DELITOS INFORMÁTICOS Y CIBERCRIMEN: TÉCNICAS Y TENDENCIAS DE INVESTIGACIÓN PENAL Y SU AFECTACIÓN A LOS DERECHOS CONSTITUCIONALES

Marcelo Temperini [1]

1. Introducción

La delincuencia evoluciona. Los delincuentes cada vez se organizan mejor, cada vez se sienten más seguros utilizando las nuevas –o ya no tan nuevas– tecnologías de la información y las comunicaciones. Ya no se llaman por teléfono para organizarse sobre el nuevo comercio que piensan atracar, sino que ahora se escriben por Whatsapp o, peor aún, se llaman por Whatsapp. Algunas bandas ya utilizan Telegram o Signal para estar comunicadas. Los delincuentes relacionados al comercio y distribución de pornografía infantil envían contenidos a través de proxys anónimos y usan contenedores virtuales cifrados para almacenar su colección privada.

La delincuencia se complejiza, se expande y continúa evolucionando. Las preguntas, pensando en el otro lado del mostrador y que motivan la elaboración de este artículo, son: *¿La justicia también evolucionó lo suficiente como para estar preparados para la detección, identificación y captura de los ciberdelincuentes? ¿Los métodos de investigación utilizados por el Estado responden a estas nuevas realidades de la delincuencia?* Y por último y quizá más importante: *¿Cuál es el nivel de afectación de los derechos en la utilización de estos nuevos métodos de investigación?*

[1] Abogado (UNL) especialista en Derecho Informático y Seguridad de la Información. Doctorando en Derecho (FCJS / UNL) dedicado a la investigación de Delitos Informáticos y Cibercrimen. Socio Fundador de AsegurarTe www.asegurarte.com.ar. Co-fundador del Proyecto ODILA: Observatorio de Delitos Informáticos de Latinoamérica. Contacto: mtemperini@asegurarte.com.ar

En este contexto, el presente trabajo pretende, a modo de conclusión, elaborar un listado de algunas de las técnicas más conocidas o utilizadas por la Justicia y las fuerzas de seguridad en relación a la investigación de delitos informáticos (entendidos en su concepto amplio). No existe una pretensión intelectual de hacer un abordaje profundo sobre cada una de estas medidas y técnicas, toda vez que su desarrollo implicaría una extensión que excede la búsqueda de este trabajo. La finalidad más bien consiste en la construcción de un decálogo o listado de las distintas técnicas más utilizadas, a modo introductorio, para aquellos lectores que recién se inician en el mundo de la investigación del ciberdelito.

Metodológicamente, iniciaremos con un abordaje jurídico sobre la tensión existente entre la eficacia en los métodos de investigación y la posible (o muy posible) afectación de derechos constitucionales que implica su utilización. En el marco de esta construcción jurídica se buscará realizar un escalonamiento o categorización de los distintos tipos de información que pueden ser obtenidos a través de la ejecución de diferentes medidas y técnicas de investigación. Al finalizar dicho análisis, listaremos las medidas de investigación más utilizadas, posicionando en un extremo aquellas menos invasivas –o más respetuosas– de las garantías constitucionales, avanzando hasta las medidas y técnicas más agresivas y cuestionables –pero quizá más eficaces– desde un punto de vista jurídico.

2. TECNOLOGÍA E INVESTIGACIÓN PENAL

De acuerdo a Federico Fumis, las nuevas tecnologías han representado un profundo cambio, en tanto posibilitaron la incorporación de nuevos métodos investigativos y medios probatorios al proceso, y –al mismo tiempo– permitieron potenciar la capacidad de viejos métodos y medios que, apoyados en los avances técnicos, resultan cada vez más eficaces. Sin embargo, no podemos avanzar en el desarrollo del tema sin dejar sentado que estos nuevos medios tecnológicos –junto con sus ventajas y posibilidades de éxito– traen aparejada la posibilidad cierta de lesionar derechos y garantías constitucionales con gran facilidad y de un modo prácticamente invisible.

Como afirma Fumis: "El descubrimiento de la verdad en el proceso penal se encuentra sometido a importantes limitaciones, como por ejemplo la prohibición de utilizar formas de investigación y pruebas que resulten violatorias de garantías consagradas en normas constitucionales y legales"[2].

[2] FUMIS, Federico, "La utilización de modernas tecnologías en la persecución penal: su utilidad en la búsqueda de mayores índices", en *REDI*: Revista Electrónica de Derecho Informático, nº 44.

