autoridad competente de la Parte, o a una persona designada por dicha autoridad, de un volumen suficiente de datos relativos al tráfico para que dicha Parte pueda identificar tanto a los proveedores de servicios como la vía por la que la comunicación se ha transmitido. 2. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los arts. 14 y 15.*"

consecuencia que se pierdan datos imprescindibles, en razón que no se ordenó la conservación a la totalidad de los proveedores que participaron de la comunicación.

En este sentido, el Convenio no especifica los medios que puedan emplearse, debiendo ser cada Estado Parte quien lo establezca en forma coherente a su sistema jurídico.

El sentido de esta norma es que los Estados parte le impriman operatividad a la medida de conservación, especialmente respecto de los datos de tráfico, garantizando la revelación parcial rápida al Estado o a la autoridad competente de la información necesaria, con el objeto de identificar a los proveedores de ese servicio que intervinieron en una comunicación determinada y la vía de comunicación, con el fin de que éstos, sean uno o varios los proveedores de servicios que hayan intervenido, conserven los datos de tráfico.

Es decir, lo que se busca es que los Estados parte adopten las medidas necesarias para que quien recibe la orden de conservación y advierta que no es el único involucrado, revele esta información a quien se disponga a tal fin, a los efectos que se determine, si es necesario, adoptar otras medidas de conservación. Algunos de los mecanismos que se proponen es la emisión de una orden global que sirvan para todos los proveedores que se identifican, o la notificación en cadena de la orden de conservación[41].

- Otra medida prevista en el Convenio es la facultad de la autoridad competente de ordenar a una persona que comunique datos almacenados en un sistema informático o en un dispositivo de almacenamiento informático, o a los proveedores de servicios que aporten los relativos a los abonados con relación a tales servicios[42].

---

[41] NEME, Catalina F., "Una mirada actual en materia de regulación de retención de datos de tráfico y conservación rápida de datos informáticos" en DUPUY Daniela y KIEFER Mariana, "Cibercrimen" Editorial BdeF, Buenos Aires, 2017.

[42] Art. 18 del Convenio sobre Ciberdelincuencia, Budapest 2001 establece: "*Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a ordenar: a. a una persona presente en su territorio que comunique determinados datos informáticos que obren en su poder o bajo su control, almacenados en un sistema informático o en un dispositivo de almacenamiento informático; y b. a un proveedor que ofrezca sus servicios en el territorio de dicha Parte, que comunique los datos que obren en su poder o bajo su control relativos a los abonados en relación con dichos servicios; 2. Los poderes mencionados en el presente artículo estará sujetos a lo dispuesto por los artículos 14 y 15. 3. A los efectos del presente artículo, se entenderá por "datos relativos a los abonados" cualquier información, en forma de datos informáticos o de cualquier otro modo, que posea un proveedor de servicios y que se refiera a los abonados de sus servicios, diferentes de los datos relativos al tráfico o al contenido, y que permitan determinar: a. el tipo de servicio de comunicación utilizado, las disposiciones técnicas adoptadas al respecto y el periodo de servicio; b. la identidad, la dirección postal o situación geográfica y el número de teléfono del abonado, así como cualquier otro número de acceso y los datos relativos a la facturación y al pago, disponibles en virtud de un contrato o de un acuerdo de prestación de*

Esta disposición refiere a aquellos almacenados ya existentes, excluyendo los de tráfico o los de contenido de comunicaciones futuras. Ello implica que sea una medida menos invasiva que otras, tales como el registro o la confiscación, siendo ella una alternativa valiosa, en coherencia con el principio de proporcionalidad.

La expresión "obren en su poder o estén bajo su control" se refiere a la posesión física de los datos en cuestión en el territorio de la Parte que imparta la orden y también a situaciones en las cuales la persona no tenga la posesión física de estos que deben presentarse pero que dicha persona pueda, no obstante, controlar libremente su presentación dentro del territorio de la Parte que imparte la orden. La mera capacidad técnica para acceder remotamente a datos almacenados no constituye necesariamente control, en el significado dado en esta disposición del Convenio[43].

A continuación, la norma no contiene una referencia a la confidencialidad, a pesar de que, en el mundo electrónico, es muchas veces utilizada como una medida preliminar, precedente de otra como el registro y el decomiso o la interceptación real de datos, por lo que el secreto resulta vital para el éxito de la investigación.

Sobre la expresión "datos relativos a los abonados", el Convenio refiere a cualquier información, cualquiera sea el soporte que posea el proveedor, referida a los usuarios, que permita identificar tipo de servicio, las disposiciones técnicas adoptadas, el periodo de servicio, la identidad, ubicación geográfica, el teléfono, o cualquier información relativa al lugar donde se ubican los equipos de comunicación.

Es decir, el término abarca cualquier tipo de información relativa al uso de un servicio y al usuario de este, con excepción de los datos de tráfico o de contenido.

La información relativa a los usuarios puede ser necesaria en una investigación por dos motivos. En primer lugar, para determinar los servicios y las medidas técnicas utilizadas por el cliente y, en segundo lugar, cuando se conoce una dirección técnica, es necesario para poder establecer la identidad de la persona en cuestión.

---

servicios; c. cualquier información relativa al lugar en que se encuentren los equipos de comunicación, disponible en virtud de un contrato o de un acuerdo de prestación de servicio."

[43] ALTMARK, Daniel Ricardo y MOLINA QUIROGA, Eduardo, "Tratado de derecho informático", Ed. La Ley, 1ª edición, Buenos Aires, 2012, T-III

En estos artículos se advierte la necesidad de la cooperación del sector privado, es decir de las empresas que brindan el servicio y que, la mayoría de las veces, tienen sus casas centrales en países distintos a los requirentes.

El Convenio ha establecido que cada Estado Parte pueda facultar a las autoridades a requerir esa información útil, pero no describe el modo que tal pedimento debe ser llevado a cabo.

En la práctica diaria, la situación es solucionada mediante acuerdos formales o informales con las mismas empresas, los que muchas veces son guías elaboradas unilateralmente por el sector privado sobre la información que puede ser obtenida, bajo qué condiciones y los mecanismos para ello[44].

Esta situación implica una comunicación directa entre el Estado requirente y empresa privada, sin participación de autoridad alguna del país donde se encuentran alojados los datos, ni rogatoria internacional alguna.

El art. 32 del Convenio ha intentado dar solución al inconveniente, estableciendo que cualquier Estado parte podrá, sin autorización de otro, acceder a los datos informáticos almacenados de libre acceso público o con el consentimiento legal y voluntario de la persona autorizada para divulgarlos a través de ese sistema. Sin embargo, el avance de la tendencia de guardar información en "nubes" puede tornar limitada la regulación de casos previstos en el Convenio[45].

España, uno de los países signatarios del Convenio sobre ciberdelincuencia de Budapest, reguló a través de la ley de enjuiciamiento criminal la facultad de requerir a cualquier persona física o jurídica la conservación y protección de datos concretos incluidos en un sistema electrónico de almacenamiento que se encuentre a su disposición hasta que se obtenga la autorización judicial correspondiente para su cesión[46].

---

[44] SALT, Marcos G., "Nuevos desafíos de la evidencia digital. El acceso transfronterizo de datos en los países de América Latina", https://informacionlegal.com.ar, AP/DOC/898/2013.

[45] SALT, Marcos G., ob. cit.

[46] Ley de Enjuiciamiento criminal española, art. 588 octies dice: "*El Ministerio Fiscal o la Policía judicial podrán requerir a cualquier persona física o jurídica la conservación y protección de datos o informaciones concretas incluidas en un sistema informático de almacenamiento que se encuentre a su disposición hasta que se obtenga la autorización judicial correspondiente para su cesión con arreglo a los dispuesto en los artículos precedentes. Los datos se conservarán durante un período máximo de noventa días, prorrogable una sola vez hasta que se autorice la cesión o se cumplan ciento ochenta días. El requerido vendrá obligado a prestar su colaboración y a guardar secreto del desarrollo de esta diligencia, quedando sujeto a la responsabilidad descrita en el apartado 3 del artículo 588 ter e".*

Es importante remarcar que la ley española también regula la facultad de conservación de datos informáticos ya almacenados, que el destinatario de la orden tenga a disposición. A su vez, el requerimiento es respecto a datos concretos, lo que echa por tierra la posibilidad de pedir la conservación a futuro o mediante requerimientos genéricos.

Asimismo, cabe resaltar que la ley española dispone que puede ser el Fiscal o la Policía Judicial quien requiera la conservación y protección de información, no siendo necesario una orden judicial. Ello presenta lógica, por cuanto no existe de parte del requirente un conocimiento de dichos datos y por tanto no hay una intrusión en la privacidad del usuario de estos. Recién cuando de la investigación surja la necesidad de revelarlo y por tanto pueda justificarse el conocimiento de estos, es necesaria la orden judicial que así lo disponga.

La medida referida tiene un carácter meramente cautelar, a fin de preservar los datos que se encuentran en riesgo de pérdida, y por tanto debe ser confidencial. En este sentido, la ley española establece que el requerido vendrá obligado a prestar su colaboración ya guardar secreto del desarrollo de dicha diligencia, bajo apercibimiento de desobediencia.

Finalmente, establece dicha norma un periodo máximo de noventa días de conservación de los datos, el que puede prorrogarse por única vez hasta que se autorice la cesión o se cumplan los ciento ochenta días.

B. Retención de datos de tráfico en Argentina

Esta medida es aquella que obliga a las empresas prestatarias del servicio de internet a almacenar la información que obre en su poder referida a los datos de tráfico de los usuarios y/o abonados del servicio que se encuentra prestando por un tiempo determinado. Implica obligar a las empresas a guardar dicha información por un lapso de tiempo específico y previo al inicio de cualquier investigación para el caso que oportunamente sea requerida por alguna autoridad judicial o administrativa. Es una medida preventiva y por tanto su realización es previa a la comisión de un hecho delictivo[47].

[47] NEME, Catalina F., "Una mirada actual en materia de regulación de retención de datos de tráfico y conservación rápida de datos informáticos" en DUPUY Daniela y KIEFER Mariana, "Cibercrimen" Editorial BdeF, Buenos Aires, 2017.

Esta es la principal diferencia entre retención y conservación de datos de tráfico. Mientras esta última, debe ser mediante requerimiento expreso, en el marco de una investigación judicial concreta iniciada sobre datos ya existentes y almacenados, la retención es previa al inicio de alguna investigación y sobre los datos que se van produciendo, en tiempo real, independientemente si son requeridos por alguna autoridad en el marco de una investigación.

En Argentina se sancionó la ley 25.873[48], luego reglamentada por decreto 1563/04[49], que modificó la ley 19.978 conocida como "ley de telecomunicaciones". Dicha ley impuso a los prestadores de servicios de telecomunicaciones la obligación de disponer de los recursos humanos y tecnológicos necesarios para la captación y derivación de las comunicaciones que transmiten, para su observación remota a requerimiento del Poder Judicial o el Ministerio Público de conformidad con la legislación vigente.

También dispone que los prestadores de servicios deberán registrar y sistematizar los datos filiatorios y domiciliarios de sus usuarios y clientes y los registros de tráfico de comunicaciones cursadas por los mismos para su consulta sin cargo por parte del Poder Judicial o el Ministerio Público de conformidad con la legislación vigente, debiendo ser conservada por los prestadores de servicios de telecomunicaciones por el plazo de diez años.

Sin embargo, más allá del decreto 357/05[50] que suspendió la aplicación de la ley, en el año 2009 hubo un pronunciamiento con carácter *erga omnes* de la Corte Suprema de Justicia de la Nación (caso "Halabi")[51] que declaró inconstitucional esta norma y su reglamentación.

En este fallo la Corte nacional sostuvo que "sólo la ley puede justificar la intromisión en la vida privada de una persona, siempre que medie un interés superior en resguardo de la libertad de los otros, la defensa de la sociedad, las buenas costumbres o la persecución del crimen (Fallos 306:1892; 316:703, entre otros). Es en

[48] http://servicios.infoleg.gob.ar/infolegInternet/anexos/90000-94999/92549/norma.htm
[49] http://servicios.infoleg.gob.ar/infolegInternet/anexos/100000-104999/100806/norma.htm
[50] http://servicios.infoleg.gob.ar/infolegInternet/anexos/105000-109999/105679/norma.htm
[51] CSJN, "Halabi, Ernesto v. Estado Nacional s/amparo", 24/02/2009, www.informacionlegal.com.ar, cita online: 70051373

este marco constitucional que debe comprenderse, en el orden del proceso penal federal, la utilización del registro de comunicaciones telefónicas a los fines de la investigación penal que requiere ser emitida por un juez competente mediante auto fundado (conf. art. 236, parte 2ª, CPPN., según el texto establecido por la ley 25760), de manera que el común de los habitantes está sometido a restricciones en esta esfera semejantes a las que existen respecto a la intervención sobre el contenido de las comunicaciones escritas o telefónicas. Esta norma concuerda con el art. 18, ley 19798 que establece que "la correspondencia de telecomunicaciones es inviolable. Su interceptación sólo procederá a requerimiento de juez competente*"*.

Así, la Corte establece que para el examen de las intercepciones de las comunicaciones es necesario la aplicación de un criterio restrictivo de interpretación y en este sentido, dijo que lo que las normas de la ley 25.873 "han establecido no es otra cosa que una restricción que afecta una de las facetas del ámbito de la autonomía individual que constituye el derecho a la intimidad, por cuanto sus previsiones no distinguen ni precisan de modo suficiente las oportunidades ni las situaciones en las que operarán las interceptaciones, toda vez que no especifican el tratamiento del tráfico de información de Internet en cuyo contexto es indiscutible que los datos de navegación anudan a los contenidos. Se añade, a ello, la circunstancia de que las normas tampoco prevén un sistema específico para la protección de las comunicaciones en relación con la acumulación y tratamiento automatizado de los datos personales. En suma, como atinadamente ha sido juzgado en autos, resulta inadmisible que las restricciones autorizadas por la ley estén desprovistas del imprescindible grado de determinación que excluya la posibilidad de que su ejecución concreta por agentes de la administración quede en manos de la más libre discreción de estos últimos, afirmación que adquiere primordial relevancia si se advierte que desde 1992 es la Dirección de Observaciones Judiciales de la SIDE, que actúa bajo la órbita del poder político, la que debe cumplir con los requerimientos que formule el Poder Judicial en orden a la interceptación de comunicaciones telefónicas u otros medios de transmisión que se efectúen por esos circuitos".

Es importante destacar que la Corte se refiere a la inconstitucionalidad de esa norma de retención en virtud de los términos en los que fue

regulada, pero no establece que cualquier norma que se legisle al respecto sería inconstitucional[52].

Y vale resaltarlo porque a la fecha no ha vuelto a haber una ley en Argentina que regule esta temática, a pesar del aporte sustancial que ello podría tener en el marco de una investigación penal, donde muchas veces requerimiento judiciales de los datos de tráfico y de abonado, son respondidos por las empresas prestatarias del servicio de comunicación de manera negativa, por no guardar registros históricos de las conexiones de sus clientes.

C. Conservación y revelación rápida de datos en Argentina

La necesidad de obtener en forma rápida los datos de tráfico suficientes para determinar la ruta por la que transitó una comunicación, ha quedado evidenciada en tramos anteriores de este capítulo.

Sin lugar a duda, ante la posibilidad de pérdida o daño de un dato informático almacenado, es vital que exista una medida rápida que permita disponer la conservación de dicha información por un tiempo determinado, sin perjuicio que luego pueda o no ser requerido, según el curso de la investigación.

Esta medida se encuentra prevista en el Convenio de Budapest y en la ley de enjuiciamiento criminal española, tal cual fue expresado previamente.

Sin embargo, en Argentina no existe regulación que incorpore y reglamente tal medida como opción para los investigadores.

En este sentido, ni el código procesal penal de la Nación, ni su reforma, introducida por ley 27.063, legislan respecto a la facultad de requerir la conservación rápida de datos informáticos, desaprovechando esta última la posibilidad de incorporar una medida de sustancial aporte a una investigación de un delito informático o cometido a través de medios informáticos.

El código procesal de la provincia del Neuquén[53], al contrario de la normativa nacional, establece la posibilidad de solicitar la conservación de datos

---

[52] NEME, Catalina F., "Una mirada actual en materia de regulación de retención de datos de tráfico y conservación rápida de datos informáticos" en DUPUY Daniela y KIEFER Mariana, "Cibercrimen" Editorial BdeF, Buenos Aires, 2017

[53] Código procesal penal de la provincia del Neuquen, aprobado por ley 2784 sancionada el 24/11/2011, promulgada el 11/01/2012 y publicada el 13/01/2012. El art. 153 dice: "*Información digital. Cuando se hallaren dispositivos de almacenamiento de datos informáticos que por las circunstancias del caso hicieran*

contenidos en dispositivos de almacenamiento cuando se presuma que pueden contener información útil para la investigación, imponiendo un plazo límite de noventa días y el deber de confidencialidad del destinatario de la medida.

Si bien esta medida presenta ciertas similitudes con el Convenio de Budapest, cabe decir que no parece ser exactamente la medida regulada en esta última, por cuanto la ley neuquina regula posibilidad de conservar los datos hallados en un dispositivo de almacenamiento de datos informáticos, sean estos de contenido o de tráfico y respecto de cualquier persona, no solo los proveedores de servicio de internet, sin necesidad de acreditar el riesgo de pérdida o de daño que justifica la medida prevista en el Convenio.

Es decir, la ley neuquina solo prevé la facultad de ordenar la conservación de datos informáticos hallados ya en un dispositivo de almacenamiento y no la posibilidad de ordenar a un proveedor de servicios que conserve ciertos datos por un tiempo, ante la eventual necesidad de ser requerido oportunamente por un Juez.

En consecuencia, más allá del avance en materia de evidencia digital que regula el código procesal neuquino, se advierte la falta de regulación en Argentina de esta medida.

Cabe recordar, en este sentido, la ley de enjuiciamiento criminal española referida anteriormente, que establece como medida de aseguramiento la orden de conservación de datos a cualquier persona, física o jurídica, por un tiempo determinado o hasta que se obtenga la autorización judicial para su revelación y pone en cabeza del Ministerio Público Fiscal y de la Policía judicial la facultad de requerirla.

Es destacable que pueda ser el Ministerio Público Fiscal o la Policía judicial quienes puedan requerir esta medida, ante la necesidad de celeridad de esta, siendo contrario a su objetivo, si se tuviera que recurrir a mecanismos de orden judicial como para el registro y secuestro.

---

presumir que contienen información útil a la investigación, se procederá a su secuestro, y de no ser posible, se obtendrá una copia. O podrá ordenarse la conservación de los datos contenidos en los mismos, por un plazo que no podrá superar los noventa (90) días. Quien deba cumplir esta orden deberá adoptar las medidas necesarias para mantenerla en secreto. También podrá disponerse el registro del dispositivo por medios técnicos y en forma remota. A cualquier persona física o jurídica que preste un servicio a distancia por vía electrónica, podrá requerírsele la entrega de la información que esté bajo su poder o control referida a los usuarios o abonados, o los datos de los mismos. La información que no resulte útil a la investigación, no podrá ser utilizada y deberá ser devuelta, previo ser puesta a disposición de la defensa, que podrá pedir su preservación. Regirán las limitaciones aplicables a los documentos".

En consecuencia, ante la falta de previsión legislativa, vuelve a retomarse el principio de libertad probatoria, que consiste en la posibilidad de incorporar prueba al proceso, no solo por los medios regulados, sino también por cualquier otro que sea idóneo para el descubrimiento de la verdad, siempre que no sea contrario a las garantías constitucionales ni a la ley.

La prohibición de analogía de la ley en materia procesal, esto es, la imposibilidad de utilizar medios de prueba no regulados por ley, sostenida por algunos autores[54], es una postura extrema, nulificante de dicho principio, al dejar prácticamente vacío el principio de libertad probatoria referido.

Sin embargo, el principio de libertad probatoria no es absoluto y el límite será cuando la medida de prueba utilizada se inmiscuya en las garantías constitucionales y dicha intromisión no resulte proporcional con el fin pretendido.

D. La orden de presentación en Argentina

Puede definirse esta medida como la facultad que tiene una autoridad competente de ordenar a una persona que se encuentre en su territorio que comunique determinados datos informáticos o datos relativos a los abonados que obren en su poder o estén bajo su control, almacenados en un sistema informático o en un dispositivo de almacenamiento de datos.

Esta ha sido prevista por el Convenio de Budapest, al que Argentina adhirió mediante ley 27.411, regulando en el art. 18, la facultad de ordenar a una persona que comunique datos informáticos almacenados en un sistema informático o en un dispositivo de almacenamiento informático, o a los proveedores de servicios que aporten datos relativos a los abonados con relación a tales servicios.

En Argentina, esta medida se encuentra regulada en la mayoría de los ordenamientos procesales, siempre tratada en los capítulos referidos a la medida de secuestro.

Así, por ejemplo, en el artículo 232 del Código de procesal penal de la Nación se prevé que "en lugar de disponer el secuestro, el Juez podrá ordenar,

[54] PEREZ BARBERÁ, Gabriel, "Nuevas tecnologías y libertad probatoria en el proceso penal", ponencia llevada a cabo en el IV Encuentro de profesores de derecho procesal penal, Salta, 2009, obra citada en NEME, Catalina F., "Una mirada actual en materia de regulación de retención de datos de tráfico y conservación rápida de datos informáticos" en DUPUY Daniela y KIEFER Mariana, "Cibercrimen" Editorial BdeF, Buenos Aires, 2017

cuando fuere oportuno, la presentación de los sujetos o documentos a que se refiere el artículo anterior (art. 231 CPP Nación- "*cosas relacionadas al delito, las sujetas a decomiso, o aquellas que puedan servir como medio de prueba*"); pero esta orden no podrá dirigirse cuando fuere con personas que puedan o deban abstenerse de declarar como testigos por razón de parentesco, secreto profesional o de Estado".

En similar sentido lo prevé el Código procesal penal de Córdoba (art. 211), el del Neuquén (art. 147) o el de Mendoza (art. 224), entre otros.

Más específica es aun, la normativa procesal neuquina que prevé que a cualquier persona física o jurídica que preste un servicio a distancia por vía electrónica, podrá requerírsele la entrega de la información que esté bajo su poder o control referida a los usuarios o abonados, o los datos de los mismos[55].

En definitiva, esta medida, aunque apuntada hacia la evidencia física en la mayoría de los ordenamientos procesales, salvo el neuquino, se encuentra regulada y prevista en el ordenamiento argentino y aunque parecía olvidada, cobra nueva relevancia, con relación a la evidencia digital.

Una característica importante reside en que el objeto se refiere de modo exclusivo a datos informáticos que obren en poder o estén bajo el control del tercero ajeno al hecho ilícito, ya que la orden de presentación es solo aplicable a datos que éste ya tiene almacenados en sus sistemas. De no ser así, y requerir de él una actividad o tarea técnica previa o posterior distinta al mero suministro, estaríamos en el marco de la ejecución de otras medidas de prueba como la conservación rápida de datos informáticos almacenados o conservación y revelación de datos de tráfico o bien la obtención e interceptación en tiempo real de aquellos relativos al contenido.

Sin duda alguna, esta sólo será aplicable en tanto el tercero mantenga los datos o la información en su poder, puesto que, en ciertas ocasiones, los proveedores de servicios no conservan en sus registros datos relativos al tráfico o a los abonados, por implicar excesivos costos, sea por el volumen de su almacenamiento o la disposición de recursos técnicos y humanos a tal fin.

---

[55] Código Procesal Penal del Neuquén, artículo 153 "(…) *A cualquier persona física o jurídica que preste un servicio a distancia por vía electrónica, podrá requerírsele la entrega de la información que esté bajo su poder o control referida a los usuarios o abonados, o los datos de los mismos. La información que no resulte útil a la investigación, no podrá ser utilizada y deberá ser devuelta, previo ser puesta a disposición de la defensa, que podrá pedir su preservación. Regirán las limitaciones aplicables a los documentos*"

No se prevé en los ordenamientos procesales argentinos que, acompañado a esta medida, surja un deber de confidencialidad del destinatario de la orden de presentación, lo que sería importante, al ser muchas veces en la práctica una medida preliminar de otras que implican un nivel de coerción e intrusión mayor, pudiendo, en caso de divulgarse la realización de la medida, frustrarse aquella posterior.

La orden de presentación es, en el marco de investigaciones de hechos producidos en el entorno digital, una medida flexible y respetuosa del principio de proporcionalidad, referido este no solo a criterios de utilidad y eficiencia sino a la adecuación entre los fines comunitarios y estatales perseguidos y la intensidad de las restricciones de derechos padecidos por las personas.

Esto último tiene vinculación con la delimitación de cuáles datos pueden ordenarse su presentación, ya que la intensidad y volumen de afectación de la privacidad de cada uno es diferente. No es lo mismo requerir la entrega de datos relativos a los abonados, datos relativos al tráfico de una comunicación o datos relativos al contenido mismo, siendo estos últimos sin duda, donde mayor expectativa de privacidad hay.

Debido a ello, será también la autoridad competente que pueda ordenar la presentación de tales datos, debiendo ser el Juez en el caso de datos de contenido y pudiendo ser el Fiscal, cuando sean datos relativos al abonado.

Mayor controversia se da respecto a los datos de tráfico, por cuanto si bien, en principio, no ingresan demasiado en la esfera de reserva del sujeto investigado, ciertos es que si uno logra obtener una cantidad suficiente de ellos, puede hacerse una idea suficientemente precisa de la ubicación georreferenciada, en determinados periodos de tiempo o las características técnicas de las comunicaciones y las plataformas utilizadas, por lo que el grado de injerencia en la intimidad y privacidad pasa a ser significativo.