El aspecto de fondo visibiliza una tensión (tan histórica como el derecho mismo) entre la eficacia de la investigación y el avance sobre los derechos y garantías constitucionales de la persona que está siendo investigada. Tensión que, a nuestro criterio, se encuentra profundamente agravada por las nuevas tecnologías, toda vez que, a diferencia de las medidas de investigación penal tradicionales, las nuevas tecnologías permiten avanzar sobre una esfera íntima de la persona de una forma mucho más "transparente" y rápida, haciendo que esta falta de tangibilidad de las barreras que delimitan estos bienes jurídicos tutelados constitucionalmente, puedan superarse con extrema facilidad en cuestión de segundos y, en muchos casos, sin dejar mayores rastros.

En consecuencia, cada vez es más cotidiano encontrar ejemplos de medidas de investigación penal que, por no contar con los requisitos jurídicos mínimos necesarios, podrían tornarse procesalmente inaprovechables por no respetar adecuadamente los derechos y las garantías procesales de las personas afectadas.

3. La afectación de garantías constitucionales

En el catálogo de derechos y garantías que pueden ser afectados a través de las distintas medidas de investigación, analizaremos la situación constitucional en Argentina y España (a modo comparativo).

Entre estos países podemos encontrar distintos derechos, como el secreto de las comunicaciones, derecho a la intimidad, derecho a la protección de los datos personales, e incluso el flamante derecho a la protección del propio entorno virtual, del cual nos ocuparemos en este capítulo.

En la Constitución española, su art. 18 contiene la mayoría de los derechos que estamos analizando aquí:

1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.

2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.

3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.

4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

En cuanto al alcance de lo que debe entenderse por "secreto de las comunicaciones", a través de una sentencia [3] del Tribunal

[3] Sentencia del Tribunal Constitucional 123/2002, de 20 de mayo.

Constitucional se ha reconocido que el mismo "garantiza a los interlocutores o comunicantes la confidencialidad de la comunicación telefónica que comprende el secreto de la existencia de la comunicación misma y el contenido de lo comunicado, así como la confidencialidad de las circunstancias o datos externos de la conexión telefónica: su momento, duración y destino; y ello con independencia del carácter público o privado de la red de transmisión de la comunicación y del medio de transmisión –eléctrico, electromagnético u óptico, etc.– de la misma".

Bajo esta interpretación, coincidente con una importante Sentencia del año 1984 [4] y la sentencia de otro reconocido fallo, como el caso "Malone" [5], se sostuvo el criterio de interpretación amplia entendiendo que "el concepto de secreto de la comunicación cubre no sólo el contenido de la comunicación, sino también la identidad subjetiva de los interlocutores", y de esta forma el Tribunal otorgó el amparo al recurrente porque la entrega por la compañía telefónica a la Policía de los listados de llamadas del investigado no contaba con la preceptiva autorización judicial.

La protección de los datos personales a la cual hace referencia el inc. 4 del art. 18 citado posee un amplio desarrollo normativo y doctrinario, expandido aún más a través de la flamante normativa del Reglamento General de Protección de Datos [6], que entró en vigencia el 25 de mayo de 2018, incorporando y profundizando aún más los derechos a la privacidad de los usuarios de servicios de comunicación.

Quizá la protección jurídica más novedosa es este "nuevo" derecho constitucional denominado "derecho a la protección del entorno virtual". Así lo ha dicho el Tribunal Supremo español en la sentencia 204/2016 [7], donde se afirmó: "Es por ello por lo que el legislador otorga un tratamiento unitario a los datos contenidos en los ordenadores y teléfonos móviles, reveladores del perfil personal del investigado, configurando un derecho constitucional de nueva generación que es el derecho a la protección del propio entorno virtual".

[4] Sentencia del Tribunal Constitucional 114/1984.

[5] Sentencia del Tribunal Europeo de Derechos Humanos de 2 de agosto de 1984 (caso Malone).

[6] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la directiva 95/46/CE (Reglamento general de protección de datos) (Texto pertinente a efectos del EEE).

[7] Sentencia nº 204/2016 de TS, Sala 2ª, de lo Penal, 10 de marzo de 2016.

Precisando aún más esta nueva protección de índole genérica a este tipo de información, sentencia: "Y es que, más allá del tratamiento constitucional fragmentado de todos y cada uno de los derechos que convergen en el momento del sacrificio, existe un derecho al propio entorno virtual. En él se integraría, sin perder su genuina sustantividad como manifestación de derechos constitucionales de *nomen iuris* propio, toda la información en formato electrónico que, a través del uso de las nuevas tecnologías, ya sea de forma consciente o inconsciente, con voluntariedad o sin ella, va generando el usuario, hasta el punto de dejar un rastro susceptible de seguimiento por los poderes públicos. Surge entonces la necesidad de dispensar una protección jurisdiccional frente a la necesidad del Estado de invadir, en las tareas de investigación y castigo de los delitos, ese entorno digital".