Por estas razones, si la cantidad y calidad de datos pretendidos en el curso de una investigación alcanzan tales características de significación, deberá necesariamente requerirse la autorización judicial, por imperio del plexo de normas internacionales, nacionales y locales que salvaguardan la información de carácter personal[56].

[56] COLEFF, Ivan, "La orden de presentación en el derecho procesal penal argentino. Necesidad de su reforma", en DUPUY Daniela y KIEFER Mariana, "Cibercrimen", Editorial BdeF, Buenos Aires, 2017

En consecuencia, en los ordenamientos regidos por el sistema acusatorio será el Fiscal quien pueda emitir la orden de presentación, con excepción de los datos relativos al contenido, o de aquellos relativos al tráfico referidos en el párrafo anterior, donde será el Juez quien pueda disponerla.

Finalmente, los ordenamientos procesales argentinos disponen una limitación a la posibilidad de ordenar la presentación de ciertos datos informáticos, al no poder dirigirse a las personas que puedan o deban abstenerse de declarar como testigo por razón de su parentesco, secreto profesional o de Estado.

Es razonable la aludida limitación, por cuanto si existe por un lado la prohibición de declarar en contra del imputado y, por el otro, la facultad de abstenerse, no entregar los documentos o los datos informáticos requeridos, importa el correcto ejercicio que tutela el interés individual. La ley protege este por encima del interés social a fin de no sacrificar la protección de la que gozan los parientes del imputado a guardar silencio cuando de aquél se trata, y también, por motivo de la profesión u oficio.

Por último, y a pesar de no ser referido expresamente en los ordenamientos procesales, también rige la limitación cuando la orden sea dirigida al imputado[57], desde que no se lo puede constreñir a que suministre prueba en su contra, conforme a la garantía del art. 18 de la Constitución Nacional.

[57] JAUCHEN, Eduardo "Tratado de la prueba en materia penal", citado en COLEFF, Ivan, "La orden de presentación en el derecho procesal penal argentino. Necesidad de su reforma", en DUPUY Daniela y KIEFER Mariana, "Cibercrimen", Editorial BdeF, Buenos Aires, 2017

CAPÍTULO III

III. Registro y decomiso de datos informáticos almacenados

Cada vez en mayor medida, los operadores judiciales y profesionales del derecho toman conciencia de la presencia y la importancia de la evidencia digital, lo que ha llevado al avance de la ciencia forense informática como rama especial dentro de la criminalística.

Si bien comparte ciertos principios con la evidencia física, tales como la minimización de cualquier contaminación del lugar del hecho, o la documentación de todo lo que se haga, la evidencia digital tiene características diferentes que responden a un paradigma distinto.

Se comparte la caracterización hecha por Leopoldo Sebastián Gómez[58], la que brevemente se expone.

La evidencia digital no ocupa espacio físico ni está completamente concentrada en un solo lugar, transcurriendo el procesamiento de información digital en un entorno volátil y distribuido.

En materia de seguridad, la evidencia digital requiere de un perímetro global, usualmente mediante técnicas de cifrado, a diferencia de la física, que necesita una medida local, como guardarse en un contenedor o sala con llave.

La evidencia digital se transmite en forma electrónica, es alterable y su difusión tiene alcance prácticamente ilimitado por sus facilidades en el envío de copias a destinatarios múltiples.

[58] GOMEZ Leopoldo Sebastián, "Evidencia Digital en la Investigación Penal" en Dupuy Daniela y Kiefer Mariana, "Cibercrimen" Editorial BdeF, Buenos Aires, 2017, p.617/635

En definitiva, surgen tres variables críticas a considerar durante las actividades de identificación y preservación de evidencia digital: temporalidad, volumen y ubicuidad. La evidencia digital es capaz de permanecer en un dispositivo de almacenamiento por segundos o bien por años, puede tratarse de un solo bit o de millones de ellos y finalmente es susceptible de estar localizada en un único dispositivo de almacenamiento o distribuido por el mundo.

Existen diferentes aproximaciones para la recolección de adquisición de evidencia digital. Una de las modalidades más tradicionales es la incautación o secuestro del hardware u objeto de almacenamiento de los datos informáticos; otra de ellas es la adquisición completa de evidencia digital en el lugar del hecho; una variante de esta última es la adquisición selectiva de evidencia digital en el lugar del hecho; finalmente existen metodologías tipo "triage" a fin de realizar una identificación de evidencia digital relevante y una posterior recolección selectiva de fuentes de evidencia digital en el lugar del hecho a través de una capacitación mínima de las fuerzas de la ley.

Cada de una de estas variantes presenta beneficios y complicaciones, teniendo en cuenta los recursos necesarios para llevar a cabo tales medidas y las posibilidades de éxito de las mismas.

Así la primera modalidad mencionada por ejemplo, no requiere de personal mayormente especializado en el área informática, ni de grandes recursos tecnológicos, al implicar simplemente la obtención física del objeto informático (hardware, Tablet, teléfono celular, etc.) y el traslado del mismo al personal especializado. Simplemente deberá el agente tener conocimiento y adecuarse a las guías y protocolos pertinentes al secuestro de un objeto y como preservarlo hasta tanto sea llevado al perito especialista que pueda analizarlo, asegurando la cadena de custodia.

Por el contrario, las restantes modalidades implican un mayor conocimiento y especialización de quien lleva a cabo la medida, así como de recursos tecnológicos, toda vez que deberá ser personal entrenado quien tome, en el lugar del hecho una imagen forense, que podrá o no ser analizada luego en laboratorio. Estas opciones presentan como virtud el hecho de disminuir los riesgos de daños que implica el traslado del objeto, pero requiere de personal sumamente entrenado y de amplios recursos tecnológicos disponibles para las labores de campo. A su vez en el caso de

adquisición selectiva en el lugar del hecho, se corre el riesgo de perder evidencia digital que puede ser relevante para la investigación, sea inculpatoria o exculpatoria.

La evidencia digital abarca prueba informática de carácter sonoro y visual, informes telefónicos, contactos telemáticos, correos electrónicos, entre otros, y exige al mismo tiempo cualidades y capacidades distintas a las que generalmente pueden encontrarse en la búsqueda de prueba en un delito ordinario. Los rastros digitales de la comisión de delitos cibernéticos no siempre pueden conservarse, en especial debido al medio comisivo utilizado. La eliminación o borrado de esa evidencia digital suele ser más sencillo que ocultar el cuerpo del delito en otros casos. Por este motivo, se han desarrollado técnicas que permiten duplicar, almacenar o copiar esa evidencia digital. La tecnología forense debe aplicarse ahora al descubrimiento de los medios utilizados y la identificación del autor que actúa, por lo general, salvaguardado por el anonimato de su dirección de IP.

Dependiendo de la naturaleza del delito, en algunos casos las variables de la investigación forense pasarán por determinar la conexión existente entre distintos usuarios que comparten material pornográfico de menores de edad, en cuyo caso la detección y la captura de imágenes de las fotos distribuidas entre el grupo de pedófilos serán determinantes para determinar la comisión de ese delito sexual, pero a la vez el secuestro de la computadora, los discos rígidos, y cualquier otro dispositivo de almacenamiento representa una condición necesaria para acreditar la tenencia con fines de comercialización

En la Argentina, las leyes procesales no incluyen dispositivos dedicados de manera exclusiva a la regulación de la investigación de la *cibercriminalidad*, más allá de las normas procesales que autorizan en trazos generales la interceptación de las comunicaciones y el secuestro de correspondencia o papeles privados (arts. 231 y ss. del CPPN; arts. 115 y 117 CPP CABA; arts. 214 y 216 CPP Córdoba; arts. 227 y ss. CPPMza, entre otros) en los términos previstos por el art. 18 de la Constitución Nacional[59].

El registro, la requisa, el allanamiento, el secuestro y la pericia son medios regulados en distintos ordenamientos legales argentinos que en la práctica han sido la base para la obtención de la prueba digital, ya que a fin de obtener la misma, a veces es necesario ingresar a un domicilio o revisar a una persona, sustraer el aparato

[59] ABOSO, Gustavo Eduardo, "Derecho Penal Cibernético", Editorial BdeF, Buenos Aires, 2017.

de almacenamiento buscado, y/o revisar el mismo, por personal especializado a fin de extraer la información necesaria.

Sin embargo, en los distintos ordenamientos procesales argentinos no se ha distinguido según la evidencia a obtener sea física o digital, lo que expone la necesidad de adaptación de la norma legal a las nuevas tecnologías y por tanto nuevos rastros, de gran utilidad en la investigación no solo de un delito informático sino también de cualquier otro tipo penal.

Al respecto, el Convenio de Budapest ha avanzado sobre la temática, disponiendo ciertas herramientas procesales que cada Estado Parte deberá aplicar en toda investigación de un delito informático, de uno cometido a través de un medio informático, o para la obtención de pruebas electrónicas de cualquier delito.

El art. 19 del Convenio establece la facultad del registro y confiscación de datos informáticos almacenados.

Así, en su párrafo 1, expresa que cada Parte deberá otorgar facultades a sus autoridades competentes a fin que ellas puedan registrar o acceder de cualquier modo a todo sistema de datos informáticos o los datos allí almacenados o todo dispositivo de almacenamiento de datos informáticos.

Registrar supone buscar, leer, inspeccionar o revisar datos. Al ampliarse esa búsqueda a "acceder de cualquier modo", se armoniza el concepto tradicional, más vinculado al allanamiento, con una terminología moderna, relativa a la informática.

Esa actualización es la que propone el Convenio, cuando la recolección de pruebas, excede lo tangible como es, por ejemplo, papeles impresos y requiere la búsqueda de datos informáticos o la revisión de herramientas tecnológicas de almacenamiento de datos.

Ambas medidas tienen el mismo fin. Pero las particulares características de un dato informático, acarrean la necesidad de nuevas disposiciones procesales en pos de la eficacia de la medida resuelta.

El modo intangible en que se encuentra almacenado, el medio físico en que los datos informáticos son almacenados (por ejemplo, el disco duro de una computadora o un pendrive), o la posibilidad de almacenamiento en un dispositivo conexo al accedido, son algunas de los elementos distintivos que requieren de nuevas formas que aseguren el éxito de la medida.

Esta disposición del Convenio se aplica a los datos informáticos almacenados, esto es que, ya existen, excluyendo la obtención en tiempo real o futura.

También prevé la facultad de acceder a un sistema informático y sus componentes conexos, o a otro sistema informático donde se considere se encuentran los datos buscados, siempre que sea accesible o disponible este sistema desde el sistema informático inicial. En esta última hipótesis, el Convenio establece la posibilidad de extensión de la medida inicialmente tomada.

Seguido prevé el Convenio en su párrafo 3, el deber de cada Estado parte de adoptar las medidas necesarias para facultar a sus autoridades competentes a confiscar u obtener de un modo similar los datos informáticos a los que haya accedido.

La confiscación de los datos informáticos obtenidos del registro, implica la facultad de obtener un sistema informático o un dispositivo de almacenamiento, realizar y conservar una copia, preservar la integridad de los datos almacenados y hacer inaccesibles o suprimir estos del sistema consultado.

Esta facultad prevista en el Convenio implica justamente obtener, extraer, prohibir su acceso o adquirir el control de cualquier modo de los datos intangibles que hayan surgido del registro.

Asimismo, ante uno de los problemas prácticos que se presenta habitualmente, el Convenio establece que la facultad de poder ordenar a toda persona que conozca el funcionamiento del sistema o las medidas aplicadas para proteger los datos informáticos, aporte la información necesaria para el registro.

Beneficios y obstáculos diversos presenta esta disposición.

Lo primero obviamente deviene de la necesidad, por el volumen de la información o, por la aplicación de medidas de seguridad de consultar a una persona que conozca el sistema informático o al administrador del mismo. El hecho que se le imponga esta obligación, puede llevar a liberarlo de alguna obligación contractual o de otra índole que obligue mantener secreto.

Sin embargo, en casos que la información a obtener, sea justamente incriminatoria de la persona consultada, esta podría ampararse en su derecho a no ser obligado a declarar en contra de sí mismo y podría negarse a proporcionar tal información. La protección de testigos o beneficios para el arrepentido o colaborador podrían ser herramientas válidas en cada derecho interno.

Esta disposición del Convenio de Budapest es importante por cuanto exhibe justamente las diferencias entre una evidencia física y una digital, a través de dos medios de pruebas tradicionales como es el registro y el secuestro de un objeto.

Así, se advierte algunas necesidades prácticas, que no surgen cuando se habla de evidencia física, tal como la posibilidad que el dato informático no se halle en el lugar registrado pero pueda accederse a través de él, lo que deviene del carácter volátil que posee el mismo, o la posibilidad que fuere necesario la colaboración de una persona que conozca las medidas de seguridad, como son las claves informáticas de acceso.

Finalmente, es importante destacar que estas facultades se encuentran sujetas a lo dispuesto por los arts. 14 y 15 del Convenio, esto es el ámbito de aplicación de las disposiciones de procedimiento, principio de proporcionalidad, y las condiciones y salvaguardias que previstas en cada derecho interno.

A. Registro o acceso de un sistema informático o de los datos informáticos allí almacenados

Tal como se expresó en el punto anterior, el Convenio, aprobado por Ley 27411, dispone que cada Estado parte adoptará las medidas necesarias para facultar a sus autoridades competentes a que puedan a registrar o acceder de cualquier modo a un sistema informático, a los datos allí almacenados o a todo dispositivo de almacenamiento.

Actualmente, el avance de las TICs permite el acceso a un dispositivo electrónico o a los datos allí almacenados, de distintos modos a los que fueron pensados décadas atrás, permitiendo no solo obtener mayores datos, sino también, utilizar menos recursos, sobre todo humanos.

A su vez, los datos informáticos no siempre se encuentran en el primer dispositivo informático registrado, sino que es necesario continuar la búsqueda en otros servidores ubicados en distinto lugar al que puede o no accederse a través del inicialmente registrado.

Estas variables investigativas, entre otras, conllevan distintos problemas, al verse confrontadas con los derechos constitucionalmente protegidos. En razón de ello, cobra relevancia aristas como la determinación de la afectación de la

intimidad, los límites y alcances, la selección de las vías legales y los requisitos para su realización, debiendo establecerse, en cada caso de acceso a datos, si implican una intromisión sobre una expectativa legítima de privacidad y, eventualmente, verificar la existencia de una norma que la autorice.

Sin dudas, la medida dispuesta por el Convenio es una medida de investigación que implica una injerencia a los derechos constitucionales de las personas, y por tanto se rige por la regla de taxatividad impuesta por el art. 30 de CADH.

El art. 18 de la Constitución nacional argentina dispone expresamente que: "…El domicilio es inviolable, como también la correspondencia epistolar y los papeles privados; y una ley determinará en qué casos y con qué justificativos podrá procederse a su allanamiento y ocupación…"; debiendo correlacionarse con el art. 19 de la misma que garantiza la posibilidad de desenvolver libremente una esfera de intimidad individual, actividad que la persona desarrolla esencialmente intramuros en su domicilio.

Estos derechos constitucionales tienen también su respaldo en la Convención americana sobre derechos humanos (art. 11.2), el Pacto internacional de derechos civiles y políticos (art. 17.1) y la Declaración universal de derechos humanos (art. 12), los que expresan que nadie será objeto de injerencias arbitrarias, ilegales y/o abusivas en su vida priva, su familia, su domicilio o su correspondencia, o ataques a su honra o reputación.

De lo expuesto surge que la protección de la intimidad pareciera extenderse a esos ámbitos físicos u otros en que la persona concretamente desarrolle ese aspecto de su existencia, ya sea de modo permanente o accidental, lo que se conoce como domicilio.

Ahora bien, como la protección de la intimidad es en forma refleja la protección de la libertad personal, lo tutelado por el derecho no se circunscribe a un espacio geográfico, sino existencial. Por ello la protección se extiende a todas aquellas comunicaciones que el propio individuo establece de un modo tal que resulta inequívoca la voluntad de sustraerlas del conocimiento de terceros[60].

En el mismo sentido, los documentos privados se encuentran amparados dentro de ese ámbito de reserva, toda vez que pueden contener datos que la

[60] FLEMING, Abel y LOPEZ VIÑALS, Pablo, "Garantías del imputado", Rubinzal Culzoni editores, 1° edición, Santa Fe, 2007

persona quiera mantener en secreto, siendo las posibilidades de almacenamiento y guarda, en la actualidad, mucho más eficaces y accesibles gracias al progreso de la informática y el desarrollo tecnológico.

En Argentina, en la mayoría de los ordenamientos procesales, no existen normas específicas que regulen el acceso a sistemas informáticos o a datos almacenados, a pesar de haberse adherido en noviembre de 2017 el Convenio de Budapest.

Sólo el Código procesal penal de la provincia del Neuquén establece que cuando se hallaren dispositivos de almacenamiento de datos informáticos que por las circunstancias del caso hicieran presumir que contienen información útil a la investigación, se procederá a su secuestro, y de no ser posible, se obtendrá una copia. También podrá disponerse el registro del dispositivo por medios técnicos y en forma remota[61].

Más allá de esta disposición neuquina, necesariamente, para acceder a los mismos se debe recurrir a institutos como el registro o allanamiento, si el sistema informático se encuentra en un lugar cerrado, o la requisa, si el mismo se encuentra en posesión de una persona.

Para diferenciar los conceptos de registro y allanamiento, cabe señalar que el registro es simplemente el acceso y búsqueda de aquellos elementos relacionados al ilícito en determinado lugar, mientras que el allanamiento es un medio destinado a superar la negativa del titular del derecho de exclusión para lograr un determinado registro. El allanamiento es un acto de coerción real limitativo de una garantía constitucional consistente en el franqueamiento compulsivo de un lugar cerrado en contra de la voluntad de quien está protegido por esa garantía, cumplido por una autoridad judicial, con fines procesales y legitimado solamente cuando se han satisfecho las formalidades impuestas por la ley ritual.

En el Código procesal de la Nación (Ley 23984), en similar sentido a las normas provinciales que lo regulan, se prevé la posibilidad de ingresar a un domicilio cuando hubiere motivos para presumir que en dicho lugar existen cosas vinculadas a la investigación de un delito, debiendo haber una orden de Juez competente que lo autorice. Incluso en casos de urgencias, las normas de rito prevén la facultad de

[61] Código procesal penal de la provincia del Neuquén, artículo 153

transmitir la orden por medios electrónicos, autorizándose en algunas regulaciones el uso de la firma digital ((art. 224 CPPN; art. 217 CPPMza).

Estas normas tienen su amparo en constituciones provinciales, como la de Mendoza, que establece en su art. 14 la necesidad de una orden escrita, motivada y determinada de juez competente y en los casos y formas que una ley determine.

La necesidad y razonabilidad que hacen procedente un allanamiento domiciliario están directamente relacionadas con la existencia de sospecha fundada o motivos suficientes de que en determinado lugar existen elementos provenientes del delito, pero estos extremos deben estar objetivamente verificados previamente con un grado de posibilidad, lo que constituirán las razones que convencerán al juez sobre la necesidad de la diligencia.

En los fundamentos de la decisión judicial, debe surgir que el juez ha verificado el grado de suficiencia de los elementos que afirmen la existencia probable de estar ante un ilícito penal, como también ante una acción penal vigente y no extinguida. A ello debe sumarse, la valoración de eficacia de la medida, esto es, la ponderación que se hace de que el allanamiento será exitoso en orden a su propósito. Finalmente, la orden judicial debe haber superado un análisis de proporcionalidad entre la entidad del delito investigado, la probabilidad concreta de la existencia del ilícito, la estimación de la eficacia ponderada de la medida, todo relacionado con la medición de lesividad que pueda provocar su cumplimiento.

De la motivación de la orden judicial se derivará también el alcance de la medida, esto es, la expresión precisa de sus límites a los que la autoridad que la ejecute se deberá ajustar, a riesgo de invalidar toda actuación o hallazgo que sea logrado ilegalmente, excediendo la autorización cuyo cumplimiento se le confiara, con más la responsabilidades de otro orden que la actuación abusiva generase.

En cuanto a la requisa personal, también se exige la existencia de una resolución fundada de que hay motivos suficientes para presumir que una persona oculta en su cuerpo cosas relacionadas al delito (art. 230 CPPN; art. 221 CPPMza). En cuanto al alcance de la inspección, ocurre lo mismo que respecto a los objetos hallados durante un registro domiciliario. Si no hubo orden de requisa, el funcionario actuante está muy limitado para intervenir y revisar el contenido de los objetos encontrados.

En definitiva, cuando lo que se pretende obtener es un dispositivo informático que se encuentra en un domicilio u oculto en una persona, sobre todo si el propósito es obtener el soporte físico de dicho dispositivo, será necesario en cada caso obtener la orden judicial respectiva.

El primer problema que se plantea es si la orden de registro domiciliario o requisa personal habilita la inspección y revisión de dicho dispositivo informático.

En este sentido, puede distinguirse algunos niveles, según el grado de vulneración de la medida: un primer nivel, devenido de la necesidad de identificar, inventariar, conservar y ubicarlos en una cadena de custodia. Ello implicaría si hablásemos de un *Smartphone* la obtención de un número de línea, de IMEI, de SIM, etc., información que no revela demasiado sobre la vida privada. Incluso, podría ser necesario para establecer el vínculo con el delito investigado revisar sobre datos contenidos en el móvil, como puede ser agenda o fotos, si ello permite saber si es de la víctima el objeto hallado.

En un segundo orden, se encuentran los datos de tráfico que son los que rodean la comunicación o al propio archivo informático (fecha y hora que fue creado, tamaño, IP, lista de llamadas si fuere un teléfono, etc.). Respecto a la solución en este caso, existen dos posturas, una que habilita al personal policial a la inspección sin orden judicial. Y la otra que considera que se encuentra comprendido por el derecho a la intimidad, al existir una expectativa razonable de no ser espiado ni controlado en orden a las personas con quienes se comunica, periodicidad, tiempo, etc., por lo que se impone la autorización judicial para su conocimiento[62].

En este sentido, Sebastián Romero[63], al referirse al registro de comunicaciones (llamada y SMS), expresó que el acceso a los datos que dichos listados proporcionan, si bien podrían constituir en alguna medida una injerencia a la privacidad, será en todo caso de un grado marcadamente menor, en comparación con la que implica la intervención de comunicaciones, medida que por tal motivo, está reservada por las leyes al magistrado de garantías. Y agrega que en el moderno diseño de la investigación penal que se ha impuesto en las provincias argentinas, que procura una clara distinción

[62] HAIRABEDIAN, Maximiliano, "El acceso a información y datos de teléfonos celulares", en DUPUY Daniela y KIEFER, Mariana, "Cibercrimen", BdeF, Buenos Aires, 2017.
[63] ROMERO, Sebastián, "Los registros de comunicaciones telefónicas ("sábanas") en la investigación penal: otro capítulo sobre la permanente tensión entre tecnología y privacidad", http://www.rubinzalonline.com.ar/index.php/doctrina/articulos/ver/739563/, visto 18/07/2018.

de roles entre órgano acusador y el juzgador, la instrucción le ha sido confiada al Ministerio Público, quien se encuentra facultado para llevar a cabo numerosos actos de prueba, entre ellos, la solicitud de registros de comunicaciones pasadas, sin que exista ningún obstáculo constitucional para ello.

En un tercer nivel se halla el contenido mismo del dato informático inspeccionado, esto es, el archivo, documento, imagen, comunicación, etc., el cual puede concluirse, que ante la mayor injerencia en la intimidad que implica, es necesaria ineludiblemente una orden judicial que lo autorice.

La posibilidad de inspección o acceso al dispositivo informático hallado en el domicilio o la persona cuyo registro fue autorizado debidamente, depende esencialmente del propósito y alcance de la propia resolución, debiendo expresarse en forma precisa si se autoriza la inspección en lo que hace referencia al segundo y tercer nivel referidos, siendo el acceso en este último caso más restrictivo aún.

Ante la menor intromisión que un registro de aquellos datos referidos en el primer nivel tiene respecto al derecho a la privacidad de la persona investigada, siempre que ello sea atinente y útil a la investigación que motivó la orden judicial, bastará la resolución judicial que permitió el ingreso al domicilio o la requisa personal para la revisión de tales datos.

Es posible afirmar que los funcionarios actuantes no están autorizados por sí para proceder a la requisa del dispositivo informático y que la orden judicial que disponga tal procedimiento deberá reunir los requisitos que tal injerencia en la privacidad exige, y que, exigen un auto fundado en la existencia de motivos bastante de sospecha y la declaración de utilidad probatoria del material que se busca.

En suma, tomando como ejemplo la obtención de un teléfono celular, la policía no podrá revisar sin autorización judicial los datos del celular amparados por el derecho a la intimidad, como mensajes, imágenes, listado de llamadas, etc. Solo podrán aquellos datos que fueren necesarios para la identificación o ubicación del dueño si fuese sustraído. Respalda esta conclusión el segundo párrafo del art. 236 CPPN que establece al igual que para la intervención de comunicaciones, que el juez podrá ordenar también la obtención de registros que hubiere de las comunicaciones del imputado o de quienes se comunicaran con él[64].

[64] HAIRABEDIAN, Maximiliano, “El acceso a información y datos de teléfonos celulares”, en DUPUY Daniela y KIEFER, Mariana, “Cibercrimen”, BdeF, Buenos Aires, 2017.

La ley de enjuiciamiento criminal española expresamente refiere que cuando con ocasión de la práctica de un registro domiciliario sea previsible la aprehensión de ordenadores, instrumentos de comunicación telefónica o telemática o dispositivos de almacenamiento masivo de información digital, la resolución del juez habrá de extender su razonamiento a la justificación, en su caso, de las razones que legitiman el acceso de los agentes facultados a la información contenida en tales dispositivos. Y agrega que la incautación de cualquiera de dichos dispositivos, aun cuando fuere su aprehensión con independencia de un registro domiciliario, no legitima el acceso a su contenido, sin perjuicio de que dicho acceso sea autorizado ulteriormente por juez competente (Ley de enjuiciamiento criminal española- art. 588 sexies a, b).

Esta norma refleja claramente la necesidad de que la orden judicial disponga específicamente el acceso al dispositivo informático hallado durante un registro domiciliario o requisa personal, no bastando los motivos iniciales de la resolución para acceder a la información contenida en tales dispositivos, lo que encuentra lógica si se comprende que este puede almacenar mucho más que un archivo físico o domicilio, siendo por tanto mayor la injerencia a la privacidad de la persona investigada.

En la actualidad, un teléfono celular, un aparato electrónico cualquiera tiene la capacidad de almacenar información, imágenes, registros o datos que pueden ser de interés para la investigación. Los datos almacenados en estos pueden ser útiles para determinar la posible intervención de terceros así como los lugares físicos (geolocalización), o sitios en las redes telemáticas que fueron visitados por el sospechoso. Obviamente, el registro y el tratamiento de esos datos deberán estar vinculados con el objeto del proceso penal, siendo inexcusable la necesidad de autorización judicial.

a. Registro de equipo informático ubicado en otro domicilio al autorizado

La situación se complejiza cuando, habiendo ingresado al domicilio, incluso accedido al dispositivo informático, se advierte o se tiene la sospecha que la información buscada no se encuentra en dicho aparato o soporte físico, sino que se encuentra alojada en otro servidor ubicado en otro domicilio o en una nube, cuyo servidor también se encuentra ubicado en otro destino.

La ley de enjuiciamiento criminal española trata también esta cuestión exigiendo una orden judicial que amplíe el alcance del registro inicialmente

ordenado. Expresamente dice: “cuando quienes lleven a cabo el registro o tengan acceso al sistema de información o a una parte del mismo…, tengan razones fundadas para considerar que los datos buscados están almacenados en otro sistema informático o, en una parte de él, podrán ampliar el registro, siempre que los datos sean lícitamente accesibles por medio del sistema inicial o estén disponibles para este. Esta ampliación del registro deberá ser autorizada por el juez, salvo que ya lo hubiere hecho en la autorización inicial.” (ley de enjuiciamiento criminal española- art. 588 sexies c, párrafo 5).

Surge de su lectura, que para la realización de dicha facultad, no solo debe haber una resolución judicial que lo autorice, sino que es imprescindible que sea accesible lícitamente desde el dispositivo inicial.

Al decir de Marcos Salt[65], quien toma como base la praxis pericial y de especialistas de las fuerzas de seguridad, prevalece la idea de que, al haberse ingresado a través de una terminal ubicada en el lugar físico alcanzado por la orden de allanamiento, la circunstancia de que la información esté alojada en un servidor en otro lugar es irrelevante. O sea, no se consideran casos en los que se viole el principio de territorialidad.

En la práctica se utiliza el criterio de "ubicación de la terminal desde la que acceden a la información"[66]. Si la terminal está en el espacio físico cubierto por la orden de allanamiento no se presta atención al lugar de la ubicación física del servidor al que están accediendo. La única excepción parece ser que el acceso a la información a la que acceden desde la terminal requiera la realización de operaciones informáticas especiales como "romper claves de acceso".

Esta regla tiene respaldo también en el propio Convenio de Budapest (art. 19 párrafo 2°) que permite extender rápidamente la orden judicial, cuando tenga motivos para creer que los datos buscados se hallan almacenados en otro sistema informático y que dichos datos son legítimamente accesibles a partir del sistema inicial o están disponibles por medio de dicho sistema inicial.

[65] SALT, Marcos G., “Nuevos desafíos de la evidencia digital. El acceso transfronterizo de datos en América latina”, www.informacionlegalonline.com.ar, AP/DOC/898/2013

[66] Daniel Petrone critica dicha regla por cuanto el dato cuya representación se visualiza en la terminal no es el mismo alojado en el servidor, puesto que es una representación del mismo y por lo tanto sus metadatos son distintos, y por cuanto, quien aloja un dato en un servidor de un determinado país, tiene la expectativa razonable de que el mismo solo podrá ser motivo de injerencia conforme las normas del país donde lo alojó. PETRONE, Daniel, “Prueba Informática”, ediciones Didot, Ciudad autónoma de Buenos Aires, 2014

Distinto es el caso si la información que se requiere, no puede accederse de forma directa sino mediante la cooperación del sector privado (*Microsoft*, G*oogle, Dropbox*, etc.), ya que surge el inconveniente si es necesario activar mecanismos de cooperación internacional, o si puede resolver contactándose a la oficina comercial de la empresa ubicada en el territorio. Esto acarrea el problema de depender del sector privado para la obtención de los datos buscados.

La situación es solucionada en la práctica diaria de las investigaciones mediante acuerdos formales o informales con las diferentes empresas y no son los mismos acuerdos ni se aplican de manera similar en todos los países de la región. En muchos casos, no se trata de "acuerdos" sino de guías elaboradas unilateralmente que el sector privado entrega a las autoridades de los diferentes países sobre la información que puede ser obtenida, bajo qué condiciones y los mecanismos para obtenerla. O sea que tanto el tipo de evidencia, los supuestos en los que es posible obtenerla y el mecanismo "procesal" son definidos por las empresas del sector privado[67].

El art. 32 del Convenio de Budapest establece que una Parte podrá sin la autorización de otra: a. Tener acceso a datos informáticos almacenados accesibles al público (fuente abierta), independientemente de la ubicación geográfica de los mismos; b. Tener acceso a datos informáticos almacenados en otro Estado, o recibirlos a través de un sistema informático situado en su territorio, si dicha Parte obtiene el consentimiento lícito y voluntario de la persona legalmente autorizada a revelárselo por medio de ese sistema informático.

Sin embargo, esta norma resulta criticable desde la práctica, especialmente el último supuesto, ya que genera dudas sobre quien es la persona autorizada y sobre la posible afectación del principio de territorialidad y soberanía al "saltearse" toda intervención del Estado nacional en el que se encuentra el servidor que aloja la información que es requerida por las autoridades de otro Estado[68].

b. Registro remoto sobre equipos informáticos

En la actualidad, no es necesario ingresar a un espacio físico para acceder a un dispositivo informático. Existe la posibilidad de acceder al mismo en forma

[67] SALT, Marcos G., ob cit.
[68] SALT, Marcos G., ob cit

remota a través de la red internet o telefónica, mediante el uso de programas espías, o por defecto de las condiciones de privacidad que el usuario establece en su máquina.

El problema que se presenta es establecer la regulación aplicable a esta injerencia a la privacidad de una persona. Nuevamente las previsiones respecto al registro domiciliario o requisa personal aparecen como alternativa análoga, ante la omisión de una norma que lo regule, pero ello contrasta contra el principio *nulla coactio sine lege*, que prohíbe la analogía en materia procesal penal, cuando de medidas de coerción se habla.

En España, la ley de enjuiciamiento criminal ha establecido que el juez competente podrá autorizar la utilización de datos de identificación y códigos así como la instalación de un *software*, que permitan, de forma remota y telemática el examen a distancia y sin conocimiento de su titular o usuario del contenido de un ordenador, dispositivo electrónico, sistema informático, instrumento de almacenamiento masivo o base de datos, siempre que persiga la investigación de delitos cometidos en el seno de organizaciones criminales, delitos de terrorismo, delitos cometidos contra menores o personas con capacidad modificada judicialmente, delitos contra la Constitución, de traición y relativos a la defensa nacional o delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación. Dicha resolución judicial deberá especificar el dispositivo objeto de la medida, el alcance de la medida, forma que se procederá y *software* a utilizar, el agente autorizado, la autorización para realizar copias de los datos obtenidos y las medidas precisas para la preservación o la inaccesibilidad o supresión de los datos informáticos. Finalmente agrega la posibilidad de autorizar la ampliación del registro cuando haya razones para creer que la información buscada se halla en otros sistema informático (Ley de enjuiciamiento criminal española- art. 588 septies a).

Es importante destacar el requisito previsto en dicha regulación, sobre que el examen a distancia debe ser realizado sin conocimiento del titular del dispositivo, sistema o dato informático. Esto sin dudas, es una diferencia sustancial respecto a las medidas que las normas argentinas prevén, como son el registro domiciliario o requisa personal, ya que en ellas la medida se realiza con conocimiento de quien puede oponer el derecho a la privacidad que está vulnerando. Claramente la regulación argentina, permite el ingreso a un domicilio, en vulneración del derecho protegido, pero no de manera oculta al titular de ese derecho. Muestra de ello es la

exigencia de algunas regulaciones de notificar los fundamentos de la resolución, aun cuando estos, por urgencia y gravedad del hecho investigado, no hayan sido exhibidos (art. 217 CPPMza).

Asimismo, implícitamente la norma española reconoce el mayor grado de injerencia de la medida, al permitir que pueda autorizarse solo en el marco de la investigación de ciertos delitos graves que taxativamente enuncia.

Ello tiene su respaldo y correlato con las previsiones del Convenio de Budapest, que establece el principio de proporcionalidad (arts. 14 y 21), al exigir la adopción de un repertorio de delitos graves, cuando lo que se pretenda es la interceptación de datos relativas a su contenido.

Se advierte, de un simple análisis, la necesidad de la reglamentación específica adecuada a los avances tecnológicos. En el presente caso, la vulneración es mucho mayor incluso a la que se acepta en un registro domiciliario, al aprovechar el uso de tecnologías para acceder a áreas de privacidad sin conocimiento del titular de ese derecho. En este sentido, cuanto más fácil y menos costoso resulte acceder a alguna de estas áreas, más debe rodearse a la misma de protecciones que eviten reducir el derecho a la intimidad a un valor nulo.

B. Confiscación u obtención de un modo similar de los datos informáticos que se haya accedido

Una vez accedido a los datos informáticos, es vital la obtención de los mismos a fin que puedan ser utilizados en la investigación e incorporados en el proceso penal.

Ya se ha expuesto en el punto anterior las vías legales para acceder legítimamente a un dispositivo informático o a los datos en él contenidos. El paso siguiente será analizar el camino y las posibilidades que surgen en relación a la obtención de los mismos, teniendo en cuenta el avance de la tecnología y de nuevas técnicas de investigación en correlato con el derecho a la privacidad protegido constitucionalmente.

En este sentido, a diferencia de una evidencia física obtenida, la digital requiere un tratamiento distinto, en razón de su volatilidad, escaso tamaño físico, aunque no de volumen de información, su dificultad para ser visualizada, la posibilidad sencilla de ser modificada, alterada o borrada, incluso remotamente.

Ello lleva que se deba adoptar recaudos distintos, como puede ser personal especializado para su obtención o para su posterior análisis en una pericia, diferentes medidas para su preservación en orden a mantener la cadena de custodia del mismo, etc.

Resulta claro que modernos instrumentos pueden contribuir a una mayor eficacia en la investigación penal y, en definitiva para la administración de justicia, pero también es claro, que el uso indebido de los mencionados mecanismos representa una seria amenaza de la vida privada de la personas, tan celosamente protegida por las normas constitucionales.

El Convenio de Budapest establece que cada Parte adoptará las medidas necesarias para facultar a sus autoridades a confiscar o a obtener de un modo similar los datos informáticos que se haya accedido. Estas medidas incluirán la facultad de confiscar u obtener un sistema informático, una parte o un dispositivo de almacenamiento masivo, realizar y conservar una copia de estos, preservar la integridad de los que están almacenados pertinentes y hacer inaccesibles o suprimirlos del sistema informático consultado (art. 19 párrafo 3°- Convenio de Budapest).

En el Convenio, "confiscar" significa secuestrar el medio físico en el cual están grabados los datos o la información, o hacer y conservar una copia de los mismos. "Confiscar" incluye el uso o la incautación de los programas necesarios para acceder a los datos que se han confiscado. Además del término "confiscar" se incluye el término "obtener de un modo similar" para dar cuenta de otros medios accesibles por los cuales los datos intangibles se extraen, se prohíbe su acceso, o se adquiere su control de otro modo en el entorno informático.

Así el hecho de confiscar datos, u obtenerlos de un modo similar, tiene dos funciones: a) reunir pruebas, por ejemplo mediante la copia de los datos, o b) confiscar los datos, por ejemplo, copiándolos y más tarde haciendo inaccesible la versión original o borrándolos. La confiscación no implica la supresión definitiva de los datos confiscados[69].

La ley de enjuiciamiento criminal española tiene una disposición específica acorde con las previsiones del Convenio de Budapest. En ella, se establece la necesidad de una resolución judicial que autorice expresamente la realización de copias

[69] ALTMARK, Daniel Ricardo y MOLINA QUIROGA, Eduardo, "Tratado de Derecho Informático", La Ley, Buenos Aires, 2012

de los datos informáticos obtenidos, la que indicará también las condiciones necesarias para asegurar la integridad de los datos y las garantías de su preservación, para hacer posible en caso que sea necesario la práctica de un dictamen pericial.

Esta orden judicial puede ser una extensión de aquella que autorice el registro de la morada o bien, una específicamente para ello. El principio expresamente establecido es que la simple incautación de los soportes físicos donde se encuentran los datos informáticos, no legitima el acceso a su contenido, sea que fueron obtenidos en un registro domiciliario o con independencia de este. Es necesario una orden específica que así lo autorice (ley de enjuiciamiento criminal española- art. 588 sexies a, b, c).

Asimismo expresa que, salvo que constituyan el objeto o instrumento del delito o tengan acceso al sistema de información o una parte de él, se evitará la incautación de soportes físicos que contengan los datos o archivos informáticos, cuando ello pueda causar un grave perjuicio a su titular o propietario y sea posible la obtención de una copia de ellos en condiciones que garanticen la autenticidad e integridad de los datos.

Esto luce lógico, atento la naturaleza del objeto buscado, el que por su carácter intangible y por los avances tecnológicos permite que una investigación pueda contar con los datos informáticos surgidos de un dispositivo hallado, sin necesidad de llevarse el soporte físico donde se encuentra, por ejemplo, la computadora, obteniendo en consecuencia, una copia de aquellos, siempre que se garantice la autenticidad e integridad de los mismos.

Finalmente, refiere la normativa española, que la autoridad encargada de la investigación podrá ordenar a cualquier persona que conozca el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos contenidos que facilite la información que resulte necesaria, bajo apercibimiento de desobediencia, siempre que no implique una carga desproporcionada, que no sea la persona investigada o que no tenga la obligación de declarar por razones de parentesco o secreto profesional.

En Argentina, sin perjuicio de la sanción de la ley 27411, que dispone la adhesión al Convenio de Budapest, no existe una norma específica referida a la obtención de datos informáticos.

En la práctica, las regulaciones sobre secuestro (CPPN- art. 231; CPPCba- art 210; CPPMza- art. 223) han sido utilizadas analógicamente cuando la investigación requería la obtención de evidencia digital.

En forma similar dichas normas disponen que se podrá disponer que sean conservadas o recogidas las cosas relacionadas con el delito, las sujetas a confiscación o aquellas que puedan servir como prueba. Dicha medida deberá ser dispuesta por el Juez, pudiendo ser por el Fiscal de Instrucción, cuando no sea necesario una orden de allanamiento.

Aunque con finalidad probatoria, la naturaleza de esta medida es coercitiva, pues inhibe coactivamente la disponibilidad de una cosa que pasa a poder y disposición de la justicia, lo que implica una restricción de derechos, patrimoniales o no, del imputado o de terceros[70].

De acuerdo a la normativa adjetiva, para ser susceptible de secuestro, el objeto debe reunir dos condiciones: 1) se tiene que tratar de una cosa (entre las que se cuentan los documentos) y, 2) debe estar vinculada al supuesto hecho delictuoso investigado, sea por a) estar relacionada con el delito, b) estar sujeta a confiscación o c) servir como prueba[71]

La referencia al término "cosa", por su correspondencia con lo material, parece excluir la posibilidad de obtener datos informáticos, más allá del secuestro del soporte físico en el que se encuentran.

En doctrina, el término de "cosa" se le ha dado un significado amplio, comprendiendo todo cuerpo sólido, líquido o gaseoso o, sea mueble o inmueble, o documentos.[72]

Cabe recordar que luego de la sanción de la ley 26.733, el término "documento" comprende toda representación de actos o hechos con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión, lo que permite concluir como comprendidos entre los objetos susceptibles de secuestro a los documentos electrónicos o informáticos.

La propia normativa procesal referida, al excluir ciertos documentos, en razón de la protección del derecho de defensa, incorpora la posibilidad

[70] CAFFERATA NORES, José I., TARDITTI, Aida, "Código Procesal Penal de la Provincia de Córdoba comentado", Ed. Mediterránea, Córdoba, 2003
[71] BALCARCE, Fabián I. "El secuestro en materia procesal penal" en AROCENA, Gustavo A. y BALCARCE, Fabián I., "Escritos penales procesales", Ed. Mediterránea, Córdoba, 2006
[72] BALCARCE, Fabián I., ob cit

de secuestrar “documentos”, mostrando el carácter amplio del término “cosa”, que, en consecuencia, no se limita solamente a lo material.

Seguido, las regulaciones procesales prevén la posibilidad de ordenar la presentación de objetos o documentos, sin necesidad de disponer el secuestro, siempre que dichas personas, por razones de parentesco, secreto profesional o de Estado, puedan abstenerse de declarar como testigos (CPPN- art. 232; CPPMza- art. 226).

Finalmente a los fines de preservar los objetos secuestrados, a fin que puedan ser analizados y/o incorporados a la investigación penal, las disposiciones procesales establecen, de modo similar, que los efectos secuestrados serán inventariados y puestos bajo segura custodia, que se podrá disponer la obtención de copias o reproducciones de las cosas secuestradas cuando éstas puedan desaparecer, alterarse, sean de difícil custodia o convenga así a la investigación penal preparatoria. Las cosas secuestradas serán aseguradas con el sello del Tribunal o Fiscalía de Instrucción que intervenga y con la Firma del Juez o del Fiscal, según corresponda, y del Secretario, debiéndose firmar los documentos en cada una de sus hojas. Si fuera necesario remover los sellos, se verificará previamente su identidad e integridad. Concluido el acto, aquéllos serán repuestos, y todo se hará constar.

La cadena de custodia encuentra su fundamento en el resguardo de la garantía del debido proceso. Es el procedimiento controlado que se aplica a los indicios materiales relacionados con el delito, desde su localización hasta su valoración por los encargados de administrar justicia y que tiene como fin no viciar el manejo que de ellos se haga y así evitar alteraciones, sustituciones, contaminaciones o destrucciones. La custodia debe garantizar al juzgador que la evidencia física que se presenta en el juicio es la misma que se recolectó en el sitio del suceso; que no ha sido cambiada, alterada o destruida.

Dicha vinculación directa entre el elemento que se incorpora al proceso como medio de prueba y el hecho que se investiga, supone además una autenticidad formal, ya que el registro de cadena de custodia debe tener en cuenta tanto los factores de identidad, estado original, condiciones de recolección, preservación, embalaje, envío del elemento que se custodia, como los lugares y fechas de permanencia y cambios que cada custodio haga[73].

[73] ROMERO VILLANUEVA, Ricardo J. y GRISETTI, Ricardo A., “Código procesal penal de la nación. Comentado. Ley 27063”, Ciudad Autónoma de Buenos Aires, Abeledo Perrot, 2015

Las características especiales de la evidencia digital, especialmente su volatilidad e inmaterialidad, requieren que el tratamiento de la misma sea distinto a la evidencia física, siendo necesario ciertos recaudos diferentes para preservar la misma y llevarla a juicio debidamente.

A nivel internacional, puede observarse ciertas guías de buenas prácticas para la recolección de evidencia digital, que recomiendan ciertas precauciones especiales que se deben tomar al momento de recolectar, manipular, documentar y examinar la evidencia digital, ya que de lo contrario dicha prueba puede tornarse inválida a los fines judiciales, o, en su caso, mostrarse imprecisa a efectos de esclarecer el hecho.

Una de ellas es la publicada en el Reino Unido por la *Association of Chief Police Officers* (ACPO, 2004, 2012), que establece cuatro principios claves para el manejo de la evidencia digital: 1) ninguna acción realizada por personal de las fuerzas de seguridad debería alterar los datos almacenados que sean susceptibles de ser presentados en juicio; 2) para aquellas circunstancias que fuere necesario el acceso a un dato original almacenado en una computadora, la persona encargada de realizar la medida debe ser competente para llevar adelante esa tarea y ser capaz de entregar la evidencia explicando la relevancia e implicaciones de sus acciones; 3)deberá crearse y preservarse un registro de auditoría sobre toda la evidencia electrónica basada en computadoras que sea recolectada. Cualquier profesional independiente debería ser capaz de examinar esos procedimientos y llegar al mismo resultado; 4) la persona que esté a cargo de la investigación tiene la responsabilidad final ante la ley de hacer cumplir estos principios[74].

Asimismo la norma ISO/IEC 27037:2012, expresa que la evidencia digital es gobernada por tres principios: la relevancia, la confiabilidad y la suficiencia[75].

La relevancia es una condición técnicamente jurídica, que habla sobre aquellos elementos que son pertinentes a la situación que se analiza o investiga con el fin de probar o no una hipótesis fáctica.

La confiabilidad refiere a la búsqueda de validar a repetibilidad y auditabilidad de un proceso aplicado para obtener evidencia digital.

Finalmente el principio de suficiencia, se relaciona con la completitud de las pruebas, esto significa, que con las evidencias recolectadas y

[74] GOMEZ, Leopoldo Sebastián, "Evidencia digital en la Investigación Penal" en Dupuy Daniela y Kiefer Mariana, "Cibercrimen" Editorial BdeF, Buenos Aires, 2017

[75] Resolución de Procuración General de la Nación N° 756/16 del 31 de Marzo de 2016

analizadas, tenemos suficientes elementos para sustentar los hallazgos y verificar las afirmaciones efectuadas sobre la situación investigada.

De dicha regla de estandarización, Leopoldo Gómez[76] destaca la definición de dos roles principales en la actuación pericial informática: el DEFR (*digital evidence first responder*) y el DES (*digital evidence specialist*). Los primeros son los que se encargan de las tareas de campo en procedimientos judiciales vinculados con la identificación y preservación de evidencia digital. Los segundos son aquellos encargados de la pericia informática, es decir aquellas tareas de laboratorio de análisis y presentación de la evidencia digital.

Estas guías o reglas mencionadas han sido receptadas en Argentina por el Ministerio Público Fiscal de la Nación y por el Poder Judicial de la Provincia de Neuquén, los que han aprobado, en respectivas resoluciones, guías o protocolos de actuación para la obtención, preservación y tratamiento de evidencia digital[77], en pericias informáticas[78] o en pericias informáticas en telefonía celular[79]

Tomando como ejemplo la primera de dichas guías, se recomienda ante el hallazgo de un dispositivo informático, verificar el estado del mismo, esto es, si encuentra encendido o apagado. En el primer caso, se aconseja remover el cable de alimentación, no encender nunca el equipo, asegurar todas las lectoras estén cerradas, encintar todas las entradas de puertos, cables alimentación, etc., y registrar la marca, modelo y número de serie del dispositivo, así como cualquier otra dato identificatorio. En caso que esté encendido, la vía más segura de preservación de la evidencia digital es quitando las fuentes de alimentación de energía, salvo que fuere necesario, mantenerlo encendido por detectarse a simple vista en pantalla información ostensible para la investigación o se encuentren activos datos encriptados, documentos, programas, etc. En estas situaciones se recomienda el uso de dispositivo de captura volátil de datos que tenga bloqueada la escritura, previo dejar expresa constancia de tal decisión.

En los casos que se encuentre en red, se aconseja la desconexión a la misma o el bloqueo de acceso. Sin perjuicio de ello, se deberá obtener información

[76] GOMEZ, Leopoldo Sebastián, ob cit
[77] Resolución de Procuración General de la Nación N° 756/16 del 31 de Marzo de 2016
[78] Poder Judicial de Neuquen, "Protocolo de actuación para pericias informáticas", aprobado por Acuerdo N° 4908, protocolizado y publicado en BO, Neuquen, 2012, visto en www.200.70.33.130/images2/biblioteca/protocoloactuacionpericiasinformáticas.pdf
[79] Poder Judicial de Neuquen, "Pericias informáticas sobre telefonía celular", aprobado por Acuerdo N° 5024, visto en www.200.70.33.130/images2/biblioteca/protocolopericiastelefoniacelular.pdf

relativa al listado de procesos servicios y aplicaciones utilizadas, el registro de logueo y usuarios identificados, información de red con detalle de puertos abiertos y cerrados, información contenida en el caché del sistema, información del registro del sistema operativo y el volcado de memoria RAM.