Por el lado de Argentina, desde un punto de vista constitucional, no existe un catálogo tan claro como hemos visto en España, aunque podemos encontrar igualmente estos derechos en los arts. 18, 19 y 43 de la Constitución Nacional de Argentina.

En el fallo "Halabi"[8], la Corte Suprema de Justicia de la Nación (CSJN) declaró la inconstitucionalidad de la ley 25.873 y su decreto reglamentario, en el cual se pretendía regular la retención de datos. En el fallo, y con relación a la interpretación sobre la protección constitucional de las comunicaciones, la CSJN expresó: "En relación con los aspectos reseñados resulta oportuno señalar que las comunicaciones a las que se refiere la ley 25.873 y todo lo que los individuos transmiten por las vías pertinentes integran la esfera de intimidad personal y se encuentran alcanzadas por las previsiones de los arts. 18 y 19 de la Constitución Nacional. El derecho a la intimidad y la garantía consecuente contra su lesión actúa contra toda 'injerencia' o 'intromisión' 'arbitraria' o 'abusiva' en la 'vida privada' de los afectados (conf. art. 12 de la Declaración Universal de Derechos Humanos y art. 11, inc. 2°, de la Convención Americana sobre Derechos Humanos, tratados, ambos, con jerarquía constitucional en los términos del art. 75, inc. 22, de la Constitución Nacional y art. 1071 bis del Código Civil)".

En relación al caso concreto que se discutía en "Halabi", también de interés para el marco de este trabajo en relación a la posibilidad de guarda de los datos de las comunicaciones, la Corte afirmó: "Es evidente que lo que las normas cuestionadas han establecido no es otra cosa que una restricción que afecta a una de las facetas del

[8] "Halabi, Ernesto c/ P.E.N. - ley 25.873 - dto. 1563/04 s/ amparo ley 16.986".

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", reconociendo de esta forma una afectación al derecho de la intimidad sobre los usuarios.

Adicionalmente a este reconocimiento constitucional, existe un refuerzo sobre la protección del secreto de las comunicaciones dentro de la Ley Nacional de Inteligencia de Argentina 25.520, donde reconoce la inviolabilidad de las comunicaciones:

> Art. 5° - Las comunicaciones telefónicas, postales, de telégrafo o facsímil o 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, son inviolables en todo el ámbito de la República Argentina, excepto cuando mediare orden o dispensa judicial en sentido contrario.

Similar regulación tiene la Ley Nacional de Telecomunicaciones 19.728, en cuyos arts. 18 y 19, establece:

> Art. 18. - La correspondencia de telecomunicaciones es inviolable. Su interceptación solo procederá a requerimiento de juez competente.
>
> Art. 19. - La inviolabilidad de la correspondencia de telecomunicaciones 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.

4. La regla de los tres escalones

Como ya hemos adelantado en la introducción, como resultado final de este trabajo buscaremos construir un catálogo de medidas de investigación penal, organizadas de acuerdo al nivel de injerencia o afectación a los derechos constitucionales. En este contexto, consideramos necesario hacer un desarrollo previo sobre una categorización sobre los datos, aceptada a nivel internacional, y que denominaremos –con cierta finalidad pedagógica– como "la regla de los 3 escalones".

A través de la misma, se pretende aclarar las distintas categorías de información a la cual es posible acceder en el contexto de una investigación penal y, sobre todo, qué nivel de afectación a los derechos implica cada una de ellas.

Sin embargo, como en toda buena construcción, nuestra escalera no podrá estar flotando en el aire, sino que deberá estar apoyada sobre una base firme, sobre algún piso que –en nuestra elaboración teórica– serán aquellos datos para cuyo acceso no se considere que existe una afectación indebida a los derechos.

Esta primera base estará apuntalada sobre un criterio –en principio, ampliamente aceptado por la jurisprudencia– que interpreta como válida la incorporación como elemento de prueba, en el marco de una investigación penal, de aquellos datos que sean considerados públicos, es decir, cuyo acceso sea posible de forma irrestricta y sin vulnerar ninguna barrera técnica o jurídica.