Al momento de empacar debe asegurarse que toda la evidencia recolectada se encuentre debidamente documentada, etiquetada, marcada, fotografiada, filmada o esquematizada. Se recomienda el embalaje en bolsas antiestáticas, o en su defecto de papel madera o cartón. Y en caso de ser necesario que continúe encendido, se recomienda cubrir los mismos en material que bloquee la señal de transferencia de datos ("jaulas *Faraday*").

El análisis y examen de dispositivos de almacenamiento de información deberán realizarse en establecimientos que dispongan de áreas acondicionadas, las cuales deberán ser zonas seguras antiestáticas, a fin de evitar cualquier intromisión vía *WI-FI, Bluetooth* u otro medio de acceso remoto.

A los fines de analizar profundamente la evidencia digital, debe realizarse una copia o imagen forense, la que puede hacerse extrayendo físicamente el disco rígido del ordenador o a través de un dispositivo externo, aunque siempre mediante una herramienta de *software* avalada internacionalmente. Para su realización es necesario utilizar un bloqueador de escritura a fin de evitar cualquier riesgo de modificación de algún dato, y una vez finalizado el copiado, el agente debe realizar el cálculo *hash* de dicha copia forense.

En definitiva, el procedimiento general de investigación judicial, utilizando servicios de informática forense consta de dos etapas principales: a) incautación confiable de la prueba y mantenimiento de cadena de custodia, y b) análisis de la información disponible con arreglo al incidente investigado y redacción del informe pericial.

La primera etapa debe ser llevada a cabo por personal policial junto al Fiscal, responsable del control o ejecución de la medida. La segunda etapa debe ser efectuada en el laboratorio por un perito siguiendo los estándares de la ciencia forense para el manejo de la evidencia, en función de los puntos de pericia que sean indicados por los operadores judiciales.

Conforme las normativas procesales, solo se podrán requerir informes periciales, cuando para descubrir o valorar alguna evidencia sea necesario poseer conocimientos especiales en informática forense.

Sólo se realizarán pericias que involucren la utilización del *hardware* y *software* para informática forense y aquellas que requieran la experticia de un profesional. Quedan excluidas del servicio de pericias informáticas toda tarea administrativa o técnica que no sea propia de la disciplina (tareas de transcripción de textos, tareas de ordenamiento de información o cruzamiento de datos, tareas de filmación, de escucha, de copias simples como *backups* o de resguardo de dispositivos de almacenamiento de información digital)[80]

Al respecto, la Tercera Cámara del Crimen de la Provincia de Mendoza[81], en fallo luego ratificado por la Suprema Corte de dicha provincia[82] expresó que "el examen de los materiales tiene naturaleza de pericia y no de un simple informe técnico. Entiendo que cuando el órgano judicial interviniente pretenda obtener una opinión especializada sobre un tema que exija conocimientos específicos en alguna ciencia, arte o técnica (art. 244 C.P.P.), debe recurrir a la realización de una pericia. La pericia tiene una conclusión, fruto de un juicio realizado al amparo de esos conocimientos especiales. Los informes técnicos tienen, en cambio, una naturaleza esencialmente descriptiva y su finalidad es "hacer constar el estado de las personas, de las cosas y de los lugares, mediante inspecciones, planos, fotografías, exámenes técnicos y demás operaciones que aconseje la policía científica".

En consecuencia, el análisis de la información digital hallada, realizado siempre por una persona especializada en la materia, debe seguir las reglas de la pericia, siempre teniendo en cuenta las especiales características, sobre todo de volatilidad, de la evidencia informática, ya que la falta de seguimiento de las normas relativas a este medio de prueba, pueden acarrear la nulidad del informe pericial, y puede

---

[80] Poder Judicial de Neuquen, "Protocolo de actuación para pericias informáticas", aprobado por Acuerdo N° 4908, protocolizado y publicado en BO, Neuquen, 2012, visto en www.200.70.33.130/images2/biblioteca/protocoloactuacionpericiasinformáticas.pdf

[81] Tercera Cámara del Crimen de la Provincia de Mendoza, Expte. N° P-19353/15 caratulada "Fc./ FLORES MUÑOZ CLAUDIO p/ DISTRIBUCIÓN DE IMÁGENES DE PORNOGRAFÍA INFANTIL EN CONCURSO REAL CON ABUSO SEXUAL GRAVEMENTE ULTRAJANTE" y su acumulada P-19407/15 caratulada "F. c/ FLORES MUÑOZ CLAUDIO p/ CORRUPCION AGRAVADA DE MENORES", 09/06/2017

[82] Suprema Corte de Justicia de Mendoza, Sala II, Expte. N° 13-04174800-6/1, "F. C/FLORES MUÑOZ CLAUDIO CESAR P/PUBLICACIONES Y REPRODUCCIONES OBSCENAS EN GRADO DE TENTATIVA (19353) P/ RECURSO EXT.DE CASACIÓN", 16/05/2018

ser necesaria la reproducción y repetición de la medida[83], más allá del debido control durante y posterior que pueda ejercer la Defensa.

[83] Tercera Cámara del Crimen de la Provincia de Mendoza, fallo citado.

CAPÍTULO IV

IV. Recopilación en tiempo real de datos informáticos

"Las medidas de investigación que impliquen el uso de las TIC y que representen una intromisión significativa en el derecho a la privacidad, como el acceso al contenido de las comunicaciones, la interceptación y acceso de datos en tiempo real, o la utilización de técnicas de investigación remota solo podrán acordarse, como regla general, previa autorización judicial, cuando exista una sospecha razonable de la comisión de un delito que pueda calificarse como grave cuando el destinatario de la medida está vinculado con ese hecho delictivo".

El párrafo anteriormente transcripto es una de las recomendaciones surgidas del XIX Congreso internacional de Derecho Penal, último congreso de la Asociación internacional de Derecho Penal, celebrado en Río de Janeiro en setiembre de 2014, bajo el nombre "Sociedad de la Información y Derecho Penal"[84].

Esta recomendación muestra claramente que a mayor intromisión mayor debe ser el recaudo que debe tomarse, resaltando la necesidad de una autorización judicial, basada en la sospecha razonable que el destinatario de la medida ha cometido un delito grave.

En el capítulo anterior, se analizó la búsqueda de aquella evidencia digital ya producida, almacenada, y en tal sentido, se revisó aquellas medidas como el registro, allanamiento o el decomiso que son medidas investigativas coercitivas que prevén las normativas procesales argentinas, aunque inicialmente para la evidencia

[84] DE LUCA, Javier Augusto, "Delitos informáticos, apuntes 2016", en DUPUY, Daniela y KIEFER, Mariana "Cibercrimen", Ed. BdeF, Buenos Aires, 2017; http://www.penal.org/es/resoluciones-del-%C3%BAltimo-congreso

física, y que debe analizarse a la luz de las nuevas posibilidades y necesidades que la tecnología actual brinda.

Así, se determinó que, si bien en la República Argentina existe regulación, aún escasa, que avizora alguna adecuación a la tendencia legislativa internacional, cierto es que ella aun deja sin prever situaciones que solo por analogía de medidas similares puede resolverse.

En este capítulo, se buscará analizar aquellas medidas investigativas que tengan por fin la recolección de evidencia digital, en tiempo real, es decir, al momento en que está llevándose a cabo.

La celeridad que requiere la investigación de *ciberdelitos* o la volatilidad de la evidencia digital implica muchas veces la necesidad de acceder a las comunicaciones, interceptando, observando y obteniendo copias en el momento que se producen.

Las legislaciones procesales argentinas, prevén la interceptación de correspondencia epistolar y la intervención de las comunicaciones telefónicas y a partir de allí, se ha autorizado pretorianamente, la adecuación de dichas medidas a las nuevas tecnologías de la información y comunicación, como es el *email,* la mensajería de texto, redes sociales como *whatsapp, Telegram, Instagram, etc.*, todas las cuales amplían sustancialmente las posibilidades de comunicaciones, que antes pareciera solo reservada a la correspondencia postal y telefónica.

En la actualidad, a través de un *Smartphone,* una *Tablet,* una *notebook,* o cualquier otro dispositivo electrónico, una persona puede no solo enviarse *emails,* o comunicarse telefónicamente, sino también transmitir de modo sencillo, "a un *click*", imágenes, sonidos, videos, archivos de texto, etc.

Además, esta comunicación por medios telemáticos, importante por su contenido, mucho más amplio que el de otras épocas, es trascendente porque también aporta numerosa información prácticamente involuntaria o inconsciente que el comunicante transmite, como la duración de la llamada, la fecha en que se realiza, la dirección IP desde la cual se transmite y hasta la ubicación del mismo.

Estos datos, llamados de tráfico, si bien hacen a lo colateral del contenido de la información, pueden ser vital en una investigación, ya que permiten acreditar por ejemplo a través de su dirección IP, quien envía y desde donde lo hace, sin necesidad de conocer el contenido de la comunicación.

Por tanto, la interceptación o intervención de una comunicación electrónica en tiempo real, conlleva una fuerte intromisión en la persona que ha sido objeto de la medida, siendo ella mayor que la realizada a través de la interceptación de una carta o una escucha telefónica, por la mayor información que se aporta, aun involuntariamente por el comunicante.

Incluso, comparativamente con el registro y decomiso de datos almacenados, se advierte la mayor intromisión de una medida de intervención de la comunicación electrónica en tiempo real, por cuanto esta última se realiza a espaldas del sujeto destinatario de la medida. Claramente si la intervención en tiempo real se realiza en conocimiento del comunicante esta pierde total sentido. Por tanto, la observación y obtención de copia de una comunicación en tiempo real, sin dudas, implica una injerencia mayor en la intimidad o privacidad de la persona vigilada.

La Constitución argentina establece en el art. 18 la inviolabilidad de la correspondencia epistolar y de los papeles privados y el art. 19 el principio de reserva, que expresa que las acciones privadas de los hombres que de ningún modo ofendan al orden a la moral pública, ni perjudiquen a un tercero, están solo reservadas a Dios y exentas de la autoridad de los magistrados.

La Corte suprema de justicia argentina, al referirse al art. 18 de la Constitución Nacional, ha expresado que en él se consagra "el derecho individual a la privacidad del domicilio de todo habitante —correlativo al principio general del art. 19— en cuyo resguardo se determina la garantía de su inviolabilidad, oponible a cualquier extraño, sea particular o funcionario público" (ver "Fiorentino" Fallos: 306:1752). Si bien allí no se hizo mención a las comunicaciones telefónicas ni a la protección de su secreto, una interpretación dinámica de su texto más lo previsto en su artículo 33 y en los artículos 11, inciso 2°, de la Convención Americana sobre Derechos Humanos, y 17, inciso 1°, del Pacto Internacional de Derechos Civiles y Políticos, en cuanto contemplan, en redacción casi idéntica, que nadie puede ser objeto de injerencias arbitrarias en su vida privada, en la de su familia, en su domicilio o en su correspondencia, permiten hacer extensivas aquellas consideraciones a casos como el presente[85].

De esta manera, se define jurisprudencialmente el derecho a la intimidad, tutelado por la Constitución Nacional, y comprensivo no solo de la

[85] CSJN, "Quaranta, José Carlos", 31/08/2010, fallo 333:1674, www.lalaleyonline.com.ar, AR/JUR/45956/2010

correspondencia epistolar, de los papeles privados sino también de las comunicaciones telefónicas y por otros medios que mantenga una persona.

A posterior, algunas otras leyes han regulado también la inviolabilidad de las comunicaciones, como la ley 19.798 de telecomunicaciones o la ley 25.520 de inteligencia, siendo esta última de importancia, por cuanto amplía el objeto de protección de la garantía no solo a comunicaciones telefónicas, postales, de telégrafo o facsímil, sino también a cualquier otro sistema de envío de objetos o transmisión de imágenes, voces o paquetes de datos, así como cualquier tipo de información, archivos, registros y/o documentos privados o de entrada o lectura no autorizada o no accesible al público.

Seguidamente, es vital remarcar la sanción de la ley 27.411 que dispone la adhesión de la República Argentina al Convenio de Budapest sobre *cibercriminalidad*, que dispone entre las medidas procesales aquellas atinentes a la recopilación en tiempo real de datos informáticos.

Al respecto, es importante destacar la distinción que realiza dicho convenio entre los datos de tráfico y los de contenido, siendo mucho más restrictiva la posibilidad de acceder en tiempo real a estos últimos, al autorizarse solo en relación a ciertos delitos.

En España, país adherente del convenio referido, se ha previsto en la ley de enjuiciamiento criminal, un capítulo específico que regula los casos y requisitos en los que puede obtenerse en tiempo real los datos informáticos necesarios, sean estos de tráfico o de contenido y establece los principios que debe cumplir la orden judicial que lo autorice.

En Argentina, el desarrollo legislativo sobre esta temática aun es escaso. El nuevo código procesal penal de la Nación, sancionado mediante ley 27.063, ha incorporado algunas reformas atinentes a estas medidas investigativas (art. 143, 144, 145), lo que implica un avance en la regulación de la obtención de datos informáticos.

También lo han hecho otras regulaciones procesales como la mendocina, ampliando la posibilidad de intervenir las comunicaciones en tiempo real no solo aquellas telefónicas, sino también por otros medios, en forma genérica.

A. Análisis de las disposiciones del Convenio de Budapest y de la ley de enjuiciamiento criminal española sobre la recopilación en tiempo real

El titulo 5 de la sección del Convenio referido a aspectos procesales, trata la posibilidad de la obtención de datos relativos al tráfico y la interceptación de datos relativos al contenido, ambos en tiempo real, siempre que se encuentren asociadas a comunicaciones específicas transmitidas en su territorio por un sistema informático.

Lo que se busca con estas medidas es la recopilación de pruebas contenidas en comunicaciones que se producen en el mismo momento. Siendo los datos intangibles, la obtención de estos no puede ser física, debiendo captarse a través de una grabación de los datos transmitidos.

Cabe destacar que el Convenio recepta la facultad de obtener datos respecto a comunicaciones específicas, no permitiendo ni exigiendo la vigilancia generalizada o indiscriminada de datos informáticos, sino que deben ser claramente determinadas las comunicaciones de las cuales podrá obtenerse la información.

Sobre los datos relativos al tráfico (art 20), el mismo Convenio los define, siendo todos aquellos relativos a una comunicación realizada por medio de un sistema informático, generados por este último en tanto que elemento de la cadena de comunicación, y que indiquen el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente (art. 1. D, Convenio sobre ciberdelincuencia Budapest 2001).

Respecto de los datos relativos al contenido (art. 21), el Convenio no define al mismo, aunque esencialmente refiere al contenido de la comunicación, mensaje, o información transmitida.[86]

El hecho que sean transmitidas las comunicaciones vigiladas por medio de un sistema informático, lo distingue de aquellas realizadas por intermedio de las telecomunicaciones, siendo en la primera mucho más amplia la información que uno pueda obtener, al poder transmitirse o almacenarse en las computadoras u otros sistemas informáticos tanto textos, como imágenes o sonidos.

[86] ALTMARK, Daniel Ricardo- MOLINA QUIROGA, Eduardo "Tratado de Derecho Informático", 1ª ed., Buenos Aires, La Ley, 2012, T. III, p. 214/490.

Por este motivo, la medida que se adopte respecto de comunicaciones transmitidas por un sistema informático es mucho más intrusiva y por tanto el perjuicio, económico, social o personal, es más significativo, debiendo tener mayor precisión la orden que disponga la misma.

En esta línea, a su vez el Convenio distingue si la obtención es de datos relativos al tráfico (art 20) o al contenido (art. 21), estableciendo para los segundos que solo puede aplicarse esta medida respecto de un repertorio de "delitos graves" definidos por cada derecho interno.

Es decir, considerando más intrusiva la interceptación de datos relativos al contenido, acota mucho la facultad de aplicación de esta medida, librando a cada parte que establezca cuales delitos son, por su gravedad, meritorios de tal medida.

Vale decir que, si bien el art. 14 del Convenio establece la posibilidad que cada Parte se reserve a ciertos delitos la posibilidad de obtener datos relativos al tráfico solo a ciertos delitos, esta categoría no puede ser más reducido que el repertorio de delitos graves del art. 21.

Finalmente, el Convenio establece la facultad de obtención de datos de tráfico o relativos al contenido en tiempo real, sino también que pueda obligarse al proveedor de servicios a obtener o grabar con medios técnicos existentes en el territorio o a prestar colaboración o asistencia para tal tarea.

Esta facultad de obligar al proveedor de servicios es siempre en la medida de sus capacidades técnicas, lo que implica que no puede obligar al mismo a obtener los medios técnicos necesarios o capacitar a su personal para la realización de la medida. Solo cuando disponga de tales recursos, puede ser obligado.

Finalmente, el Convenio fija que deberá obligarse al proveedor a mantener secreto sobre la medida realizada, así como la información obtenida. Obviamente la eficacia y éxito de la medida, dependerá de que la persona vigilada no tenga conocimiento de su práctica, siendo por ello imprescindible la obligación de secreto que recae sobre el proveedor de servicio.

España, país signatario del Convenio de Budapest, regula la facultad de interceptar una comunicación en tiempo real, sea aquella practicada a través de medios telefónicos o telemáticos, o sea, la captación y grabación de la comunicación oral a través de la utilización de dispositivos electrónicos o de dispositivos técnicos de seguimiento, localización y captación de la imagen.

Sin perjuicio de la distinción hecha para cada medida, establece ciertos principios rectores, aplicables también al registro de dispositivos de almacenamiento masivo de información y los registros remotos sobre equipos informáticos.

Así, establece que se podrá disponer alguna de dichas medidas, siempre que medie autorización judicial, dictada con plena sujeción a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad. El primero de ellos exige que una medida esté relacionada con la investigación de un delito concreto. El principio de idoneidad servirá para definir el ámbito subjetivo y objetivo y la duración de la medida en virtud de su utilidad. Los principios de excepcionalidad y necesidad implican que solo podrá dictarse esta medida cuando no exista otra medida menos gravosa para el esclarecimiento del hecho o, cuando el descubrimiento y comprobación de este se vea dificultado sin recurrir a dicha medida. Finalmente, para que sean reputadas proporcionadas, deberá meritarse de las circunstancias del caso que el sacrificio de los derechos e intereses afectados no sea superior al beneficio que implique para el interés público y de terceros, debiendo tenerse en cuenta, la gravedad del hecho su trascendencia social o el ámbito tecnológico de producción, la intensidad de los indicios existentes y la relevancia del resultado perseguido (Ley de enjuiciamiento criminal española- *LEC*- art. 588 bis a)

También exige como disposición común el secreto de la solicitud y las actuaciones posteriores a la medida (LEC- art. 588 bis d), la necesidad de especificarse una duración que no podrá exceder el imprescindible para el esclarecimiento del hecho (LEC- art. 588 bis e), la existencia de un control judicial durante y posterior de la medida adoptada (LEC- art. 55 bis g) y la destrucción de los registros una vez que ponga fin a los procedimientos mediante resolución firme (LEC- art. 588 bis k).

Sin perjuicio de las disposiciones comunes que prevé la normativa española, seguido a ello regula la facultad de interceptación de las comunicaciones telefónicas y telemáticas y así establece, en primer lugar que podrá autorizarse solo en la investigación de ciertos delitos que expresamente determina en el mismo digesto o de aquellos cometidos a través de instrumentos informáticos u otra tecnología de la información o la comunicación (LEC- art. 588 ter a), lo que encuentra lógica desde el principio de proporcionalidad antes referido y también, regulado en el Convenio de Budapest.

Así, podrá autorizarse, mediante resolución judicial, el acceso al contenido de las comunicaciones y a los datos de tráfico o asociados al proceso de comunicación, así como los que se produzcan con independencia de una concreta comunicación, en los que participe el sujeto investigado o en las terminales o medios de comunicación que este sea titular o usuario. También puede intervenirse las terminales o medios de comunicación de la víctima, cuando sea previsible un grave riesgo para su vida o integridad (LEC- art. 588 ter b).

Al igual que en el Convenio de Budapest, se establece la obligación de todo prestador de servicios de telecomunicaciones, de acceso a una red, así como de toda persona que contribuya de cualquier modo a facilitar la comunicación telefónica, telemática, lógica o virtual, a prestar asistencia y colaboración precisas para facilitar el cumplimiento de los autos de intervención de las telecomunicaciones, debiendo guardar secreto acerca de sus actividades (LEC- art. 588 ter e).

Respecto a la duración, establece un plazo de tres meses desde la autorización judicial, prorrogables por iguales periodos, hasta un plazo máximo de dieciocho meses (LEC- art. 588 ter i).

Avanza asimismo la normativa española, al establecer que podrá autorizarse la colocación y utilización de dispositivos electrónicos que permitan la captación y grabación de comunicaciones orales directa que se mantengan por el investigado, sea en la vía pública, en otro lugar abierto, en el domicilio o en cualquier otro lugar cerrado (LEC- art. 588 quater a) e incluso complementarse con la obtención de imágenes, siempre que haya autorización expresa por resolución judicial.

Para ello, se prevé como presupuestos, que sean comunicaciones que puedan tener lugar en uno o varios encuentros concretos y sobre cuya previsibilidad haya sido puesta de manifiesto en la investigación. A su vez solo puede realizarse en el marco de la investigación de ciertos delitos determinados que taxativamente establece, y siempre que racionalmente pueda preverse que la medida aportará datos esenciales y de relevancia probatoria para el esclarecimiento del hecho.

Respecto al catálogo de delitos, a pesar de ser una injerencia a la privacidad del destinatario de la medida, el mismo es bastante amplio, al incluir más allá de delitos graves como terrorismo o aquellos cometidos en el seno de un grupo u organización criminal, a aquellos delitos dolosos que tengan al menos como pena máxima

de tres años, lo que extiende el abanico de delitos en gran medida (LEC- art. 588 quater b).

Finalmente, la ley de enjuiciamiento criminal española regula la posibilidad de obtener y grabar por cualquier medio técnico imágenes de la persona investigada cuando se encuentre en un lugar o espacio público, si ello fuere necesario para facilitar su identificación, para localizar los instrumentos o efectos del delito u obtener datos relevantes para el esclarecimiento de los hechos. Esta medida puede extenderse a otras personas distintas al investigado, siempre que de otro modo se reduzca de forma relevante la vigilancia o existan indicios fundados de la relación de dichas personas con el investigado y los hechos objeto de la investigación (LEC- art. 588 quinquies a).

A su vez pueden utilizarse dispositivos o medios técnicos de seguimiento y localización cuando concurran razones de necesidad y la medida resulte proporcionada, debiendo especificarse el medio técnico que va a ser utilizado. Incorpora en este aspecto el referido plexo normativo la posibilidad que cuando concurran razones de urgencia, pueda la policía judicial colocar los dispositivos o medios técnicos de seguimiento y localización, sin autorización judicial, dando cuenta en un plazo máximo de veinticuatro horas al juez a fin de que ratifique o haga cesar la medida (LEC- art. 588 quinquies b).

B. Intervención de las comunicaciones electrónicas

Se define dicha herramienta como la interferencia a las comunicaciones realizadas por el imputado por cualquier medio técnico (telefónico, telefax, e-mail, etc.) y dispuesta por un órgano jurisdiccional en forma fundada durante la sustanciación de un proceso penal, con el objeto de conocerlas o impedirlas.

Es una limitación a la libre y secreta comunicación personal por medios escritos o técnicos impuesta al imputado y a terceros que se comuniquen con él, en el curso de un proceso penal, destinada a asegurar el fiel cumplimiento de determinadas limitaciones de libertad ambulatoria de carácter cautelar (incomunicación), como así también la libre producción de elementos de prueba de cargo o descargo vinculados a la causa.[87]

Esta medida judicial se afinca en el derecho constitucional individual a la protección de la privacidad del domicilio de todo habitante (arts. 18 y 19,

[87] BALCARCE, Fabián, "Escritos penales procesales", Ed. Mediterránea, 1° ed., Córdoba, 2006, p. 331

CN), lo que incluye, pues, a las "comunicaciones telefónicas", en virtud de una interpretación dinámica de la Constitución Nacional, más lo previsto en su art. 33 y en los arts. 11, inc. 2º, de la Convención Americana de Derechos Humanos, y 17, inc. 1º, del Pacto Internacional de Derechos Civiles y Políticos, en cuanto contemplan, en redacción casi idéntica, que nadie puede ser objeto de injerencias arbitrarias en su vida privada, en la de su familia, en su domicilio o en su correspondencia, lo que permite hacer extensivas dichas consideraciones a las comunicaciones telefónicas.[88]

Puede señalarse, de modo general, que los requisitos para la validez probatoria de la información obtenida como resultado de las intervenciones telefónicas son:

1.- Judicial: La medida coercitiva debe ser autorizada por un Juez, en tanto que es la única autoridad a quien constitucionalmente se le ha conferido la facultad y la responsabilidad para determinar la procedencia de la medida;

2.- Especialidad: Tales diligencias han de ser acordadas con motivo de concretas actuaciones llevadas a cabo para la investigación de unos hechos presuntamente delictivos determinados "en el marco de un proceso penal"; con absoluta exclusión de actuaciones de carácter prospectivo e indeterminado, esto es: no se puede ordenar tales medidas por una sospecha de criminalidad genérica o a los fines de la investigación de hipotéticos delitos futuros;

3.- Proporcionalidad: de tan grave injerencia, en proporción a la importancia y gravedad de la infracción investigada;

4.- Excepcionalidad y Necesidad: de acudir a semejante medio de investigación, atendidas las características de los hechos investigados, la grave dificultad para su descubrimiento y la trascendencia social del delito investigado, sin que pueda ser sustituido por otros mecanismos menos aflictivos o gravosos para el ciudadano objeto de investigación. Si se puede recurrir a otros medios menos gravosos a los fines de conseguir igual o mejor resultado a los fines de la investigación delictiva, la medida no es necesaria;

---

[88] GÓMEZ, Claudio D. “La "Intervención de llamadas telefónicas" en la jurisprudencia de la Corte Suprema de Justicia de la Nación. A propósito del caso: "Q." LA LEY 23/12/2010 , 4 • LA LEY 2011-A , 47

5.- Motivación suficiente: La decisión judicial debe reflejar la existencia de los anteriores requisitos, bien expresamente o al menos por remisión a algún elemento objetivo de la causa que pudiera fundar una mínima sospecha razonable. Se impone al Tribunal el deber concreto de fundar el Auto que ordena la medida, defiriendo el contradictorio y la defensa en juicio del imputado, para una vez que se ejecuta la medida, pudiendo el encartado articular la nulidad de la medida cuando la intervención se produjo sin la debida fundamentación legal.

Todos estos requisitos integran el estándar de legalidad en clave constitucional, de suerte que la no superación de este control de legalidad convierte en ilegítima por violación al art. 18 y 19, de la Const. Nacional, con una nulidad insanable, que arrastrará a todas aquellas otras pruebas directamente relacionadas y derivadas de las intervenciones telefónicas en las que se aprecie esa "conexión de antijuridicidad" y que constituya el único cause de investigación (teoría del fruto del árbol envenenado).

En Argentina, esta medida judicial se encuentra prevista en leyes sustantivas como la ley de telecomunicaciones (ley 19798) o de inteligencia (ley 25520), como en leyes adjetivas (código procesal penal de la Nación y los códigos procesales provinciales).

Sin perjuicio de ello, es opinión de Carlos Carbone[89] que no existe en Argentina aquella ley que exige la Constitución Nacional para vulnerar la inviolabilidad de la correspondencia epistolar y el domicilio. Ninguna de las normas nacionales o provinciales que permiten las intervenciones telefónicas establecen precisamente los casos, los delitos y bajo qué fundamentos tendrá lugar. En ese sentido, considera el autor que es necesario una ley federal, dictada por el Congreso de la Nación para toda Argentina, a pesar del carácter procesal de la misma que pueda especificar los alcances y proyecciones del art. 18 de la Constitución Nacional.

En contrario, la jurisprudencia argentina mantiene el criterio de que tal inmunidad no es absoluta en la medida en la medida que el propio texto constitucional advierte que una ley determinará en qué casos y con qué justificativos podrá reconocerse a su allanamiento y ocupación, y que la reglamentación legal de esa garantía debe encontrarse en el artículo 236 del CPPN, en la ley 19798 de

[89] CARBONE, Carlos, "Requisitos constitucionales de las intervenciones telefónicas", Rubinzal-Culzoni, Santa Fe, 2008.

telecomunicaciones y en las disposiciones procesales regulatorias de otros medios de prueba que guarden sustancial analogía con el de los registros magnetofónicos[90]

Más allá de ello, tal como fue referida previamente, se ha dictado la ley 19798 de telecomunicaciones[91], la que en su artículo 18 prevé la inviolabilidad de la correspondencia de telecomunicaciones, salvo interceptación requerida por juez competente. También define el alcance de dicha inviolabilidad, al decir que, ella importa la prohibición de abrir, sustraer, interceptar, interferir, cambiar su texto, desviar su curso, publicar, usar, tratar de conocer o facilitar que otra persona que no sea su destinatario conozca la existencia o el contenido de cualquier comunicación confiada a los prestadores del servicio y la de dar ocasión de cometer tales actos (art 19).

La ley 25520[92], actualizada por ley 27126, regula en el artículo 5 la inviolabilidad de las comunicaciones telefónicas, postales, de telégrafo o facsímil, y amplia también a cualquier otro sistema de envío de objetos o transmisión de imágenes, voces o paquetes de datos, así como cualquier tipo de información, archivos, registros y/o documentos privados o de entrada o lectura no autorizada o no accesible al público, salvo orden o dispensa judicial.

Asimismo, en el título VI regula la interceptación y captación de comunicaciones durante el desarrollo de actividades de inteligencia y contrainteligencia, estableciendo los principios y reglas de cuando y como debe llevarse a cabo dicha medida.

En este sentido, esta ley exige la necesidad de una autorización judicial, la que deberá formularse por escrito y estar fundada con indicación precisa de los números telefónicos o direcciones electrónicas o de cualquier medio, cuyas comunicaciones se pretendan interceptar o captar. Esta autorización judicial tendrá una duración de 60 días, la que puede prorrogarse por 60 días más cuando fuere imprescindible para el curso de la investigación.

A continuación, la posibilidad de intervenir una comunicación encuentra regulación en las leyes adjetivas, tanto nacional como provincial.

Así, el código procesal penal de la nación establece en su art. 236 que, el juez podrá autorizar la intervención de las comunicaciones telefónicas o cualquier otro medio de comunicación del imputado, para impedirlas o conocerlas. En términos

[90] CARBONE, Carlos, ob cit.
[91] http://servicios.infoleg.gob.ar/infolegInternet/anexos/30000-34999/31922/texact.htm
[92] http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70496/texact.htm

similares también lo hacen las provincias en sus códigos procesales (CPPMza.- art. 229; CPPCba.- art. 216, etc.).

Al respecto, la ley 27.063, que establece un nuevo código procesal penal de la Nación y se encuentra vigente en Argentina, aunque no sea aplicable aún en todas las provincias, conforme el régimen de implementación progresiva previsto por Ley 27.150 y decreto N° 257/2015, establece expresamente en su art. 143 que siempre que sea útil para la comprobación del delito, el juez podrá ordenar la interceptación y secuestro de la correspondencia postal, telegráfica, electrónica o cualquier otra forma de comunicación o de todo otro efecto remitido por el imputado o destinado a este, aunque sea bajo nombre supuesto. De esta manera, incorpora la posibilidad de intervenir una comunicación electrónica, siempre que sea a través de orden judicial, con carácter excepcional y por una duración de 30 días que puede ser renovada

Intervenir, significa vigilar con autoridad y agrega a la observación la toma de contenido de las conversaciones, en un soporte físico con factibilidad de ser reproducidas con posterioridad. Designa una actividad de interposición de carácter técnico desarrollada entre interlocutores de una conversación, que, si se trata de aparatos telefónicos, fijos, inalámbricos o móviles podrá comprender solo la observación y/o la inmovilización de la conversación mediante su registro por medio idóneo: grabación, pudiendo en cualquier caso, producir la inmovilización de la comunicación mediante cualquier forma de registro[93].

En síntesis, las normas adjetivas exigen para la intervención de las comunicaciones la existencia de una resolución judicial, sea ella un auto (CPPN- art. 236) o un decreto (CPPMza- art. 229; CPPCba- art. 216), siempre que esta se encuentre fundada. Como excepción, el código procedimental nacional permite que, en casos que se investigue los delitos previstos en el artículo 142 bis y el artículo 170, ambos del código penal, o en causas conexas a estas, cuando existiere peligro en la demora, debidamente justificado, dichas facultades podrán ser ejercidas por el representante del Ministerio público fiscal, mediante auto fundado, con inmediata comunicación al juez, quien deberá convalidarla en el término de veinticuatro horas, bajo apercibimiento de nulidad del acto e ineficacia de sus resultas (CPPN- art. 236 último párrafo).

[93] CARBONE, Carlos Alberto, "Requisitos constitucionales de las intervenciones telefónicas", Rubinzal-Culzoni, Santa Fe, 2008

Seguido, si bien no surge de la normativa nacional[94], se encuentra previsto en el nuevo código procesal penal de la nación (ley 27.063) y en algunos códigos provinciales, el tiempo de duración de la medida, el cual no puede ser *sine die,* estableciéndose un término de 30 (ley 27.063), o 60 días (CPPMza) como máximo, el que puede ser prorrogable por igual término (CPPMza- art. 229 ter). Expresamente establece esta norma provincial que no podrá concederse una autorización de manera indeterminada, referencia que incorpora la ley 27.063, agregando la obligación de interrumpir inmediatamente la intervención si los elementos de convicción tenidos en cuenta para la medida desaparecieren o hubieren alcanzado su objeto.

Cabe recordar a esta altura la limitación impuesta a la duración de la medida por la ley española antes comentada, que establece un plazo mucho mayor de tres meses, prorrogables por iguales períodos hasta un máximo de dieciocho meses. La ley mendocina desde la interpretación de su texto, no parece permitir la prorroga más que por una sola vez, es decir, solo sesenta días más.

Siguiendo la norma procedimental mendocina, más amplia que la nacional, se advierte también el impedimento de autorizarse la intervención de aquellas comunicaciones practicadas entre el imputado y el abogado defensor, lo que encuentra lógica desde la protección del derecho de raigambre constitucional y convencional a la defensa en juicio, aplicado a la necesidad de todo imputado de poder comunicarse libremente con su abogado defensor.

Sobre la motivación de la resolución judicial, la jurisprudencia argentina se ha expresado en numerosos fallos, estableciendo desde su lugar y a través de cada caso concreto, lineamientos para la realización de la medida, en resguardo de las previsiones constitucionales.

La Corte suprema de justicia en este sentido ha dicho que el secreto de las comunicaciones, como derecho federal protegido constitucional y convencionalmente, sólo es realizable de modo efectivo restringiendo ex ante las facultades de los órganos administrativos para penetrar en él, sujetando la intromisión a la existencia de una orden judicial previa debidamente fundamentada, exigencia esta última que se deriva del mismo artículo 18 de la Constitución Nacional. Sólo en este

[94] TOF de Mar del Plata, causa "T.A." (1999) "No puede durar indefinidamente, sine die" "CPPN permite extraer un plazo máximo de interceptación telefónica que es el asignado al Juez para concluir la Instrucción (art. 207 CPPN)" – Es decir, 4 meses, prorrogables por 2 más

sentido puede asegurarse que los jueces, como custodios de esa garantía fundamental, constituyen una valla contra el ejercicio arbitrario de la coacción estatal, pues, si su actuación sólo se limitara al control ex post, el agravio a la inviolabilidad de este derecho estaría ya consumado de modo insusceptible de ser reparado, ya que la Constitución no se restringe a asegurar la reparación sino la inviolabilidad misma. Esa es la inteligencia que, por otra parte, acuerda el Código Procesal Penal Nacional, al establecer que la resolución del juez que ordene la intervención judicial deberá ser siempre fundada[95].

Así, establece que para autorizar una orden de registro de las comunicaciones telefónicas a los fines de develar su secreto y conocer su contenido, es necesario que sea dictada por juez, solo cuando medien "elementos objetivos idóneos para fundar una mínima sospecha razonable"[96]

Todos los elementos materiales que constituyen los presupuestos de la orden de intervención de las telecomunicaciones deben ser reconocibles en el auto del juez que la ha decidido. En general, debe reunir, cuanto menos la referencia a: a) los elementos del hecho que sustentan la sospecha; b) la necesidad e idoneidad de la medida para conseguir el fin perseguido, c) las valoraciones en torno a la gravedad del hecho que justifican la injerencia. Es la invocación de estos elementos la que, en definitiva, permitirá conocer el juicio seguido por el juez, y posibilitará ex post el examen de proporcionalidad en cuanto mecanismo para evitar injerencias arbitrarias. No bastarán las meras alusiones a sospechas genéricas de que se están cometiendo o se han cometido delitos, ni rumores, corazonadas o intuiciones, sino que debe haber una inferencia fundada y relevante basada en las circunstancias fácticas objetivas que obren a disposición del juez[97].

Ahora bien, la jurisprudencia reseñada, ha sido desarrollada en relación a las comunicaciones telefónicas, y es en relación a ellas que ha habido mayor evolución en cuanto a la posibilidad de interceptación en tiempo real de las mismas, delimitando el marco de injerencia que esta medida significa.

Sin embargo, el avance de la tecnología conlleva la posibilidad de nuevos modos de comunicación, que son mucho más amplio que la telefónica, que solo

---

[95] CSJN, "Quaranta, José Carlos", 31/08/2010, fallo 333:1674, www.laleleyonline.com.ar, AR/JUR/45956/2010

[96] CSJN, "Quaranta, José Carlos", 31/08/2010, fallo 333:1674, www.laleleyonline.com.ar, AR/JUR/45956/2010.

[97] CNCP, sala II, "Herbas Ramirez, Rubén Ricardo s/ rec. de casación", causa N° 7793, 21/05/12, http://jurisprudencia.pjn.gov.ar/jurisp/principal.htm

transmite un contenido oral. Hoy, a través de las comunicaciones electrónicas, no solo se puede comunicar oralmente, sino también y al mismo tiempo transmitir imágenes, documentos, videos y hasta comunicarse a través de videollamadas. Las comunicaciones en la actualidad trascienden la mera comunicación verbal a través del teléfono, siendo hoy común realizar una comunicación por servicios de telefonía vía IP como *Skype* o *WhatsApp*, la transmisión por internet de todo tipo de mensajería escrita, incluidas fotos, videos u otro tipo de documentos.

Esta comunicación digital expuesta, contiene además, otro tipo de información, anexada a la propia comunicación, que excede a aquella que de una comunicación telefónica puede obtenerse, tal como aquella relativa al tráfico (usuario que lo envía, destinatario, fecha, dirección IP desde la que se generó, ubicación de dicha IP, etc.) o la que se encuentra relacionada al documento adjunto a dicha comunicación (por ejemplo sistema operativo que se utilizó para crearlo, fecha y usuario de creación y/o modificación).

La interceptación de una comunicación implica consecuentemente el conocimiento de toda esa cantidad de información y, por tanto, merece un estándar de sospecha y necesidad que justifique esa mayor intromisión, no solo por ser una injerencia más profunda, sino también, por cuanto, en una comunicación telefónica, una persona, aún con una expectativa razonable de privacidad, es consciente de la información que emite, mientras que en una comunicación electrónica existe una gran parte de información que se pone en circulación en forma inconsciente, sin que ello sea parte del contenido esencial de la información, siendo involuntario por la estructura del sistema informático a través del cual se realiza la comunicación[98].

En este sentido, la legislación argentina, tanto sustantiva como adjetiva, no prohíbe la intervención de la comunicación electrónica o informática, aunque haya sido diseñada para la telefónica. De la redacción de su articulado, al hablar de "cualquier otro medio de comunicación" (CPPN- art. 236) o de comunicaciones del imputado "cualquiera sea el medio técnico utilizado" (CPPMza- art. 229; CPPCba- art. 216) se desprende que el término es en sentido amplio, comprensivo también de las comunicaciones electrónicas o informáticas.

Como excepción a esto último aparece la ley 27.063, de aplicación en algunas provincias, que expresamente refiere a la posibilidad de interceptar

[98] PETRONE, Daniel, "Prueba informática" Ed. Didot, CABA, 2015

la correspondencia electrónica o "cualquier otra forma de comunicación" (ley 27.063- art. 143), fórmula a través de la cual incluye y regula la intervención de todo tipo de comunicación, sea por la vía que fuere.

Asimismo, la propia ley 25.520, actualizada por ley 27.126, expresamente refiere la inviolabilidad de estas por cualquier sistema de envío de objetos o transmisión de imágenes, voces o paquetes de datos, así como cualquier tipo de información, archivos, registros y/o documentos privados o de entrada o lectura no autorizada o no accesible al público, salvo dispensa u orden judicial, reconociendo la posibilidad de interceptación más allá de la telefónica.

Sin embargo, no existe una discriminación legislativa especifica según cada tipo de comunicación, por lo que las posibilidades de su interceptación parecieran regirse no solo por los mismos principios, sino también por los mismos estándares, a pesar que, como ya se ha expresado, la comunicación electrónica conlleva necesariamente mayor información y por tanto su interceptación implica mayor grado de injerencia en la intimidad y privacidad del sujeto.

En este sentido, la legislación española ha avanzado mucho más, al desarrollar en un capítulo especial, todo lo relativo a las comunicaciones electrónicas o informáticas, en primer lugar a través de reglas y principios generales para toda medida relativa al almacenamiento y recopilación de datos informáticos, para luego expresar las reglas privativas para la interceptación en tiempo real de las comunicaciones electrónicas, teniendo especial ahínco en las particularidades que dicha medida presenta en contraste con los derechos constitucionalmente protegidos.

El Convenio de Budapest también desarrolla específicamente la posibilidad de interceptar comunicaciones electrónicas o informáticas. Y lo hace, distinguiendo la interceptación de datos de tráfico y de contenido, considerando esta última más intrusiva y consecuencia exigiendo la aplicación de esta medida solo en ciertos delitos graves, que cada Estado expresamente determine (Convenio de Budapest- art- 21), la que no puede ser más amplia que aquella que se exige para cualquier tipo de medida relativa a un dato o sistema informático (Convenio de Budapest- art. 14).

También prevé la posibilidad de obligar al proveedor de servicios a obtener o grabar con medios técnicos existentes en el territorio o a prestar colaboración o asistencia para tal tarea, siempre en la medida de sus capacidades técnicas.

Todos estos aspectos específicos a las comunicaciones telemáticas no se encuentran regulados en las leyes argentinas, más allá de la sanción de la ley 27.411 referida. Así, no distingue si la medida va destinada a datos de tráfico o de contenido, si las mismas pueden ser utilizadas para la investigación de cualquier delito o solo respecto a aquellos específicamente determinados, etc., todas situaciones que se encuentran previstas en el Convenio de Budapest suscripto por Argentina, pero que no han encontrado reglamentación específica.

Nuevamente la analogía en materia de coerción procesal aparece, a pesar de las diferencias antes reseñadas y de la mayor intrusión que dicha medida implica.

C. Interceptación de correspondencia

La intervención de la comunicación tiene en la legislación procesal argentina dos finalidades distintas, según que la orden sea para impedir la comunicación o para conocerla. En el primer caso, lo que se protege es la libertad de expresión, y en el segundo, el derecho a la intimidad, ejercido a través de la comunicación a distancia.

Adentrarse en el contenido de la comunicación tiene la misma significación que ingresar en la intimidad del domicilio, o intervenir una conversación telefónica.

En el caso de la correspondencia postal o telegráfica, el elemento distintivo respecto a las comunicaciones telefónicas es la palabra escrita. Esta nota distintiva, implica que, en principio, no se justifique delegar en otra autoridad más que la incautación de la pieza postal y reservar el examen del contenido al juez que dispuso la medida y sea éste quien realice un análisis de pertinencia del contenido del mensaje, siempre en el marco de un juicio de necesidad, especificidad y proporcionalidad de la medida, en resguardo de la mínima lesividad posible.

En este aspecto, hay una notable asimilación con la correspondencia electrónica o *e-mail*, compartiendo ambas la escritura como vía de comunicación. Así lo ha entendido también la jurisprudencia argentina, al equiparar la correspondencia epistolar con la electrónica[99].

[99] C. Casación Penal, sala I, 7/11/2008, "Ventura Luis", AP n. 70051479; C. Nac. Crim. y Corr., sala VII, 9/10/2008 "Abreu Carlos A.", AP n. 70049340

Sin embargo, el transporte virtual y no físico del mensaje conlleva que deba ser diferente el modo de adquisición de la prueba.

Así, el mensaje puede ser adquirido por vía del examen de la memoria de la computadora o *Smartphone* del emisor o el receptor, no por vía de secuestro, sino de pericia informática dado que lo que se busca no es una cosa sino registro magnéticos o de memoria.

También puede ser necesario en el marco de una investigación, interceptar en tiempo real una comunicación por vía de *emails*, para lo cual la tecnología de *softwares* ha avanzado notoriamente, permitiendo en forma remota la obtención de dichas comunicaciones.

Se ha definido el correo informático como toda correspondencia, mensaje, archivo, dato u otra información electrónica que se transmite a una o más personas por medio de una red de interconexión entre computadoras. Es un sistema mediante el cual se puede enviar y recibir mensajes desde una casilla de correo de una persona hacia la casilla de correo de otra. Es un sistema que permite la emisión y recepción de mensajes. Es un mecanismo de transmisión caracterizado por ser: un medio electrónico (utiliza medios electrónicos de gestión y transporte); asincrónico (no necesita sincronía de envío y recepción); ubicuo (permite su acceso en diferentes lugares); digital (utiliza información digitalizada); informático (está en relación con las tecnologías de la información). Se sindican como sus marcadas ventajas: rapidez y fiabilidad en la recepción y envío de mensajes; no requiere simultaneidad del remitente y el receptor; facilidad de archivo, reenvío e integración; bajo costo[100]

Los presupuestos de la interceptación de correspondencia, su previsión constitucional y reglamentaria, por fuerza de los avances tecnológicos fueron extendidos pretorianamente, en doctrina, y por último, en reformas legislativas, al campo de las intervenciones telefónicas[101].

"Siempre que se considere útil para la averiguación de la verdad" y la existencia de "decreto fundado de juez", son los requisitos que las normas procesales

[100] VANINETTI, Hugo A., "correo electrónico como herramienta de trabajo y facultades de control", publicado en RDLSS 2015-24, 29/12/2015, 2485, cita online: AP/DOC/1150/2015

[101] FLEMING, Abel, LOPEZ VIÑALS, Pablo, "Garantías del imputado", Ed. Rubinzal Culzoni, Santa Fe, 2007

han utilizado para poder interceptar o secuestrar una correspondencia[102] (CPPMza- art. 227; CPPCba- art. 214).

Es importante destacar que las legislaciones, al hablar de correspondencia hacen referencia a la interceptación y no a la intervención, hecho que plantea un conflicto cuando hablamos de correspondencia electrónica, ya que hoy es posible el conocimiento de la misma, no solo por la aprehensión del soporte físico que sirve de vehículo, sino también en forma remota a través del monitoreo de mensajes de correos electrónicos a través de la creación de "cuentas espejo"[103].

Desde un punto de vista restrictivo, la correspondencia electrónica se asimila por nuestra jurisprudencia a la correspondencia epistolar y esto implica la aprehensión física sin solución de continuidad de su soporte material, ya que la propia Cámara de casación penal ha sostenido que el término "interceptar" significa apoderarse de una cosa antes de que llegue al lugar o a las personas a las que se destina, y la imposibilidad de la observación o monitoreo.

Sin embargo, desde un mirador más amplio, el art. 236 CPPN hace referencia a la intervención de cualquier otro medio de comunicación del imputado para impedirla o conocerla, lo que implicaría la facultad judicial de acceder al monitoreo de las comunicaciones que fueren *online* y en tiempo real o de modo inmediato para conocer su contenido sin interrumpir el proceso de remisión[104].

La importancia de ello se suscita al definir las reglas aplicables, es decir, si resultan aplicables las normas de la interceptación de la correspondencia (CPPN- art. 234 y 235; CPPMza.- art. 227) o de la intervención de las comunicaciones (CPPN- art. 236; CPPMza.- art. 229).

La asimilación hecha por parte de la jurisprudencia del *email* al correo postal parece indicar que solamente el procedimiento de la interceptación del mensaje es el aplicable, tornando impracticable el uso de las "cuentas espejo".

Ello trae, como consecuencias algunas dificultades prácticas. Una de ellas es que al ser aplicables las normas de la interceptación de correspondencia, deberá ser el juez quien revise la totalidad de la misma y decida si es pertinente o no a la

[102] Código Procesal Penal de la Nación, Ley 23984, art. 234 Dicha norma refiere como requisitos "siempre que fuere útil para la comprobación de la verdad" y exige auto fundado del juez y no decreto fundado.
[103] BLANCO, Hernán, "La adaptación de los medios de prueba a la realidad tecnológica en el nuevo código procesal penal: un avance a medias", www.rubinzalculzoni.com.ar, cita online RC D 472/2015
[104] ROMERO VILLANUEVA, Horacio J. y GRISETTI, Ricardo "Código Procesal Penal de la Nación, comentado, Ley 27.063", Abeledo Perrot, C.A.B.A., 2015

investigación (CPPN- art. 235; CPPMza.- art. 228), lo que no se condice con el volumen de correspondencia digital que recibe una persona en la actualidad, si comparamos con aquella epistolar que refería la norma originalmente.

Asimismo, la decisión exclusiva del juez en torno a la pertinencia probatoria de cada correo electrónico probablemente se base en su contenido o archivos adjuntos. Pero esa sola verificación deja afuera un montón de datos que contienen los mails y que solo pueden ser interpretados con la traducción de los datos de tráfico. Estos metadatos pueden ser útil, más allá de lo que a simple vista pueda observarse, pudiendo privar a las partes, fiscal o defensa, de prueba que hace a su interés procesal, al desechar la incorporación de correos que, a juicio del juez, no se vinculan con el objeto procesal[105].

El nuevo código procesal penal de la nación, sancionado por ley 27.063, en su art. 143, regula de un modo diferente la cuestión, al establecer de modo amplio la posibilidad de intervenir una comunicación, sin importar si esta es postal, telegráfica, electrónica o cualquier otra forma de comunicación, lo que incluye la telefónica u telemática.

De su redacción, aunque no muy clara, puede deducirse que el art. 143 es de aplicación cuando lo que se busca conocer y obtener es la comunicación en tiempo real, al momento en que se está produciendo y en razón de ello, prevé un plazo de duración de 30 días, renovable, que deberá procederse de modo análogo al allanamiento (ley 27.063- art. 132), que será una medida excepcional y que el juez controlará la razonabilidad y legalidad del requerimiento.