Un claro ejemplo de esta primera categoría de información será aquella que es posible obtener a través de la utilización de las difundidas técnicas de OSINT (*Open Source Intelligence*), las cuales precisamente apuntan a la búsqueda, identificación y procesamiento de información sobre fuentes abiertas, es decir, sobre aquellas que pueden obtenerse de forma pública y, por lo tanto –en principio–, no existe afectación alguna sobre la privacidad del titular de esos datos.

Dentro de la jurisprudencia, un caso en Argentina[9] logró condenar a una persona por homicidio agravado gracias a que, a través de su perfil de Facebook, se logró identificar al criminal. Se trató de un caso de homicidio sobre un hombre que fue asesinado mientras dormía en la vía pública por dos personas que lo rociaron con combustible y luego lo prendieron fuego. Los vecinos del lugar señalaron que uno de los autores de apodaba "Chucky". Gracias a la mención de ese nombre, los investigadores del caso lograron dar con el principal sospechoso, Alexis Bejarano, quien tenía un perfil público en Facebook. Se hizo una rueda de reconocimiento y una de las testigos no dudó de que se trató de uno de los autores.

Ante dicha situación, la defensa del condenado interpuso una queja que sostenía que había que equiparar a la prueba informática por la que se obtuvo el perfil de Facebook del encartado, con la correspondencia epistolar. La defensa aseguró que debía existir orden judicial para obtener la información del correo electrónico y las redes sociales.

[9] "Bejarano, Alexis s/recurso de casación", Sala IV de la Cámara Federal de Casación Penal, Argentina.

Sin embargo, el Tribunal sostuvo que la red social Facebook es un sitio web que se encuentra disponible para cualquier usuario de la red y se utiliza para que sus usuarios puedan intercambiar comunicación fluida y compartir contenido de forma sencilla a través de Internet. A partir de sus características públicas la página de Facebook propiedad del imputado "no goza de la protección de la privacidad como la clásica vía postal". Según la Casación Federal, si bien para el funcionamiento y utilización de la red social "se requiere indispensablemente de un prestador del servicio, el nombre de usuario y clave de acceso destinados a impedir que terceros extraños se entrometan en los datos y contenidos que se emiten y reciben", en el caso el perfil del condenado "era público y casi toda la información que compartía podía ser vista por cualquier persona que accediera a través de internet a la página". "La página de Facebook no puede ser considerada la 'correspondencia epistolar' que protege la Constitución Nacional, razón por la cual el modo en que fue obtenida e incluso su incorporación como prueba al juicio, mal puede violar la garantía contenida en el art. 18 de la CN", señalaron los camaristas.

Hacia el final de la sentencia se afirma: "A partir de lo expuesto, entiendo que el procedimiento por el cual se obtuvo e incorporó como prueba la página de Facebook mediante la cual se pudo corroborar que el sujeto apodado 'Chucky' se correspondía con el nombre y fotografía que figuraban en ese perfil de la red social fue realizado conforme a las disposiciones legales vigentes sin afectar la garantía que prohíbe intromisiones arbitrarias en la intimidad y privacidad del imputado y por ello propongo rechazar el presente agravio".

Es decir, queda claro, en base a este último párrafo, el criterio adoptado, donde se entiende que las garantías constitucionales que prohíben la intromisión arbitraria en la intimidad y privacidad del imputado no se encuentran afectadas cuando se trata de información disponible de forma pública e irrestricta.

A modo de comentario final, aclaramos que distinto hubiese sido el análisis jurídico si se hubiese tratado de una imagen publicada con alguna limitación sobre la privacidad (amigos o amigos de mis amigos).

4.1. El primer escalón: los datos de abonado

Superada la explicación sobre la base de los datos públicos, es momento de avanzar hacia nuestro primer escalón: los datos de identificación de usuario, o también denominados "datos de abonado", o en el caso de redes sociales, más conocidos como BSI (*Basic Subscriber Information*).

En este primer escalón encontraremos distintos tipos de información identificatoria relacionada al titular de la cuenta o del servicio consultado. A nivel internacional contamos con una defini-

ción en el Convenio de Cibercrimen de Budapest[10], quizás uno de los instrumentos jurídico más importantes en la materia a nivel penal y procesal penal. En el art. 18 donde se regula la "orden de presentación", en su inc. 3, se define:

> "A los efectos del presente artículo, por «datos relativos a los abonados» se entenderá toda información, en forma de datos informáticos o de cualquier otra forma, que posea un proveedor de servicios y esté relacionada con los abonados a dichos servicios, excluidos los datos sobre el tráfico o sobre el contenido, y que permita determinar:
> "a) El tipo de servicio de comunicaciones utilizado, las disposiciones técnicas adoptadas al respecto y el periodo de servicio;
> "b) la identidad, la dirección postal o geográfica y el número de teléfono del abonado, así como cualquier otro número de acceso o información sobre facturación y pago que se encuentre disponible sobre la base de un contrato o de un acuerdo de prestación de servicios;
> "c) cualquier otra información relativa al lugar en que se encuentren los equipos de comunicaciones, disponible sobre la base de un contrato o de un acuerdo de servicios".

En la base de la definición, existe una conceptualización casi por exclusión, al decir que es toda información (generalmente datos personales) que posea un proveedor de servicios, relacionada con el abonado del servicio, que no sean ni datos de tráfico ni datos de contenido. Por otro lado, en una guía publicada entre la documentación oficial de Naciones Unidas[11], se detallan algunos de los datos de suscriptor que podrán estar disponibles para la consulta judicial:

· Nombre de la cuenta, nombre de usuario o de acceso.
· Nombre y apellido registrados.
· Domicilios registrados.
· Correo electrónico registrado.
· Números de teléfonos asociados a la cuenta.
· Dirección IP utilizada al momento de la creación de la cuenta.
· Fecha y hora de creación de la cuenta.
· Información de sesiones iniciadas (*user agent*, IP de acceso, fecha y duración).
· Otros datos identificatorios del suscriptor (formas de pago, tipos y números de tarjetas de crédito utilizadas, etc.).

[10] Convenio de Ciberdelincuencia del Consejo de Europa de Budapest, de 23 de noviembre de 2001.

[11] *Guide to Obtaining Communication Service Provider Evidence from the United States, United Nations*, www.un.org.

Vale destacar que los datos identificatorios disponibles dependen del tipo de servicio que estemos analizando, toda vez que dentro de la categoría genérica de los CSP [12] podemos incluir tanto los ISP [13] como toda otra plataforma de prestación de servicio de comunicaciones, como redes sociales, sitios de comercio electrónico, hosting, etc.

A modo de ejemplo, en el caso de tratarse de un ISP, estaremos hablando de los datos personales del titular de la línea o servicio, tales como nombre, apellido, domicilio, tipo de servicio contratado, número de usuario, formas de pago utilizadas, tarjetas de crédito utilizadas, entre otros datos. En el caso de otros servicios, como redes sociales, podrá considerarse también parte de estos datos básicos del suscriptor algunos datos tales como el correo electrónico, dirección IP desde la cual se ha generado la cuenta, incluso las direcciones IP de los últimos accesos a la misma, pueden formar parte de este paquete de datos (BSI).

Este primer escalón, como categoría inicial de datos que avanzan sobre un ámbito de privacidad, presenta como característica que nos encontramos ante datos identificatorios que gozan de la protección de los datos de carácter personal, por lo que les serán aplicables todas aquellas normativas relacionadas con la protección de datos personales, en la inteligencia de que se trata de información que permitiría identificar o hacer identificable a una persona [14].

Una de las primeras discusiones clásicas que podría darse dentro de esta categoría tenía relación con la naturaleza de la dirección IP: si esta podía o no ser considerada un dato de carácter personal y, en consecuencia, debía aplicarse todo el andamiaje protectorio correspondiente. En este sentido, el Informe 327/2003 [15] de la Agencia de Protección de Datos Española (AGPD) ha señalado que "aunque no siempre sea posible para todos los agentes de internet identificar a un usuario a partir de datos tratados en la red, desde esta Agencia de Protección de Datos se parte de la idea de que la posibilidad de identificar a un usuario de Internet existe en muchos casos y, por lo tanto, las direcciones IP, tanto fijas como dinámicas, con independencia del tipo de acceso, se consideran datos de carácter personal resultando de aplicación la normativa sobre protección de datos".

[12] CSP: *Communication Service Provider* (Proveedor de Servicios de Comunicación).

[13] ISP: *Internet Service Provider* (Proveedor de Servicio de Internet).

[14] Art. 2 de la ley 25.326 de Protección de Datos Personales en Argentina.

[15] AGPD: Agencia de Protección de Datos Española, Carácter de dato personal de la dirección IP. Informe 327/2003, www.agpd.es.