En caso que la correspondencia ya haya sido recibida por el destinatario, sería de aplicación el art. 144 que prevé el registro de un sistema informático o medio de almacenamiento electrónico, rigiendo las condiciones del art. 129 para la inspección de cosas y lugares, las limitaciones del secuestro de documentos y las reglas de apertura y examen de correspondencia una vez secuestrados los componentes del sistema u obtenida la copia de los datos.

Sobre esto último, el art.145 de dicho nuevo código procesal penal de la nación fija que será el Ministerio Público Fiscal quien proceda a la apertura de la correspondencia recibida o efectos secuestrados, examinando y leyendo los mismos y será éste quien, en audiencia unilateral solicitará al Juez mantener el secuestro de los

[105] PETRONE, Daniel, "Prueba informática" Ed. Didot, CABA, 2015

objetos que tuvieran relación con el proceso. Del resto el juez mantendrá la reserva y dispondrá su devolución, bajo constancia.

En definitiva, respecto a la correspondencia electrónica, la ley 27.063 distingue según la misma este en curso o sea necesaria la intervención de la comunicación en tiempo real, para lo cual deberá regirse por las reglas del allanamiento, o si la misma ya fue recibida, es necesario el registro del sistema informático donde se encuentra alojado, lo cual se rige por las reglas de la inspección de lugares y cosas.

El avance respecto a una adecuación tecnológica que se le exige a la normativa procesal es claro, pero no por ello suficiente. Puede advertirse que a pesar de la actualización terminológica, y de comprender en forma expresa la correspondencia electrónica, se pierde la oportunidad de realizar una adecuación más profunda, distinguiendo los parámetros necesarios para autorizar una intervención de comunicaciones electrónicas, según si lo que interesa es el contenido mismo, o si es necesario los datos de tráfico.

El Convenio de Budapest o la normativa española referida lo distinguen, siendo mucho más reservada la posibilidad de intervenir la comunicación misma, es decir su contenido, permitiéndola solo para la investigación de ciertos delitos graves, expresamente determinados.

Sin perjuicio de ello, es importante de esta ley que no distingue el medio de comunicación optado, sea escrito u oral, como tampoco el soporte físico utilizado, que puede ser una computadora, *notebook*, *Tablet*, o *Smartphone*, u otro. Ello adquiere relevancia en la actualidad, en razón del uso cada vez más frecuente de los correos electrónicos en los *smartphones* o de la mensajería de texto a través de la computadora o *notebooks*, lo que hace muy difusa la diferencia que anteriormente se marcaba y que llevaba que se aplicara a los correos electrónicos las reglas de la interceptación de correspondencia y a la mensajería de texto la parte final del art. 236 del CPPN que habilita registro de mensajes de texto recibidos.

Si los correos son correspondencia epistolar, no existe ningún motivo para pensar que lo son menos cuando son enviados o recibidos desde teléfonos móviles. Resulta infundado asumir que una persona tiene más expectativa de privacidad en sus correos que en sus mensajes de texto, por lo que la diferenciación es arbitraria.

La situación solo puede solucionarse por una interpretación *pro homine* que obliga a interpretar las normas a favor del ciudadano y por lo tanto la única

respuesta posible es que ni los mensajes de texto, ni las conversaciones de programas como el de *Whatsapp* o similares ni los correos pueden ser revisados por personal policial[106], siendo necesaria una orden judicial que lo autorice.

[106] PETRONE, Daniel, "Prueba informática" Ed. Didot, CABA, 2015

CAPÍTULO V

V. Agente encubierto digital

Una investigación penal sobre delitos cometidos a través de medios informáticos, o bien, cuyo objeto del delito es la información, conlleva en la actualidad numerosos desafíos para las fuerzas de seguridad. En razón de ello, surgen diversas figuras, tal como el agente encubierto digital, como una herramienta de investigación, a través del cual un agente de seguridad o civil pueda, ocultando su identidad y por medios electrónicos, obtener información útil para el avance de investigaciones de aquellos delitos cuya gravedad lo merite.

Cierto es que la complejidad de algunos delitos requiere un cierto nivel de organización, que ha llevado a las bandas cibercriminales a actuar como empresas, tanto desde el punto de vista de la visión estratégica, como desde la operativa, logística y el despliegue de sus operaciones.

Las organizaciones cibercriminales se organizan de forma jerárquica y cada fase diferente de la cadena cuenta con más de un especialista, cada vez más profesionalizado, todo lo que aumenta los desafíos a la hora de la investigación.

Asimismo, el espacio de la *Deep web* cada vez más accesible para los usuarios, lleva a la necesidad de nuevas herramientas para su detección.

Esencialmente la *Deep Web* no es más que una parte de internet, aquellas cuyos contenidos no pueden ser indexados por los motores de búsqueda tradicionales, como *Google, Yahoo*, etc., lo que le ha dado su nombre como internet profunda u oculta en contraste con la Internet superficial.

Esto puede ser porque son páginas web dinámicas, sitios bloqueados, sitios sin *linkear*, sitios privados, o sitios con contenidos que no son HTML o contextual, o redes de acceso ilimitado.

Dentro de estos últimos, se encuentra el proyecto *TOR*, que es una de las herramientas más conocidas en la actualidad y cuyo principal objeto es el desarrollo de una red de comunicaciones distribuida, de baja latencia y superpuesta sobre internet, en la que el encaminamiento de los mensajes intercambiados ente los usuarios no revela la identidad de la conexión (dirección IP) permitiendo un anonimato a nivel de la red, y que, además, mantiene la integridad y el secreto de la información que viaja por ella.

Para ello, se desarrolló un *software* que construye un circuito de conexiones cifradas a través de repetidores en la red, donde el circuito se extiende un salto a la vez, y cada nodo a lo largo del camino conoce únicamente el nodo que le proporciona los datos y retransmitir los cuales se los entrega. De esta forma, un nodo de forma individual nunca conoce el recorrido completo que ha tomado un paquete de datos. El cliente negocia un paquete separado de claves de cifrado para cada tramo a lo largo del circuito, asegurándose que la información circulante entre los nodos no pueda ser rastreada. Este circuito de conexión a través de tres nodos distintos cambia cada aproximadamente diez minutos, dificultando aún más cualquier intento de análisis o traqueo de las conexiones circulantes por lo nodos[107].

Más allá del desafío que implica la *Deep Web, TOR* y tantas otros *software* que permiten comunicarse y compartir información, asegurando la privacidad, es importante destacar que cada día más los delincuentes se encuentran más informados respecto a técnicas antirrastreos como antiforenses, complejizando o dificultando la labor de los investigadores.

A modo genérico, las técnicas antirrastreos son aquellas que se utilizan para evitar dejar huellas o rastros de las acciones realizadas, imposibilitando o dificultando el traqueo por las fuerzas de seguridad. En cambio, las técnicas antiforenses buscan que ante el caso que las fuerzas de seguridad obtuvieran los dispositivos, la información que se encuentra en ellos no pueda ser accedida o analizada en el marco de una pericia informática, por ejemplo por contar con procesos como cifrado o borrado seguro.

En definitiva cada vez más las bandas de delincuentes utilizan herramientas tecnológicas que brindan grandes niveles de anonimato, usando conexiones a través de *TOR* y generación de espacios de intercambio en el *Deep Web*.

[107] TEMPERINI, Marcelo y MACEDO, Maximiliano, "Nuevas herramientas de investigación penal: el agente encubierto digital" en Dupuy Daniela y Kiefer Mariana, "Cibercrimen" Editorial BdeF, Buenos Aires, 2017

Estos casos suelen ser los de mayor dificultad de investigación para las fuerzas de seguridad, toda vez que las conexiones suelen cambiar cada pocos minutos, conectándose desde distintos *proxys* anónimos ubicados en distintos lugares del mundo, de difícil cooperación judicial. Particularmente en estos casos es donde se justificaría la utilización del agente encubierto digital, toda vez que a través de la misma sería posible que los investigadores ingresaran en el ámbito de confianza de las bandas de ciberdelincuentes, pudiendo obtener información útil para identificar a los delincuentes por un lado y para probar los delitos por otro.

A. Concepto de agente encubierto. Diferencia con agente provocador

Al decir de José Cafferata Nores, el agente encubierto[108] es un funcionario público que fingiendo no serlo, se infiltra por disposición judicial en una organización delictiva con el propósito de proporcionar desde adentro información que permita el enjuiciamiento de sus integrantes y como consecuencia, el desbaratamiento de esa asociación ilícita; el agente encubierto es aquel funcionario público que simula ser delincuente. Asimismo señala el autor que para que el agente encubierto pueda utilizarse en el caso concreto, debe cumplir con ciertas condiciones:

Excepcionalidad: esto se relaciona con el principio de subsidiariedad, es decir, solo cuando el esclarecimiento de los hechos no es posible lograrlo por otras vías;

Taxatividad: solo se permite en delitos y procesos expresamente determinados y autorizados;

Sanciones: debe haber sanciones especiales para el agente encubierto que aporte datos inexactos o formule imputaciones falsas.

Cardoso Pereira[109] por ejemplo, define al agente encubierto como el policía judicial, especialmente seleccionado, que bajo identidad supuesta, actúa pasivamente con sujeción y bajo el control del Juez, para investigar delitos propios de la delincuencia organizada y de difícil averiguación, cuando han fracasado otros métodos

[108] CAFFERATA NORES, Jose "Cuestiones actuales sobre el proceso penal", Editores del Puerto, Buenos Aires, 200, pp 221-230; obra citada en TEMPERINI, Marcelo y MACEDO Maximiliano, "Nuevas herramientas de investigación penal: el agente encubierto digital" en Dupuy Daniela y Kiefer Mariana, "Cibercrimen" Editorial BdeF, Buenos Aires, 2017

[109] CARDOSO PEREIRA, Flavio, "Agente encubierto y proceso penal garantista: Límites y desafíos", Editorial Lerner SRL, 1ª Ed, Córdoba, 2012, p.363

de investigación o estos sean manifiestamente insuficientes, para su descubrimiento y permite recabar información sobre su estructura y modus operandi, así como obtener pruebas sobre la ejecución de hechos delictivos.

Profundiza el autor[110], al decir que el agente encubierto merece el calificativo de medio de control extraordinario al conllevar una alteración de principios constitucionales básicos y un fuerte ataque a determinados derechos fundamentales, razones ambas determinantes de que su empleo quede sometido al cumplimiento de estrictos requisitos legales, paliativos de los riesgos para las garantías procesales vigentes en un Estado de Derecho.

De esto se desprende que la intervención del agente encubierto requiere que se trate de la investigación de delitos graves, atendiendo no solo a la previsión legal de una pena privativa de libertad alta, sino además a la trascendencia social del delito que se trata de investigar.

En este sentido violaría el principio de proporcionalidad la utilización de agentes infiltrados, a los fines de buscar pruebas, datos e informaciones respecto a delitos sin destacada gravedad y practicados por delincuentes callejeros, incluso aunque actúen en forma mínimamente organizada. Y la explicación es sencilla, pues al tratarse de una técnica policial que presenta una alta carga de restricción de derechos fundamentales su utilización deberá ocurrir en situaciones extremas, cuando las otras formas tradicionales de investigación se demostraren ineficaces u obsoletas.

Detalla asimismo Cardoso Pereira los principios sobre los que debe regir la actuación del agente encubierto[111]:

Principio de legalidad: este implica que el procedimiento de obtención de autorización de una operación encubierta quedará detallado por el ordenamiento jurídico, evitándose situaciones que no se encuentren previstas y reglamentadas y por lo tanto sin previsión legal. No se podrá exigir que la reglamentación de este medio extraordinario revele el modo de actuar del agente encubierto, pues ello conllevaría al fracaso de la investigación y podría en riego la vida e integridad del infiltrado.

Principio de especialidad: debe autorizarse solo en relación a la investigación de un delito concreto, sin que pueda autorizarse de modo genérico ante

[110] CARDOSO PEREIRA, Flavio, ob. cit., p.432-437
[111] CARDOSO PEREIRA, Flavio, ob. cit., p.452-464

cualquier solicitud policial. Es decir solo se aplicará la medida cuando exista la sospecha cierta y sólida que el hecho delictivo se cometerá y nunca con la finalidad de descubrir de modo indiscriminado cualquier conducta delictiva.

Principio de subsidiariedad: Consiste en que este método sea utilizado siempre que se hayan agotado previamente todas las posibilidades de utilización de técnicas y métodos de investigación menos invasivos y restrictivos de derechos y garantías. Ello conlleva que la policía no solo deba poner en conocimiento del Juez todas las diligencias que se han practicado, sino también que no existe otro medio para descubrir los canales por los que se está cometiendo un delito o varios.

Principio de proporcionalidad: Esencialmente consiste que como medio extraordinario de investigación, este solo sea utilizado en casos de extrema y diferenciada gravedad. Ahora bien este principio no solo responde a la limitación de derechos fundamentales sino también a las peculiaridades de este medio de investigación. El uso del engaño efectivo a través de la identidad supuesta, su consideración de medio extraordinario y su consideración como más agresivo con las personas objeto de investigación, son causas suficientes para hacer el principio de proporcionalidad no solo deba estar presente en la adopción de la medida sino en la actuación del agente encubierto con respecto a los demás integrantes de la organización criminal.

Principio de control jurisdiccional: es indispensable la intervención judicial para otorgar el debido valor probatorio a las actuaciones llevadas a cabo por el agente encubierto. Esto surge de la necesidad de protección y tutela de los derechos del investigado, porque al desconocer este la ejecución de la actividad autorizada no puede impugnarla ni autodefenderse de ella, por lo que en garantía de ella, el Juez y el Fiscal deben ser especialmente rigurosos.

Ahora bien, dentro de esta herramienta de investigación, como es el agente encubierto, es necesario distinguirlo del agente provocador, que es aquel sujeto que induce que induce a otro a cometer un delito para que en el intento de realizar el mismo se lo detenga y, eventualmente, se lo declare penalmente responsable por la conducta realizada.

La diferencia entre ambas figuras es que el agente encubierto no está provocando la consumación del delito, ni induce a la conducta ilícita, sino que lo que hace es agregar un eslabón probatorio más dentro del marco de una causa judicialmente controlada. En cambio el agente provocador tiende a inducir a la consumación del delito,

con el claro riesgo de afectación a derechos y garantías, toda vez que el sujeto provocado actúa sin libertad ni espontaneidad ya que el delito surge por la maquinación del agente provocador[112].

Así, cuando la actividad del agente encubierto está dirigida al mero descubrimiento del delito ya cometido previamente, o que se está cometiendo, y que definitivamente con su actuación no se hace nacer la decisión de delinquir en la persona investigada, la misma es totalmente lícita, siendo punible el delito investigado y válidos los medios de prueba obtenidos. Eventuales excesos y actos arbitrarios de los infiltrados deberán ser imputados, siendo los parámetros de proporcionalidad y legalidad los que den el tamiz de análisis de una operación encubierta[113]

B. El Agente encubierto en Argentina. Caso de Mendoza

En la Argentina, el agente encubierto se encuentra regulado por Ley 27319[114], publicada el día 22 de noviembre de 2016[115], cuyo principal objeto es brindar a las fuerzas de seguridad las herramientas y facultades necesarias para ser aplicadas a la investigación, prevención y lucha de los delitos complejos.

Esta ley deroga la anterior regulación prevista en ley 23737 (arts. 31 bis, ter, quater, quinquies y sexies)[116], cuyo alcance era exclusivamente para los delitos previstos en dicha ley y en el art. 866 del Código aduanero.

Por el contrario, esta ley prevé, junto a otras herramientas de investigación, que el agente encubierto pueda ser utilizado en distintas figuras penales que expresamente determina, siempre que se rija por los principios de necesidad, razonabilidad y proporcionalidad.

Así, la ley 27319 amplia el alcance[117] de aplicación de esta técnica a: 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,

[112] TEMPERINI, Marcelo y MACEDO, Maximiliano, "Nuevas herramientas de investigación penal: el agente encubierto digital" en Dupuy Daniela y Kiefer Mariana, "Cibercrimen" Editorial BdeF, Buenos Aires, 2017

[113] CARDOSO PEREIRA, Flavio, "Agente encubierto y proceso penal garantista: Límites y desafíos", Editorial Lerner SRL, 1ª Ed, Córdoba, 2012, p.382-383

[114] http://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/268004/norma.htm

[115] https://www.boletinoficial.gob.ar/#!DetalleNormaBusquedaAvanzada/11512997/null

[116] Art. 19 de ley 27319

[117] Art. 2 ley 27319

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, define como agente encubierto a todo aquel funcionario de las fuerzas de seguridad autorizado, altamente calificado, que presta su consentimiento y ocultando su identidad, se infiltra o introduce en las organizaciones criminales o asociaciones delictivas, con el fin de identificar o detener a los autores, partícipes o encubridores, de impedir la consumación de un delito, o para reunir información y elementos de prueba necesarios para la investigación, con autorización judicial[118].

De dicha definición, se desprende que el agente encubierto debe ser un funcionario de las fuerzas de seguridad autorizado, altamente calificado, descartando la posibilidad que sea un civil quien actúe como infiltrado, quedando a cargo del Ministerio de Seguridad de la Nación la designación e instrumentación necesaria para su protección[119].

La distinción hecha por la ley 27319 respecto a funcionario de las fuerzas de seguridad o policiales, permite concluir que se autoriza que sean agentes encubiertos no solo efectivos policiales, sino también aquellos pertenecientes a las restantes fuerzas de seguridad (Gendarmería Nacional, Policía de Seguridad Aeroportuaria o Prefectura Naval Argentina).

A su vez, debe ser un encargo que deberá ser aceptado voluntariamente por el funcionario de las fuerzas de seguridad designado, no pudiendo su negativa ser tenida como antecedente desfavorable[120].

La actuación del agente encubierto será dispuesta por el Juez, de oficio o a pedido del Ministerio Público Fiscal, siendo además quien deba ejercer el control durante la infiltración, al imponerse la carga sobre el agente de poner en conocimiento del Juez y del Ministerio Público Fiscal la información que se vaya obteniendo.

[118] Art. 3 ley 27319
[119] Art. 4 ley 27319
[120] Art. 3 y 9 ley 27319

Finalmente, la adopción de las disposiciones de esta ley estará supeditada a un examen de razonabilidad, con criterio restrictivo, en el que el Juez deberá evaluar que no exista otra medida más idónea para esclarecer los hechos que motivan la investigación o el paradero de los autores, partícipes o encubridores[121].

Por último, el agente encubierto se encuentra previsto también en otra regulación normativa argentina, cual es el artículo 29 del Código Procesal Penal mendocino[122], presentando algunas diferencias respecto de legislación nacional.

En primer lugar, no es el Juez quien autoriza la utilización de esta herramienta de investigación, sino que será el Fiscal de Instrucción, quien deba hacerlo por resolución fundada. Será al Fiscal de Instrucción, incluso, a quien deba ir poniéndose en conocimiento de las informaciones que se vayan obteniendo, teniendo por tanto la dirección y control de esta medida investigativa.

Más allá del principio acusatorio que rige el proceso penal mendocino, atento la restricción a derechos y garantías fundamentales que implica la utilización de esta herramienta de investigación, no es comprensible que la ley no prevea control alguno por parte del Juez, quien es justamente el garante del proceso penal. Téngase en cuenta que al momento que el imputado o la Defensa de este tome conocimiento, la actividad del agente encubierto ya ha sido desarrollada y, por tanto, ya habrían sido vulnerados los derechos y garantías del primero. El control posterior que hace el Juez, en relación a la validez de la incorporación de las pruebas obtenidas mediante actuación encubierta, no es suficiente, debiendo tener mayor incidencia en la decisión de razonabilidad, necesidad y conveniencia durante el ejercicio de esta herramienta de investigación.

En segundo lugar, no determina expresamente los delitos que pueden investigarse mediante esta técnica, sino que amplía el rango de figuras delictivas a todas aquellas que prevean una pena mayor a tres años de prisión[123]. Cabe resaltar que

---

[121] Art. 12 in fine ley 27319

[122] Art. 29 Código Procesal Penal de Mendoza- Ley 6730: "Actuación encubierta: El Fiscal de Instrucción podrá, por resolución fundada, de manera permanente o durante una investigación, por un delito con pena mayor de tres años, autorizar que una persona o miembro de la policía, actuando de manera encubierta a los efectos de comprobar la comisión de algún delito o impedir su consumación, o lograr la individualización o detención de los autores, partícipes o encubridores, o para obtener o asegurar los medios de prueba necesarios, se introduzca como integrante de alguna organización delictiva, o actúe con personas que tengan entre sus fines la comisión de delito y participe de la realización de alguno de los delitos previstos en el Código Penal y leyes especiales. (…)"

[123] El art. 29 del Código Procesal Penal mendocino expresa solamente "por un delito con pena mayor de tres años", no determinando si refiere a tres años de prisión u otro tipo de pena. Autores como Jorge Coussirat critican el límite legal previsto, aun interpretando que la ley habla de tres años de pena privativa

quedan excluidos del alcance de esta norma, aquellos delitos expresamente determinados como de competencia de la Justicia federal (art. 33 del Código Procesal Penal de la Nación).

El carácter de orden público[124] que las disposiciones de la ley 27319 tienen, no modifica el alcance ni las prerrogativas de la normativa provincial, toda vez que, conforme el sistema federal argentino, son las provincias quienes pueden legislar en materia procesal, siendo facultad exclusiva de las mismas.

En tercer lugar, la norma de rito mendocina habilita que pueda ser agente encubierto un miembro policial o cualquier otra persona, con lo cual abre la posibilidad a que civiles puedan actuar como tal, no siendo imprescindible que sea personal de alguna fuerza de seguridad.

A pesar de las críticas realizadas por parte de la doctrina[125] a dicho requisito amplio, cabe resaltar la utilidad que, en el caso del agente encubierto digital, tiene la posibilidad que no sea un miembro de la policía. Téngase en cuenta que en delitos informáticos, la exposición del agente es solo virtual, a través de un usuario en la red, no existiendo contacto físico con la organización criminal o el autor del delito que se investiga. Por el contrario, el agente encubierto requiere simplemente la creación de un seudónimo o la utilización de uno existente, a fin de ingresar en la red, y tratar a través del mismo de obtener la confianza a fin de lograr los objetivos trazados.

En consecuencia, el hecho que no sea miembro de la policía no representa un riesgo mayor, a diferencia del agente encubierto infiltrado en otro tipo de investigaciones, como puede ser narcotráfico por ejemplo, donde la preparación como agente de una fuerza de seguridad deviene imprescindible. Sin perjuicio de ello, es importante que en caso que sea un civil quien se infiltre, este deberá igualmente respetar las órdenes de quien dirija la investigación, manteniendo las mismas obligaciones que el caso que fuere un funcionario policial.

Finalmente, el Código mendocino prevé que el agente encubierto pueda ser de manera permanente o durante una investigación, lo que también lo diferencia

---

de libertad, refiriendo al mismo como *desmesurado* o *desproporcionado, ya que desnaturaliza el fundamento teórico de ella, que surge de la necesidad de luchar contra grave y peligrosa delincuencia y contra organizaciones criminales*. Ver Coussirat, Jorge y Peñaloza Fernando "Código Procesal Penal comentado de la Provincia de Mendoza" Ed. La Ley, 1ª edición, Ciudad Autónoma de Buenos Aires, 2012, T. I, p.158

[124] Art. 1 ley 27319

[125] Coussirat, Jorge y Peñaloza Fernando "Código Procesal Penal comentado de la Provincia de Mendoza" Ed. La Ley, 1ª edición, Ciudad Autónoma de Buenos Aires, 2012, T. I, p.158.

de la norma nacional, que solo lo autoriza del último modo. La doctrina mendocina[126] critica esta posibilidad de tener un agente encubierto de manera ininterrumpida, expresando que ello atenta con el principio de razonabilidad y necesidad, perdiendo fundamento su utilización, al atentar contra su excepcionalidad.

C. El agente encubierto en España. Previsión del agente encubierto digital

A continuación vale resaltar la normativa española, la que luego de algunas reformas, introdujo en la Ley de Enjuiciamiento criminal el artículo 282 bis[127] que regula el agente encubierto, e incorpora entre ellos el agente encubierto digital o informático.