En la parte final, el mismo informe nos deja una sencilla reflexión sobre la interpretación de los datos personales, que es plenamente aplicable a los demás datos identificatorios desarrollados en esta categoría. Sostiene la AGPD que "En cuanto a la consideración de los *log in* de acceso a Internet o a páginas personales como datos de carácter personal, resultarán de aplicación las consideraciones que se realizan en párrafos anteriores. Si identifica de forma directa al usuario, no hay duda de que estaremos ante un dato de carácter personal; por el contrario si este es anónimo, en principio no sería un dato de carácter personal, pero si, por ejemplo, el proveedor de servicios de Internet a través de ese *log in* puede identificar al usuario con el que tiene un contrato de acceso a Internet, sí será considerado como un dato de carácter personal".

Superado este primer desafío, y quedando claro que estamos en presencia de un conjunto de datos personales que hacen a la identificación de una persona, un segundo interrogante sale a la luz en relación con los requisitos legales que deberán cumplirse para poder solicitar este tipo de datos: *¿Es necesaria una autorización judicial para acceder a esta información? ¿O será suficiente un pedido realizado por el fiscal en el marco de las potestades establecidas para dirigir una investigación penal?*

Sobre este interrogante se ha planteado un interesante caso en Argentina [16]. En el marco de la investigación de un caso de distribución de pornografía infantil, el allanamiento sobre el domicilio del imputado había sido posible gracias a los datos de identificación suministrados por dos CSP (Telecom y Microsoft), pedido de información que había sido solicitado solamente por el fiscal que llevó adelante la causa, es decir, sin autorización judicial.

En este caso, los jueces de Cámara, para declarar la nulidad del requerimiento de juicio, argumentaron "que las direcciones IP (*Internet Protocols*) son datos de carácter personal protegidos por la ley 25.326 y que, por esa razón, la solicitud de aquellos informes debía equipararse a una "interceptación telefónica" y debió solicitarse la pertinente orden judicial, de conformidad con lo establecido en el art. art. 93, *in fine*, del CPPCABA". En ese sentido, afirmaron que "una amplia protección al derecho a la intimidad obliga a entender que los datos personales de quien afirmó ser usuario de un correo electrónico asociado a un protocolo de internet (al crear la cuenta de correo electrónico), registrados por las firmas de telecomunicaciones, se encuentran alcanzados por la regla que ampara la pri-

[16] "Ministerio Público –Fiscalía de Cámara Norte de la CABA– s/queja por recurso de inconstitucionalidad denegado en 'A., C. sinfr. art. 128.2, párr. 2°, CP'".

vacidad y sólo con orden judicial pueden requerirse informes sobre estos datos, en principio, reservados".

Siguiendo con el voto del juez José Casás, afirma: "Sin embargo, lejos de formular argumentación alguna que permita sostener dicha afirmación, los magistrados omitieron explicar por qué razón correspondería equiparar, a la luz de la expectativa de intimidad del individuo, los datos de contenido y los datos de tráfico de una comunicación, con la simple identificación de un usuario. Dicha circunstancia resultaba de vital trascendencia a los fines de analizar la problemática constitucional planteada en el caso concreto. En tercer lugar, tampoco la invocación de la ley de protección de datos personales (ley 25.326) resulta dirimente para la solución del caso, porque no está en discusión que la información requerida a las empresas mencionadas en las resultas perseguía la obtención de 'datos personales'. Lo que no advierten los camaristas es que la propia ley prevé que dicha información puede ser recabada, sin que se requiera el consentimiento del titular, en el ejercicio de funciones propias de los poderes del Estado (art. 5.2.b) y también cuando esos datos se limitan al nombre, documento y domicilio de la persona en cuestión (art. 5.2.c). No otra cosa se pretendió respecto del titular de la IP aportada a la investigación cuando el fiscal, en el ejercicio de sus funciones de instructor, formuló el cuestionado pedido de informes".

En este primer voto, se analiza con extrema precisión la confusión que ha dado lugar al planteo, y es la confusión entre los datos identificatorios, datos de tráfico y datos de contenido, toda vez que erróneamente (a nuestro criterio) la Cámara interpretó que los datos identificatorios son "datos de contenido", exigiendo en consecuencia el requisito de autorización judicial para su obtención.