Dicho artículo en sus incisos 6 y 7 expresa: "6. El juez de instrucción podrá autorizar a funcionarios de la Policía Judicial para actuar bajo identidad supuesta en comunicaciones mantenidas en canales cerrados de comunicación con el fin de esclarecer alguno de los delitos a los que se refiere el apartado 4 de este artículo[128] o cualquier delito de los previstos en el artículo 588 ter a[129]. El agente encubierto

[126] Coussirat, Jorge y Peñaloza Fernando "Código Procesal Penal comentado de la Provincia de Mendoza" Ed. La Ley, 1ª edición, Ciudad Autónoma de Buenos Aires, 2012, T. I, p.158. Allí dice: "En rigor de verdad resulta inimaginable pensar en una actuación encubierta de naturaleza ininterrumpida. Teniendo en cuenta el sistema de competencia funcional que se atribuye a cada uno de los Fiscales de Instrucción, no parece posible que uno de ellos disponga una actuación encubierta con esa amplitud y generalidad sin incurrir en abuso funcional

[127]http://www.boe.es/buscar/pdf/1882/BOE-A-1882-6036-consolidado.pdf

[128] Art. 282 bis Ley de Enjuiciamiento Criminal española. http://www.boe.es/buscar/pdf/1882/BOE-A-1882-6036-consolidado.pdf "4. A los efectos señalados en el apartado 1 de este artículo, se considerará como delincuencia organizada la asociación de tres o más personas para realizar, de forma permanente o reiterada, conductas que tengan como fin cometer alguno o algunos de los delitos siguientes: a) Delitos de obtención, tráfico ilícito de órganos humanos y trasplante de los mismos, previstos en el artículo 156 bis del Código Penal. b) Delito de secuestro de personas previsto en los artículos 164 a 166 del Código Penal. c) Delito de trata de seres humanos previsto en el artículo 177 bis del Código Penal. d) Delitos relativos a la prostitución previstos en los artículos 187 a 189 del Código Penal. e) Delitos contra el patrimonio y contra el orden socioeconómico previstos en los artículos 237, 243, 244, 248 y 301 del Código Penal. f) Delitos relativos a la propiedad intelectual e industrial previstos en los artículos 270 a 277 del Código Penal. g) Delitos contra los derechos de los trabajadores previstos en los artículos 312 y 313 del Código Penal. h) Delitos contra los derechos de los ciudadanos extranjeros previstos en el artículo 318 bis del Código Penal. i) Delitos de tráfico de especies de flora o fauna amenazada previstos en los artículos 332 y 334 del Código Penal. j) Delito de tráfico de material nuclear y radiactivo previsto en el artículo 345 del Código Penal. k) Delitos contra la salud pública previstos en los artículos 368 a 373 del Código Penal. l) Delitos de falsificación de moneda, previsto en el artículo 386 del Código Penal, y de falsificación de tarjetas de crédito o débito o cheques de viaje, previsto en el artículo 399 bis del Código Penal. m) Delito de tráfico y depósito de armas, municiones o explosivos previsto en los artículos 566 a 568 del Código Penal. n) Delitos de terrorismo previstos en los artículos 572 a 578 del Código Penal. o) Delitos contra el patrimonio histórico previstos en el artículo 2.1.e de la Ley Orgánica 12/1995, de 12 de diciembre, de represión del contrabando."

[129] Ley de Enjuiciamiento Criminal española. http://www.boe.es/buscar/pdf/1882/BOE-A-1882-6036-consolidado.pdf; Artículo 588 ter a. "Presupuestos. La autorización para la interceptación de las

informático, con autorización específica para ello, podrá intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido y analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos; 7. En el curso de una investigación llevada a cabo mediante agente encubierto, el juez competente podrá autorizar la obtención de imágenes y la grabación de las conversaciones que puedan mantenerse en los encuentros previstos entre el agente y el investigado, aun cuando se desarrollen en el interior de un domicilio."

Sin lugar a dudas, la regulación del agente encubierto digital, significa un aporte sustancial en la investigación de la delincuencia, tal como viene desarrollándose en la actualidad, siendo cada vez mayor el ámbito digital o informático donde se cometen viejos y nuevos delitos.

A fin de mantener los puntos de análisis realizados en la normativa argentina, cabe decir que la ley española expresa que será el Juez de Instrucción, o el Fiscal dando inmediato conocimiento al Juez, quienes pueden mediante resolución fundada autorizar la utilización de este medio de investigación, así como también son quienes harán el control durante y después de la actuación encubierta.

Asimismo, determina taxativamente cuáles delitos pueden ser investigados mediante esta técnica, los que detalla en el apartado 4 del artículo 282 bis referido. Vale destacar que a dicha lista se agrega aquellos previstos en el art. 588 ter a., cuando el agente encubierto sea autorizado a actuar en canales cerrados de comunicación (agente encubierto informático previsto en el apartado 6 del art. 282 bis).

Ingresando al análisis de este instituto incorporado por la ley española, se observa que el Juez podrá autorizar a un funcionario policial para actuar bajo identidad supuesta en comunicaciones mantenidas mediante canales cerrados de comunicación y agrega que este agente, mediante autorización específica pueda intercambiar o enviar por si mismos archivos ilícitos por razón de su contenido y analizar los resultados de los algoritmos aplicados para la para la identificación de dichos archivos ilícitos.

---

comunicaciones telefónicas y telemáticas solo podrá ser concedida cuando la investigación tenga por objeto alguno de los delitos a que se refiere el artículo 579.1 de esta ley o delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación. Artículo 579.1: (…)1.º Delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión. 2.º Delitos cometidos en el seno de un grupo u organización criminal. 3.º Delitos de terrorismo.

Esta opción es muy importante para la finalidad buscada en la figura, toda vez que, por ejemplo, en el caso de las redes de distribución de pornografía infantil, para pertenecer a un grupo o foro cerrado dedicado a esa actividad, es muy posible que sea necesario que el usuario (agente encubierto digital) tenga que intercambiar o enviar al grupo contenidos de este tipo, a fin de ser aceptado por el grupo y generar la confianza necesaria, generando el entorno adecuado para que posteriormente se puedan llevar a cabo las tareas de recolección de información clásicas de un agente encubierto[130].

Es importante destacar, que la ley española expresamente determina que hace falta una autorización específica para realizar este intercambio, no siendo suficiente la autorización inicial respecto a la actuación encubierta. A tal fin, los principios de razonabilidad y de proporcionalidad imponen al Juez, que deba tener especial cuidado respecto al material que se utilice, buscando en lo posible, material que no sea mayormente degradante, o que las víctimas sean mayores de edad, o que ya hayan sido utilizados anteriormente en otras intervenciones, entre otras opciones que pueden tenerse en cuenta en el caso concreto.

Finalmente en relación a la regulación española, cabe decir que la actuación encubierta digital se encuentra comprendida también por el inciso 5 del art. 282 bis referido, en cuanto excluye de responsabilidad la actuación que sea consecuencia necesaria del desarrollo de la investigación, siempre que se guarden la debida proporcionalidad con la finalidad de la misma y no constituyan una provocación al delito.

[130] TEMPERINI, Marcelo y MACEDO, Maximiliano, "Nuevas herramientas de investigación penal: el agente encubierto digital" en Dupuy Daniela y Kiefer Mariana, "Cibercrimen" Editorial BdeF, Buenos Aires, 2017

CONCLUSIONES

A lo largo de este trabajo, ha podido observarse la importancia de la evidencia digital y el avance de las tecnologías de la información y comunicación en una investigación penal, sea esta por delitos informáticos, cometidos a través de sistemas informáticos o cualquier otro delito.

Las distintas regulaciones procesales en la Argentina, no han acompañado dicho avance del modo que se requiere, tanto en calidad como en precisión normativa. Solo aparecen algunas modificaciones legislativas en los ordenamientos provinciales, entremezcladas con los institutos procesales tradicionales que habían sido pensados para la evidencia física, tales como el registro o la intervención de comunicaciones.

La sanción de la ley 27.411, dispuso la adhesión de la Argentina al Convenio sobre cibercriminalidad celebrado en Budapest, en 2001, en el marco del Consejo de Europa, lo que modifica el escenario legislativo en el país, sobre todo en los aspectos procesales y de cooperación internacional en la lucha contra el cibercrimen.

La adhesión a este convenio internacional implica la incorporación de conceptos y pautas legislativas que Argentina no tenía hasta el momento, al menos aquellas relativas al proceso penal. Cabe recordar que por ley 26.388 ya se había dispuesto ciertas modificaciones en la parte especial del código penal, incorporando ciertas figuras delictivas de conformidad a las previsiones del Convenio de Budapest, lo que también formó parte del proceso de adhesión al mismo.

Asimismo, enuncia y define conceptos claves en el tratamiento de la evidencia digital, que no encuentran distinción en la normativa procesal argentina, tales como sistema informático, datos informáticos, prestador de servicios y sobre todo, el de datos de tráfico, siendo una categoría diferente de los datos de contenido y de aquellos relativos al abonado.

Justamente los datos de tráfico es uno de los aportes diferenciales de la evidencia digital sobre la física, al sumar al propio contenido de una comunicación o archivo, una serie de metadatos que permite a la investigación dilucidar el origen, destino itinerario, hora, fecha, tamaño y duración de la comunicación o el tipo de servicio subyacente. La evidencia física, al contrario, nada suma al respecto, siendo solo lo tangible u observable lo único sustancial en una investigación.

Así, Convenio de Budapest propone una regulación uniformada de los aspectos procesales de la lucha contra el *cibercrimen*, previendo que sea aplicable no solo a la investigación de los delitos enumerados y previstos en el convenio (*ciberdelitos* propiamente dichos), sino también, de todos aquellos delitos cometidos a través de un sistema informático y a la obtención de prueba electrónica de cualquier delito, lo que implica un reconocimiento de la incidencia transversal de la evidencia digital y del uso de las tecnologías de información y la comunicación en toda investigación.

Solo dos excepciones dispone el Convenio que limitan el amplio ámbito de aplicación referido. En primer lugar, la facultad de interceptar los datos relativos al contenido deberá estar limitada a una serie de delitos graves que serán determinados por la legislación nacional. Y en segundo lugar, la facultad de obtener en tiempo real datos relativos al tráfico, debe ser aplicada solo a aquellos delitos previstos en la reserva, siempre que esta no sea más restringida que la serie prevista para la interceptación de datos relativos al contenido.

También establece como salvaguardia, el deber de las legislaciones procesales de proteger adecuadamente los derechos humanos y las libertades individuales, el respeto de los Pactos suscriptos en la materia[131] y principalmente el principio de proporcionalidad.

Sobre el principio de proporcionalidad, será cada derecho interno quien deba definir su alcance, siendo solo ejemplos las limitaciones referidas respecto a interceptación de datos relativos al contenido u obtención en tiempo real de datos relativos al tráfico.

[131] La República Argentina ha suscripto sobre la materia la Declaración Americana sobre los Derechos y Deberes del Hombre, la Declaración Universal de Derechos Humanos, la Convención Americana sobre Derechos Humanos, el Pacto Internacional de Derechos económicos, sociales y culturales, todos los cuales tienen jerarquía constitucional.

Muchas de las medidas procesales que el Convenio establece, implican una injerencia sobre la privacidad o intimidad de las personas, motivo por el cual resulta vital que el principio de proporcionalidad guíe las mismas, en función de la naturaleza de delito y el grado de intromisión de estas.

La eficacia de una investigación criminal, no puede justificar, so pena de las garantías constitucionales, diversas injerencias al ámbito privado fundadas en reglas procesales que no regulan la misma.

Por tanto, el principio de proporcionalidad debe redefinirse, tomando en cuenta, la invasión que significa a la intimidad el desarrollo de las tecnologías de la información y de la comunicación, poco perceptible para el afectado, que resulta aún más agresiva, si consideramos la ilimitada capacidad de almacenamiento e interrelación de datos logrados en sistemas computarizados y en el espacio virtual.

- Una de las medidas que el Convenio de Budapest prevé como necesaria es la relativa a la conservación y revelación de datos informáticos y en este sentido dispone tres variables para que cada Estado parte adopte en sus legislaciones internas.

En primer lugar, regula la facultad de ordenar o imponer la conservación inmediata de datos electrónicos especificados almacenados a través de un sistema informático, incluidos los datos de tráfico, cuando haya razones para pensar que son susceptibles de pérdida o de modificación.

Para destacar es el plazo de noventa días que dispone como máximo para la conservación, el que puede ser renovado y la obligación de secreto que se debe imponer al destinatario de la medida, a fin de proteger la eficacia de la medida y la intimidad del sujeto de los datos a resguardar.

En segundo lugar, prevé que se adopten las medidas legislativas para que cada Estado parte pueda procurar la conservación inmediata de los datos de tráfico cuando uno o más prestadores de servicio haya participado en la transmisión de dicha comunicación y asegurar la comunicación inmediata a la autoridad competente de datos de tráfico suficientes para permitir la identificación de los prestadores de servicio y de la vía por la que la comunicación se ha transmitido.

La necesidad de esta medida es esencialmente práctica, por lo que la operatividad es imprescindible para la eficacia de la medida, puesto que lo que se busca es identificar a los proveedores del servicio que intervinieron en una comunicación

determinada y la vía de comunicación, con el fin que estos puedan conservar los datos informáticos almacenados.

Finalmente, en tercer lugar, dispone que cada Estado Parte pueda ordenar a una persona que comunique los datos informáticos especificados almacenados en un sistema informático o en un soporte de almacenamiento informático o, a los proveedores de servicios que aporten datos relativos a los abonados y que conciernan a tales servicios.

Esta disposición refiere a datos almacenados ya existentes, excluyendo los datos de tráfico o los datos de contenido de comunicaciones futuras. Ello implica que sea una medida menos invasiva que otras, tales como el registro o la confiscación de datos, siendo ella una alternativa valiosa, en coherencia con el principio de proporcionalidad.

Como miembro del Consejo de Europa y signatario del Convenio de Budapest, España introdujo modificaciones a su ley de enjuiciamiento criminal acordes a las pautas establecidas por este, debiendo resaltarse que puede ser el Fiscal o la Policía Judicial quien requiera la conservación y protección de los datos concretos, no siendo necesario una orden judicial para ello. Ello presenta lógica, por cuanto no existe de parte del requirente un conocimiento de dichos datos y por tanto no hay una intrusión en la privacidad del usuario de estos. Recién cuando de la investigación surja la necesidad de revelarlo y por tanto pueda justificarse el conocimiento de estos, es necesaria la orden judicial que así lo disponga.

Al revisar la situación legislativa en Argentina, fue necesario distinguir la retención de datos de tráfico respecto a la conservación de estos, pudiendo concluirse que mientras esta última, debe ser mediante requerimiento expreso, en el marco de una investigación judicial concreta iniciada sobre datos ya existentes y almacenados, la retención es previa al inicio de alguna investigación y sobre los datos que se van produciendo, en tiempo real, independientemente si son requeridos por alguna autoridad en el marco de una investigación.

Sobre retención de datos de tráfico, se sancionó la ley 25.873, luego reglamentada por decreto 1563/04, que modificó la ley 19.978 conocida como "ley de telecomunicaciones", pero luego fue suspendida inicialmente mediante decreto 357/05 y luego, en el año 2009, declarada inconstitucional por un pronunciamiento *erga omnes* de la Corte Suprema de Justicia de la Nación (caso "Halabi").

De este fallo, es importante destacar que la Corte resuelve la inconstitucionalidad de esa norma de retención en virtud de los términos en los que fue regulada, pero no refiere que cualquier norma que se legisle al respecto sería inconstitucional, por lo que la regulación de esta medida no se encuentra prohibida, sino que deberá hacerse teniendo en consideración las pautas que la Corte Suprema de Justicia dispuso.

Sobre conservación y revelación rápida de datos informáticos en Argentina no existe regulación que incorpore y reglamente tal medida como opción para los investigadores. Ni el código procesal penal de la Nación, ni su reforma, introducida por ley 27.063, legislan respecto a esta medida.

El código procesal de la provincia del Neuquén solo prevé la posibilidad de ordenar la conservación de datos informáticos hallados ya en un dispositivo de almacenamiento de datos informáticos y no la posibilidad de ordenar a un proveedor de servicios que conserve ciertos datos por un tiempo, ante la eventual necesidad de ser requerido oportunamente por un Juez.

Por tanto, más allá del avance en materia de evidencia digital que regula el código procesal neuquino, se advierte la falta de regulación en Argentina de esta medida.

Como propuesta, es valiosa la regulación de la ley de enjuiciamiento criminal española que establece como medida de aseguramiento la orden de conservación de datos a cualquier persona, física o jurídica, por un tiempo determinado o hasta que se obtenga la autorización judicial para su revelación y pone en cabeza del Ministerio Público Fiscal y de la Policía judicial la facultad de requerirla.

Distinta es la situación respecto a la orden de presentación en Argentina, toda vez que esta medida encuentra recepción legislativa en los ordenamientos procesales (art. 232 CPPN; art. 211 CPPCba; art. 224 CPPMza, entre otros), como medida sustitutiva del secuestro.

Más específica es la ley procesal neuquina que permite requerir a cualquier persona física o jurídica que preste un servicio a distancia por vía electrónica, la entrega de la información que esté bajo su poder o control referida a los usuarios o abonados, o los datos de los mismos (art. 153).

Una característica importante reside en que el objeto se refiere de modo exclusivo a datos informáticos que obren en poder o estén bajo el control del tercero

ajeno al hecho ilícito, ya que la orden de presentación es solo aplicable a datos que éste ya tiene almacenados en sus sistemas.

Sobre quien puede requerir la presentación de los datos informáticos, será necesario distinguir si estos son de contenido, de tráfico o relativos al abonado, siendo más claro que se requiera orden judicial para los primeros y pueda pedirlos el Fiscal aquellos relativos al abonado.

Respecto a los de tráfico, si bien no ingresan demasiado en la esfera de la intimidad, cierto es que si uno logra obtener una cantidad suficiente de ellos, puede hacerse una idea suficientemente precisa de la ubicación georreferenciada, en determinados periodos de tiempo o las características técnicas de las comunicaciones y las plataformas utilizadas, por lo que el grado de injerencia en la intimidad y privacidad pasa a ser significativo.

En consecuencia, en los ordenamientos regidos por el sistema acusatorio será el Fiscal quien pueda emitir la orden de presentación, con excepción de los datos relativos al contenido, o de aquellos relativos al tráfico referidos en el párrafo anterior, donde será el Juez quien deba disponerla.

- También se encuentra previsto en el Convenio de Budapest, el registro y decomiso de datos informáticos almacenados, y esto fue analizado en el capítulo III del presente trabajo.

Para ello inicialmente fue necesario definir la evidencia digital, distinguiendo sus características respecto a la física, surgiendo tres variables críticas a considerar durante las actividades de identificación y preservación de evidencia digital: temporalidad, volumen y ubicuidad. La evidencia digital es capaz de permanecer en un dispositivo de almacenamiento por segundos o bien por años, puede tratarse de un solo bit o de millones de ellos y finalmente es susceptible de estar localizada en un único dispositivo de almacenamiento o distribuido por el mundo.

El Convenio de Budapest, expresa que cada Parte deberá otorgar facultades a sus autoridades competentes a fin que ellas puedan registrar o acceder de cualquier modo a todo sistema de datos informáticos o los datos allí almacenados o todo dispositivo de almacenamiento de datos informáticos.

La previsión de acceso “de cualquier modo”, implica no solo una actualización terminológica más atinada a la actualidad informática, sino que implica asimismo, que no solo a través de la obtención física del dispositivo puede registrarse el

mismo, sino también de forma remota, a través de softwares específicos o del modo que fuera necesario y proporcional según la tecnología disponible.

Asimismo, prevé la facultad de acceder a un sistema informático y sus componentes conexos, o acceder a otro sistema informático donde se considere se encuentran los datos buscados, siempre que sea accesible o disponible este sistema desde el sistema informático esencial. En esta última hipótesis, el Convenio establece la posibilidad de extensión de la medida inicialmente tomada.

Seguidamente, prevé el Convenio la facultad de confiscar u obtener de un modo similar los datos informáticos a los que haya accedido, lo que implica la facultad de obtener un sistema informático o un dispositivo de almacenamiento informático, realizar y conservar una copia, preservar la integridad de los datos informáticos almacenados y hacer inaccesibles o suprimir datos informáticos del sistema consultado.

En Argentina no ha habido buena recepción legislativa, al no haber prácticamente normas específicas que regulen el acceso a los sistemas informáticos o a datos informáticos almacenados.

Solo la provincia del Neuquén ha previsto en su ordenamiento procesal la posibilidad del secuestro del dispositivo informático, o la obtención de una copia, cuando se hallaren dispositivos de almacenamiento de datos informáticos que por las circunstancias del caso hicieran presumir que contienen información útil a la investigación, o la posibilidad de registro por medios técnicos o en forma remota.

Esta norma implica un avance sin dudas hacia la adecuación de nuestros ordenamientos procesales a la realidad tecnológica imperante y a las normas del Convenio de Budapest, pero esta situación no es uniforme en el país.

Necesariamente, para acceder a los mismos se debe recurrir a institutos como el registro o allanamiento, si el sistema informático se encuentra en un lugar cerrado, o la requisa, si el mismo se encuentra en posesión de una persona.

Y en este sentido, tanto para el registro como para la requisa se requiere orden judicial motivada que justifique el ingreso a un domicilio o la revisión a una persona, siempre en el marco de cumplimiento de los principios de especialidad, razonabilidad y proporcionalidad.

Sobre el alcance de una orden de registro domiciliario o requisa personal ante el hallazgo de un dispositivo informático y la necesidad de su inspección

por su utilidad en la investigación, es importante distinguir tres niveles, según el grado de vulneración de la medida, lo que no se aprecia de las regulaciones procesales argentinas.

Un primer nivel, surge de la necesidad de identificar, inventariar, conservar y ubicarlos en una cadena de custodia. En un segundo nivel se encuentran los datos de tráfico, que son los que rodean a la comunicación o al propio archivo informático. Y en un tercer nivel, se halla el contenido mismo del dato informático almacenado, esto es, el archivo, documento, imagen, comunicación, etc.

La posibilidad de inspección o acceso al dispositivo informático hallado en el domicilio o la persona cuyo registro fue autorizado debidamente, depende esencialmente del propósito y alcance de la propia resolución, debiendo expresarse en forma precisa si se autoriza la inspección en lo que hace referencia al segundo y tercer nivel referidos, siendo el acceso en este último caso más restrictivo aún.

Ante la menor injerencia que un registro de aquellos datos referidos en el primer nivel tiene respecto al derecho a la privacidad de la persona investigada, siempre que ello sea atinente y útil a la investigación que motivó la orden judicial, bastará la resolución judicial que permitió el ingreso al domicilio o la requisa personal para la revisión de tales datos.

En consecuencia, la orden judicial debe disponer específicamente el acceso al dispositivo informático hallado durante un registro domiciliario o requisa personal, no bastando los motivos iniciales de la resolución para acceder a la información contenida en tales dispositivos, lo que encuentra lógica si se comprende que dicho dispositivo puede almacenar mucho más que un archivo físico o domicilio, siendo por tanto mayor la injerencia a la privacidad de la persona investigada.

En caso que se advierta o se tenga la sospecha que la información buscada no se encuentra en dicho aparato o soporte físico, sino que se encuentra alojada en otro servidor ubicado en otro domicilio o en una nube, cuyo servidor también se encuentra ubicado en otro destino, siempre que el dispositivo informático se encuentre en el espacio físico cubierto por la orden de allanamiento, no se presta atención a la ubicación física del servidor al que se está accediendo.

Esta solución parece la correcta y se corresponde con el Convenio de Budapest.

Asimismo, ante la posibilidad de acceder a un dispositivo informático en forma remota a través de la red internet o telefónica, mediante el uso de

programas espías, o por defecto de las condiciones de privacidad que el usuario establece en su máquina, salvo en el ordenamiento procesal de la provincia del Neuquén, no hay regulación expresa, y por tanto, es necesario establecer la regulación aplicable, apareciendo nuevamente las previsiones respecto al registro domiciliario o la requisa personal.

Pudo observarse en este sentido que el examen a distancia implica una mayor vulneración a la persona que es sujeto de la medida, por cuanto, la misma se realiza sin el conocimiento de este, es decir, sin conocimiento de quien puede oponerse a la medida.

La normativa española, que prevé esta posibilidad de registro en forma remota, sin conocimiento del sujeto de la medida, establece que pueda ordenarse la misma solo respecto a determinados delitos graves, lo que implica un reconocimiento de la mayor injerencia de esta modalidad de registro.

Por tanto, cuanto más fácil y menos costoso resulte acceder a alguna de estas áreas, más debe rodearse a la misma de protecciones que eviten reducir el derecho a la intimidad a un valor nulo, lo que explica la necesidad de una regulación específica que reglamente esta modalidad a distancia.

Sobre la confiscación u obtención de los datos informáticos a que se haya accedido, se ha determinado que, a diferencia de una evidencia física obtenida, la evidencia digital requiere un tratamiento distinto, en razón de su volatilidad, escaso tamaño físico, aunque no de volumen de información, su dificultad para ser visualizada, la posibilidad sencilla de ser modificada, alterada o borrada, incluso remotamente.

El Convenio de Budapest prevé la facultad de confiscar u obtener un sistema informático, una parte o un dispositivo de almacenamiento masivo, realizar y conservar una copia de esos datos informáticos, preservar la integridad de los datos informáticos almacenados pertinentes y hacer inaccesibles o suprimir dichos datos informáticos del sistema informático consultado.

La ley de enjuiciamiento criminal española tiene una regulación específica acorde con las previsiones del Convenio de Budapest, al establecer la necesidad de una resolución judicial que autorice expresamente la realización de copias de los datos informáticos obtenidos, la que indicará también las condiciones necesarias para asegurar la integridad de los datos y las garantías de su preservación, para hacer posible en caso que sea necesario la práctica de un dictamen pericial. La simple incautación de los

soportes físicos donde se encuentran los datos informáticos, no legitima el acceso a su contenido, sea que fueron obtenidos en un registro domiciliario o con independencia de este. Es necesario una orden específica que así lo autorice.

En Argentina, sin perjuicio de la sanción de la ley 27411, que dispone la adhesión al Convenio de Budapest, no existe una norma específica referida a la obtención de datos informáticos.

En la práctica, las regulaciones sobre secuestro (CPPN- art. 231; CPPCba- art 210; CPPMza- art. 223) han sido utilizadas analógicamente cuando la investigación requería la obtención de evidencia digital.

En forma similar dichas normas disponen que se podrá disponer que sean conservadas o recogidas las cosas relacionadas con el delito, las sujetas a confiscación o aquellas que puedan servir como prueba. Dicha medida deberá ser dispuesta por el Juez, pudiendo ser por el Fiscal de Instrucción, cuando no sea necesario una orden de allanamiento.