En un segundo voto, el Dr. Luis Lozano analiza con mayor precisión el aspecto procesal que aquí nos interesa, sobre los alcances en las medidas de investigación que puede llevar adelante un fiscal: "asiste razón al MPF en cuanto manifiesta que ese pronunciamiento ha extendido el alcance de la norma local sobre cuya base aquel se sostiene a un supuesto no contemplado e importa una declaración implícita de inconstitucionalidad de las facultades de investigación que la ley le confiere. Este artículo (art. 93 del CPPCABA[17]) inviste

[17] Ley 2303/07, Código Procesal Penal de la Ciudad Autónoma de Buenos Aires, art. 93: "A fin de desarrollar la investigación preparatoria el/la Fiscal podrá citar a testigos, requerir los informes y peritajes que estime pertinentes y útiles, practicar las inspecciones de lugares y cosas, disponer o requerir secuestro de elementos y todas las medidas que considere necesarias para el ejercicio de sus funciones. Deberá solicitar orden judicial para practicar

al fiscal de un cúmulo de facultades para reunir prueba. Lo hace en términos en que incluye no sólo las expresamente contempladas, sino también "...todas las medidas que considere necesarias para el ejercicio de sus funciones". Reserva algunas al juez, rodeándolas así de una garantía específica sólo posible en el sistema acusatorio, ya que, en ese sistema, el órgano que decide, el juez, a diferencia del juez inquisidor, cuya jurisdicción suma o absorbe atribuciones propias de la acción fiscal, no tiene fijada la meta de investigar –en efecto, en los procesos de tipo acusatorio, el juzgador, árbitro de una contienda entre partes legitimadas, carece de iniciativa propia en la investigación y de poderes autónomos para investigar la verdad de los acontecimientos–, sino que está colocado en situación de ponderar imparcialmente entre el interés del pueblo en conocer y probar y el del sujeto de preservar su privacidad".

Este interesante análisis establece con claridad las potestades investigativas del fiscal, en el marco de un sistema acusatorio, donde la norma procesal penal establece expresa reserva para determinadas medidas, que el legislador ha considerado que afectan en mayor medida las garantías constitucionales (allanamientos, requisas o interceptación de comunicaciones o correspondencia).

A modo de conclusión de este primer escalón, y de respuesta a los interrogantes planteados, destacamos que los datos identificatorios (o de abonado, como se denominan en España) son datos de carácter personal, que avanzan sobre una primera barrera de privacidad de la persona investigada, pero que no deben confundirse con los datos de tráfico, ni menos aún con los datos de contenido.

Desde un punto de vista jurídico, podemos interpretar que esos datos personales –de acuerdo a la normativa aplicable– podrán ser accedidos sin contar con el consentimiento de su titular para aquellos casos de ejercicios de funciones propias del Estado (art. 5.2.b de la ley 25.326 argentina), por lo que en el contexto de una investigación penal –en el marco de un proceso acusatorio– se considera suficiente para su acceso una orden librada por el fiscal a cargo, no siendo necesario contar con una autorización judicial, reservada para otras instancias de mayor afectación de los derechos.

4.2. El segundo escalón: los datos de tráfico

En este segundo escalón encontraremos una categoría distinta de datos, conocida como datos de tráfico, datos asociados, datos transaccionales, metadatos de la comunicación, entre otras denominaciones que podrán encontrarse en la doctrina y jurisprudencia.

---

allanamientos, requisas o interceptaciones de comunicaciones o correspondencia", www.buenosaires.gob.ar.

Nuevamente consultando el Convenio de Cibercrimen de Budapest[18], donde si bien su art. 1 contiene muy pocas definiciones, entre ellas encontramos la de "datos de tráfico", que de acuerdo a este instrumento son "...cualquier dato informático relativo a la comunicación por medio de sistema informático, generado por el sistema informático que forma parte de la cadena de comunicación, indicando origen, destino, ruta, hora, fecha, tamaño, duración o tipo de servicio subyacente".

De acuerdo a esta definición, podríamos interpretar que los registros de un servidor que guarda las comunicaciones electrónicas entrantes y salientes son un listado de datos de tráfico, toda vez que incluye la dirección IP de origen, dirección IP destino, fecha, hora y ruta de esa comunicación. De la misma forma, esta misma definición es aplicable para las conocidas "*listas sábanas*" de las llamadas telefónicas, donde es posible identificar número de línea que realiza la llamada, número de destino, fecha, hora y duración de la comunicación. Es decir, independientemente del detalle que pueda establecerse en relación al tipo de comunicación, lo importante es tener en claro que entre los datos de tráfico nunca podremos encontrar algún tipo de contenido de la comunicación.

En la normativa española podemos encontrar otro concepto similiar dentro de la Ley Orgánica de Enjuiciamiento Criminal 13/2015, en el Capítulo V "La interceptación de las comunicaciones telefónicas y telemática", en el art. 588 ter b), define "datos electrónicos de tráfico o asociados" como "todos aquellos que se generan como consecuencia de la conducción de la comunicación a través de una red de comunicaciones electrónicas, de su puesta a disposición del usuario, así como de la prestación de un servicio de la sociedad de la información o comunicación telemática de naturaleza análoga".