Respecto a la cadena de custodia, las características especiales de la evidencia digital, especialmente su volatilidad e inmaterialidad, requieren que el tratamiento de la misma sea distinto a la evidencia física, siendo necesario ciertos recaudos diferentes para preservar la misma y llevarla a juicio debidamente.

A nivel internacional, puede observarse ciertas guías de buenas prácticas para la recolección de evidencia digital, que recomiendan ciertas precauciones especiales que se deben tomar al momento de recolectar, manipular, documentar y examinar la evidencia digital, ya que de lo contrario dicha prueba puede tornarse inválida a los fines judiciales, o, en su caso, mostrarse imprecisa a efectos de esclarecer el hecho.

Una de ellas es la publicada en el Reino Unido por la *Association of Chief Police Officers* (ACPO, 2004, 2012) y otra es la norma ISO/IEC 27037:2012. Ambas han sido receptadas en Argentina por el Ministerio Público Fiscal de la Nación y por el Poder Judicial de la Provincia de Neuquén, los que han aprobado, en respectivas resoluciones, guías o protocolos de actuación para la obtención, preservación y tratamiento de evidencia digital, en pericias informáticas o en pericias informáticas en telefonía celular.

Más allá de las previsiones de dichos protocolos, las que son desarrolladas en el capítulo, el procedimiento general de investigación judicial, utilizando servicios de informática forense consta de dos etapas principales: a) incautación confiable

de la prueba y mantenimiento de cadena de custodia, y b) análisis de la información disponible con arreglo al incidente investigado y redacción del informe pericial.

La primera etapa debe ser llevada a cabo por personal policial junto al Fiscal, responsable del control o ejecución de la medida. La segunda etapa debe ser efectuada en el laboratorio por un perito siguiendo los estándares de la ciencia forense para el manejo de la evidencia, en función de los puntos de pericia que sean indicados por los operadores judiciales.

En consecuencia, el análisis de la información digital hallada, realizado siempre por una persona especializada en la materia, debe seguir las reglas de la pericia, siempre teniendo en cuenta las especiales características, sobre todo de volatilidad, de la evidencia digital, ya que la falta de seguimiento de las normas relativas a este medio de prueba, pueden acarrear la nulidad del informe pericial, y puede ser necesaria la reproducción y repetición de la medida, más allá del debido control durante y posterior que pueda ejercer la Defensa.

- En el capítulo IV, se analizó aquellas medidas investigativas que tengan por fin la recolección de evidencia digital, en tiempo real, es decir al momento en que se están llevando a cabo.

Así se advirtió inicialmente y en comparación con el registro y decomiso de datos almacenados, la mayor intromisión de una medida de intervención de la comunicación electrónica en tiempo real, por cuanto esta última se realiza a espaldas del sujeto destinatario de la medida. Claramente si la intervención en tiempo real se realiza en conocimiento del comunicante esta pierde total sentido.

También implica una mayor intromisión, respecto a medidas similares que prevé la normativa procesal tradicionalmente como son la interceptación de correspondencia postal y las escuchas telefónicas, en razón de la mayor información que aporta una comunicación electrónica, prácticamente involuntaria o inconsciente que el comunicante transmite, como la duración de la llamada, la fecha en que se realiza, la dirección IP desde la cual se transmite y hasta la ubicación del mismo.

El Convenio de Budapest regula dos medidas, por un lado, recopilar o guardar, en tiempo real, los datos informáticos a través de sus propios medios técnicos existentes y, por el otro, obligar a un prestador de servicios a recopilar o grabar datos informáticos en tiempo real o que preste su colaboración y asistencia para ello.

La principal distinción que realiza el Convenio, deviene de la diferencia entre datos de tráfico y datos de contenido, ya que prevé un ámbito de aplicación más restringido para este último, solo respecto a "infracciones consideradas graves conforme el derecho interno", aun cuando se haya determinado un repertorio de delitos para la obtención de datos relativos al tráfico, conforme al art. 14 del Convenio.

A continuación, esta medida es solo para comunicaciones específicas, no permitiendo ni exigiendo la vigilancia generalizada o indiscriminada de datos informáticos, sino que deben ser claramente determinadas las comunicaciones de las cuales podrá obtenerse la información.

Finalmente, en relación a la facultad de obligar al prestador de servicios, dos particularidades surgen. Por un lado, solo puede obligarse al mismo en la medida de sus capacidades técnicas, por lo que no puede obligarse a obtener los medios técnicos necesarios o capacitar a su personal para la realización de la medida. Por el otro, deberá obligarse al proveedor de servicios a mantener secreto de la medida realizada como de la información obtenida, ya que el éxito y eficacia de la medida dependerá de que la persona vigilada no tenga conocimiento de la misma.

España regula, en consonancia con el Convenio de Budapest, la facultad de interceptar una comunicación en tiempo real, sea aquella practicada a través de medios telefónicos o telemáticos, o sea, la captación y grabación de la comunicación oral a través de la utilización de dispositivos electrónicos o de dispositivos técnicos de seguimiento, localización y captación de la imagen.

Es interesante la regulación española, por cuanto, más allá del cumplimiento como medida de injerencia de la necesidad de autorización judicial, dictada con sujeción a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad, la ley de enjuiciamiento criminal española prevé que esta medida solo puede aplicarse respecto a ciertos delitos determinados o aquellos cometidos a través de medios informáticos.

Sin embargo el catálogo de delitos es bastante amplio, al incluir a aquellos delitos dolosos que tengan al menos como pena máxima de tres años, lo que extiende el abanico de delitos en gran medida, más aún si adoptásemos esta reglamentación en Argentina, y pone en duda el carácter restrictivo que tiene la uso de esta medida.

Asimismo, esta ley española, más allá de la posibilidad de interceptar las comunicaciones electrónicas o telemáticas en tiempo real, regula la posibilidad de obtener y grabar por cualquier medio técnico comunicaciones orales directa que se mantengan por el investigado, sea en la vía pública, en otro lugar abierto, en el domicilio o en cualquier otro lugar cerrado, o imágenes de la persona investigada cuando se encuentre en un lugar o espacio público, si ello fuere necesario para facilitar su identificación, para localizar los instrumentos o efectos del delito u obtener datos relevantes para el esclarecimiento de los hechos, o utilizarse dispositivos o medios técnicos de seguimiento y localización cuando concurran razones de necesidad y la medida resulte proporcionada.

En Argentina, la intervención de comunicaciones, inicialmente solo las telefónicas, se encuentra prevista en leyes sustantivas como la ley de telecomunicaciones (ley 19798) o de inteligencia (ley 25520), como en leyes adjetivas (código procesal penal de la Nación y los códigos procesales provinciales).

La ley 27.063, que establece un nuevo código procesal penal de la Nación y se encuentra vigente en Argentina, aunque no sea aplicable aún en todas las provincias, conforme el régimen de implementación progresiva previsto por Ley 27.150 y decreto N° 257/2015, establece expresamente la posibilidad de ordenar la interceptación y secuestro de correspondencia

Sobre la motivación de la resolución judicial, la Corte Suprema ha dicho que para autorizar una orden de registro de las comunicaciones telefónicas a los fines de develar su secreto y conocer su contenido, es necesario que sea dictada por juez, solo cuando medien “elementos objetivos idóneos para fundar una mínima sospecha razonable” y estableció una serie de pautas que deben valorarse a fin de proteger el secreto de las comunicaciones.

Sin embargo, la jurisprudencia existente, ha sido desarrollada en relación a las comunicaciones telefónicas, y es en relación a ellas que ha habido mayor evolución en cuanto a la posibilidad de interceptación en tiempo real de las mismas, delimitando el marco de injerencia que esta medida significa.

La comunicación digital contiene otro tipo de información, anexada a la propia comunicación, que excede a aquella que de una comunicación telefónica puede obtenerse, tal como aquella relativa al tráfico (usuario que lo envía, destinatario, fecha, dirección IP desde la que se generó, ubicación de dicha IP, etc.) o la

que se encuentra relacionada al documento adjunto a dicha comunicación (por ejemplo sistema operativo que se utilizó para crearlo, fecha y usuario de creación y/o modificación).

La interceptación de una comunicación electrónica, por tanto, merece un estándar de sospecha y necesidad que justifique esa mayor intromisión, no solo por ser una injerencia más profunda, sino también, por cuanto, en una comunicación telefónica, una persona, aún con una expectativa razonable de privacidad, es consciente de la información que emite, mientras que en una comunicación electrónica existe una gran parte de información que se pone en circulación en forma inconsciente, sin que ello sea parte del contenido esencial de la información, siendo involuntario por la estructura del sistema informático a través del cual se realiza la comunicación.

La legislación argentina, no prohíbe la intervención de comunicación electrónica o informática, aunque haya sido diseñada para la telefónica. Incluso se advierte de la lectura de las leyes la referencia a cualquier tipo de comunicación o la referencia expresa a la comunicación electrónica.

Pero no existe una discriminación legislativa especifica según cada tipo de comunicación, por lo que las posibilidades de su interceptación parecieran regirse no solo por los mismos principios, sino también por los mismos estándares, a pesar que, como ya se ha expresado, la comunicación electrónica conlleva necesariamente mayor información y por tanto su interceptación implica mayor grado de injerencia en la intimidad y privacidad del sujeto.

Tampoco distingue la ley argentina, si la interceptación está destinada a los datos de contenido o a los datos de tráfico, aun cuando el Convenio de Budapest lo hace, siendo más restrictiva la posibilidad de intervenir datos informáticos relativos al contenido que aquellos de tráfico, en razón de la mayor injerencia a la privacidad del sujeto de la medida.

Tampoco refieren las normas argentinas la posibilidad de obligar al prestador de servicios de realizar la medida o prestar colaboración en orden a sus capacidades técnicas, ni especifican si pueden ser utilizadas en la investigación de cualquier delito o solo respecto de algunos, todas situaciones que encuentran regulación en el Convenio de Budapest.

En definitiva, y a pesar de prever la intervención de cualquier tipo de comunicación, inclusive la electrónica o telemática, se aprecia que la legislación

argentina ha mantenido las mismas reglas que tenía para la comunicación telefónica, a pesar de las diferencias reseñadas y de la mayor información y accesibilidad que presenta una comunicación electrónica.

Seguido, las legislaciones, al hablar de correspondencia hacen referencia a la interceptación y no a la intervención, hecho que plantea un conflicto cuando hablamos de correspondencia electrónica, ya que hoy es posible el conocimiento de la misma, no solo por la aprehensión del soporte físico que sirve de vehículo, sino también en forma remota a través del monitoreo de mensajes de correos electrónicos a través de la creación de "cuentas espejo".

El nuevo código procesal penal de la nación, sancionado por ley 27.063, regula de un modo diferente la cuestión, al establecer que cuando lo que se busca conocer y obtener es la comunicación en tiempo real, deberá procederse de modo análogo al allanamiento (ley 27.063- art. 132), siendo una medida excepcional, en que el juez controlará la razonabilidad y legalidad del requerimiento.

Y que en caso que la correspondencia ya haya sido recibida por el destinatario, prevé el registro de un sistema informático o medio de almacenamiento electrónico, rigiendo las condiciones para la inspección de cosas y lugares, las limitaciones del secuestro de documentos y las reglas de apertura y examen de correspondencia una vez secuestrados los componentes del sistema u obtenida la copia de los datos.

Si bien se observa un avance respecto a una adecuación tecnológica que se le exige a la normativa procesal, este es insuficiente, ya que se pierde la oportunidad de realizar una adecuación más profunda, distinguiendo los parámetros necesarios para autorizar una intervención de comunicaciones electrónicas, según si lo que interesa es el contenido mismo, o si es necesario los datos de tráfico.

Sin perjuicio de ello, es importante de esta ley que no distingue el medio de comunicación optado, sea escrito u oral, como tampoco el soporte físico utilizado, que puede ser una computadora, *notebook*, *Tablet*, o *Smartphone*, u otro, si los correos son correspondencia epistolar, no existe ningún motivo para pensar que lo son menos cuando son enviados o recibidos desde teléfonos móviles

- Por último, en el capítulo V se analizó la figura del agente encubierto, en razón de la importancia que tiene en la investigación de un delito informático o cometido a través de un sistema informático.

Como pudo verse el agente encubierto digital presenta algunas particularidades que lo distinguen de aquel infiltrado en otras investigaciones. El anonimato, la falta de contacto directo entre víctima y victimario, la prosperabilidad del engaño, son algunos de los factores especiales de esta técnica investigativa.

El agente encubierto digital no requiere la construcción de una completa identidad falsa, sino que basta con una identidad virtual, y la creación de cuentas de correo electrónico o de líneas telefónicas a fin de habilitar tales cuentas.

Téngase en cuenta que el usuario virtual solo conoce al otro, con quien mantiene una comunicación en red, a través del perfil que cada uno ha creado en la misma, no existiendo contacto físico. Así cada uno asume dicho contexto, resignando ciertos parámetros de control respecto a la persona con la que está manteniendo una comunicación, al no importarle quizás la verdadera cara o el nombre del otro.

En razón de ello, puede concluirse que el engaño que incurre el Estado al autorizar y utilizar la infiltración como técnica investigativa, tiene mayor impacto en el ámbito informático que quizás el de otras organizaciones delictivas al haber un aprovechamiento de dicha vulnerabilidad y que por tanto sea más permeable la infiltración y más probable la obtención de información.

Esto tiene incidencia respecto a la autorización judicial necesaria para la actuación de un agente encubierto como técnica investigativa, toda vez que requerirá un mayor ahínco en la justificación de la medida, teniendo en cuenta los parámetros de excepcionalidad y proporcionalidad de la misma, al haber una mayor facilidad para el engaño en el campo virtual que en el físico.

Es decir, si bien es el propio usuario informático quien prescinde en mayor medida ciertos controles a fin de determinar con quien se comunica, cierto es que el Estado no puede aprovecharse de dicha situación, avalando una medida sin resguardo de los parámetros de excepcionalidad y proporcionalidad.

El solo hecho que sea más accesible el engaño, con la sola utilización de un perfil informático falso, no es suficiente para que esta técnica investigativa pueda generalizarse. Por el contrario, el Juez debe mantener el carácter restrictivo de la misma.

Esta situación no se encuentra regulada ni distinguida en la normativa argentina, la que solo prevé la infiltración de un agente de modo tradicional,

sin tomar en cuenta las especiales características del agente encubierto digital o informático.

En la actualidad, resulta necesaria una adecuación legislativa a las especiales características de esta técnica investigativa, tomando en cuenta la necesidad de la misma, atento el desarrollo tecnológico que obstaculiza cada vez más el avance de una investigación, pero sin perder su carácter restrictivo y excepcional.

En este sentido, es cierto que la utilización de esta técnica investigativa es mucho menos riesgosa en el mundo informático que en el físico, al no exponer más que un perfil virtual del agente infiltrado. Y también es cierto que cada vez resulta más necesaria la aplicación de esta herramienta para determinar la autoría u obtener los elementos de prueba en delitos informáticos.

Sin embargo, ello no debe trasponer el carácter excepcional de la medida, por más útil que fuere en cada vez más investigaciones. La generalización de la medida o su utilización para ver si se está cometiendo un delito ("ir de pesca"), no pueden permitirse, en razón de la mayor vulneración de garantías individuales producidas por el engaño que lleva a cabo el Estado a través de la incorporación de un agente infiltrado.

Interesante en esta línea es la regulación española, que prevé expresamente la posibilidad de una situación frecuente en el mundo informático, y que avala en definitiva el carácter restrictivo de esta herramienta, cual es el intercambio de material para ganar la confianza del grupo cerrado. Así, requiere una autorización especial del Juez, distinta de aquella inicial que dio origen a la actuación encubierta.

Si bien la ley 27.319 o el Código procesal penal mendocino, prevén el control y dirección de la actuación del agente durante la misma por parte del Juez y del Fiscal respectivamente, estas facultades son posteriores al accionar, no siendo suficiente en razón de la mayor vulneración que ciertos actos implican. Es necesario, en estos casos, que la autoridad judicial pueda ejercer un control anterior del actuar del agente infiltrado, previéndose la necesidad de una autorización previa.

Finalmente, las especiales características de la criminalidad informática y las posibilidades de éxito de la utilización de un agente encubierto digital, permiten pensar una mayor amplitud de delitos que pueden investigarse por esta vía y que no han sido tenidos en cuenta por la normativa argentina.

Así, la normativa nacional determina una lista estricta de crímenes que pueden ser investigados mediante esta técnica, quedando fuera de ellas,

delitos de cada vez mayor incidencia en la sociedad argentina, como es el *grooming* (art. 131 CP) o donde menores resultan víctima de algún tipo de abuso (psicológico, físico o sexual).

Al respecto, cabe hacer una distinción respecto al carácter excepcional del agente encubierto, toda vez que esta característica se presenta justificada, en el caso del infiltrado digital o informático, solo en el sentido de insustituibilidad respecto a otras técnicas de investigación.

Pero no parece tanto en relación a los delitos que pueden ser investigados, en razón de las particularidades y ventajas que tiene el agente encubierto digital en las investigaciones de crímenes cometidos contra o a través de un sistema informático.

Sin lugar a dudas, la incorporación de un agente encubierto en el ámbito de una investigación por narcotráfico tradicional, requiere mayores riesgos para el agente y mayores posibilidades de no tener éxito en la misma, de lo que se desprende mayores costos para su utilización. Todos estos factores tienen como consecuencia que solo se justifique la utilización de esta herramienta, en la investigación de ciertos delitos especialmente graves y, por tanto, taxativamente determinados.

Sin embargo, estos elementos disminuyen cuando hablamos de un agente encubierto digital, toda vez que no requiere contacto físico, solo implica la creación de un usuario virtual y no el cambio completo de la identidad del agente, las posibilidades de éxito aumentan, incluso teniendo en cuenta la mayor facilidad para obtener las pruebas en razón del registro electrónico que puede ir siendo guardado.

Todos estos factores nos llevan a sostener, que pueda utilizarse en la investigación de otros delitos, que si bien no tienen la especial gravedad como es el narcotráfico el terrorismo, puedan únicamente ser investigados por esta vía, aportando enormes avances en la misma.

El continuo avance de las nuevas tecnologías trae consigo nuevos desafíos. En el ámbito de la delincuencia, el crecimiento en la utilización de Internet brinda toda una nueva gama de formas y medios, sobre los cuales cometer delitos, aprovechándose de usuarios que diariamente acceden de todo tipo de dispositivos. Ello trae como consecuencia paralela el aumento por un lado de la población pasiva de delitos, así como también la mayor sofisticación y complejidad de la población activa criminal.

Por tanto, es imprescindible que la legislación recepte estos avances, generando nuevas herramientas procesales que permitan investigar eficazmente estos delitos, siendo el agente encubierto informático, cada vez más necesario en la investigación de estos.

Bibliografía

ABOSO, G. E. (2017). *Derecho penal cibernético.* Buenos Aires: BdeF.

ALTMARK, D. R.-M. (2012). *Tratado de Derecho Informático.* Buenos Aires: La Ley.

BALCARCE, F. I. (2006). El secuestro en materia procesal penal. En G. A.-B. AROCENA, *Escritos penales procesales.* Cordoba: Mediterránea.

BLANCO, H. (2015). *La adaptación de los medios de prueba a la realidad tecnológica en el nuevo código procesal penal: un avance a medias*. Obtenido de www.rubinzalculzoni.com.ar: RC D 472/2015

BLANCO, H. (2016). *El nuevo código procesal penal de la Nación y la requisa de Smartphones y otros dispositivos móviles*. Obtenido de www.rubinzalculzoni.com.ar: RC D 143/2016

CAFFERATA NORES, J. (s.f.). *Cuestiones actuales sobre el proceso penal.* Buenos Aires: Ediotres del Puerto.

CAFFERATA NORES, J. I.-T. (2003). *Código Procesal Penal de la Provincia de Córdoba comentado.* Cordoba: Mediterránea.

CARBONE, C. (2008). *Requisitos constitucionales de las intervenciones telefónicas.* Santa Fe: Rubinzal Culzoni.

CARDOSO PEREIRA, F. (2012). *Agente encubierto y proceso penal garantista: Límites y desafíos.* Córdoba: Lerner SRL.

COLEFF, I. (2017). La orden de presentación en el derecho procesal penal argentino. Necesidad de su reforma. En D. D.-K. Mariana, *Cibercrimen.* Buenos Aires: BdeF.

DE LUCA, J. A. (2017). Delitos informáticos, apuntes 2016. En D. -K. DUPUY, *Cibercrimen.* Buenos Aires: BdeF.

DELLE DONNE, C. P. (2013). *Analisis de la jurisprudencia argentina sobre delitos informáticos y prueba digital: periodo 2010-2011*. Obtenido de www.informacionlegal.com.ar: cita online: AP/DOC/1668/2013

DUPUY, D. -K. (2017). *Cibercrimen. Aspectos de derecho penal y procesal penal. Cooperación internacional. Recolección de evidencia digital. Responsabilidad de los proveedores de servicios de internet.* Buenos Aires: BdeF.

FLEMING, A. -L. (2007). *Garantías del imputado.* Santa Fe: Rubinzal-Culzoni.

GARCIA GONZALEZ, J. (2015). *Oportunidad criminal, internet y redes sociales*. Obtenido de Revista InDret: www.indret.com

GARCÍA GUILABERT, N. (2017). *El ciberacoso. Análisis de la victimización de menores en el ciberespacio desde la Teoría de las actividades cotidianas.* Buenos Aires: BdeF.

GARIBALDI, G. E. (2010). *Las modernas tecnologías de control e investigación del delito.* Buenos Aires: Ad Hoc.

GÓMEZ, C. D. (2010). La "Intervención de llamadas telefónicas" en la jurisprudencia de la Corte Suprema de Justicia de la Nación. A propósito del caso: "Q.". *LA LEY* .

GOMEZ, L. S. (2017). Evidencia Digital en la Investigación Penal. En D. -K. DUPUY, *Cibercrimen* (pág. 617/635). Buenos Aires: BdeF.

HAIRABEDIAN, M. (2017). El acceso a información y datos de teléfonos celulares. En D. -K. DUPUY, *Cibercrimen.* Buenos Aires: BdeF.

LERMAN, M. (2004). *La prohibición de analogía en materia procesal penal: Nulla coactio y teoría del fruto del árbol envenenado*. Obtenido de https://informacionlegal.com.ar, AR/DOC/812/2004

LUCERO, P. G.-K. (2010). *Delitos informáticos.* Buenos Aires: DyD.

NEME, C. F. (2017). Una mirada actual en materia de regulación de retención de datos de tráfico y conservación rápida de datos informáticos. En D. -K. DUPUY, *Cibercrimen.* Buenos Aires: BdeF.

PALAZZI, P. A. (2012). *Derecho Penal Informático. Breves reflexiones sobre la evidencia digital en procesos penales*. Obtenido de www.informacionlegal.coom.ar: AP/DOC/3575/2012

PALAZZI, P. A. (2012). *Los delitos informáticos en el Código Penal. Análisis de la ley 26.388.* Buenos Aires: Abeledo Perrot.

PEREZ BARBERÁ, G. (2009). Nuevas tecnologías y libertad probatoria en el proceso penal. *IV Encuentro de profesores de derecho procesal penal.* Salta.

PETRONE, D. (2014). *Prueba informática.* Buenos Aires: Ediciones Didot.

RIQUERT, M. A. (2009). *Delincuencia informática en Argentina y el Mercosur.* Buenos Aires: Ediar.

RIQUERT, M. A. (2014). *Ciberdelitos.* Buenos Aires: Hammurabi.

ROMERO VILLANUEVA, H. J. (2017). *Actualidad jurisprudencia penal y procesal penal 04/2017*. Obtenido de www.informacionlegal.com.ar: AP/DOC/915/2017

ROMERO VILLANUEVA, R. J.-G. (2015). *Código procesal penal de la nación. Comentado. Ley 27063.* Buenos Aires: Abeledo Perrot.

ROMERO, S. (s.f.). *Los registros de comunicaciones telefónicas ("sábanas") en la investigación penal: otro capítulo sobre la permanente tensión entre tecnología y privacidad*. Obtenido de http://www.rubinzalonline.com.ar/index.php/doctrina/articulos/ver/739563/

SAIN, G. (2016). *Actualización del código procesal penal de la Nación en materia informática jurídica y criminalística digital*. Obtenido de www.rubinzalculzoni.com.ar: RC D 306/2016

SAIN, G. R. (2012). *Delito y nuevas tecnologías: fraude, narcotráfico y lavado de dinero por internet.* Buenos Aires: Editores del Puerto.

SALLIS, E. (2017). Desafíos de la investigación de los delitos informáticos en la Deep & Dark Web. En D. -K. DUPUY, *Cibercrimen.* Buenos Aires: BdeF.

SALT, M. G. (2013). *Nuevos desafíos de la evidencia digital. El acceso transfronterizo de datos en los países de América Latina*. Obtenido de https://informacionlegal.com.ar, AP/DOC/898/2013

TEMPERINI, M. -M. (2017). Nuevas herramientas de investigación penal: el agente encubierto digital. En D. -K. DUPUY, *Cibercrimen.* Buenos Aires: BdeF.

VANINETTI, H. A. (29 de diciembre de 2015). *correo electrónico como herramienta de trabajo y facultades de control*. Obtenido de rubinzalculzonionline: AP/DOC/1150/2015

ZOCO ZABALA, C. (2010). *Interceptación de las comunicaciones electrónicas. Concordancias y discordancias de SITEL con el art. 18.3 CE*. Obtenido de Revista InDret: www.indret.com