Teniendo en claro el alcance de su concepto, podremos avanzar quizás hacia uno de los tópicos claves de este artículo, que es el argumento jurídico sobre la legitimidad en el acceso a esta clase de información, discusión que desde ya, adelantamos, con el paso de los años se han observado distintas posturas, que intentaremos ir desandando. Entre todas las preguntas que el lector podría realizarse sobre esta temática, elegimos algunas para abordar aquí: *¿Que nivel de afectación a las garantías constitucionales existe al acceder a los datos de tráfico de una comunicación? ¿Es necesario contar con autorización judicial para poder acceder a un listado de datos de tráfico de las comunicaciones realizadas por una persona? ¿Es constitucional obligar*

[18] Convenio de Ciberdelincuencia del Consejo de Europa de Budapest, de 23 de noviembre de 2001.

a un proveedor de comunicaciones que realice la guarda de todos los datos de tráfico de las comunicaciones de sus abonados?

Si bien algo ya se ha adelantado en el desarrollo del primer escalón, veremos aquí con mayor profundidad el alcance y protección jurídica de esta segunda categoría de datos. En relación a la primera pregunta, sobre el nivel de afectación de las garantías a través de los datos de tráfico, ya hemos citado uno de los antecedentes más importantes, como es el caso "Malone"[19], en el cual se debatió el alcance en el amparo al secreto de las comunicaciones.

En este denominado *leading case*, analizado en un reciente y completo estudio del Dr. David Calvo Lopez[20], se reconoció expresamente la posibilidad de que el art. 8 CEDH[21] pudiera resultar violado por el empleo de un artificio técnico que permita registrar cuáles hayan sido los números telefónicos marcados sobre un determinado aparato, aunque no acceda al contenido de la comunicación misma. Es decir, relacionado a la primera pregunta que nos hemos realizado, podemos responder que, en principio, existe aceptación jurisprudencial en entender que la protección jurídica de los datos de tráfico, por la potencialidad en la afectación de las garantías que posee esta categoría de datos, se encuentra asimilada al mismo nivel de protección jurídica que los datos de contenido.

Decimos en principio, toda vez que válidamente el lector podría preguntarse si todos los datos de tráfico afectarían de la misma forma a los derechos constitucionales aquí involucrados. En este sentido, la circular 1/2013[22] de la Fiscalía General del Estado es-

[19] Ibídem.

[20] Calvo López, David, "Capacidades de actuación del Ministerio Público Fiscal y la Policía Judicial tras la reforma procesal operada por la Ley Orgánica 13/2015", *Jornadas de Especialistas celebradas en el Centro de Estudios Jurídicos de Madrid*, 16 y 17 de febrero de 2017.

[21] Art. 8 del Convenio para la Protección de los Derechos Humanos y de las libertades fundamentales: "Derecho al respeto a la vida privada y familiar. 1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás".

[22] Fiscalía General del Estado (España), circular 1/2013 sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas. www.fiscal.es.

pañol explica que "no todos los datos digitalizados merecen la consideración de datos propios del contenido material del derecho a la inviolabilidad de las comunicaciones. Debe analizarse la funcionalidad de cada dato para ubicarlo bajo el manto protector del derecho a la intimidad (art. 18.1 CE), del derecho a la inviolabilidad de las comunicaciones (art. 18.3 CE) o del derecho a la protección de datos (art. 18.4 CE), cada uno con su propio sustrato axiológico y, correlativamente, cada uno con una protección de intensidad variable".

Sí estarían incluidos, como señala la citada circular, aquellos "datos accesorios pero íntimamente ligados a la propia comunicación" por revelar el origen y destino de la misma, su momento y duración y, por último, los referentes al volumen de la información transmitida y el tipo de comunicación entablada. Son, en definitiva, datos que se generan mientras la comunicación se encuentra en curso.

En similar criterio se ha expresado el Tribunal Supremo en la Sentencia STS 247/2010[23], relacionado a un caso de posesión de pornografía infantil, donde se discutía la validez o no de las medidas de investigación realizadas, y la posible afectación de los derechos constitucionales del imputado. En la sentencia, se realiza una distinción fundamental para resolver cualquier cuestión relativa a los derechos amparados por el art. 18 CE. En la misma afirma: "Distinguimos pues dos conceptos: a) Datos personales externos o de tráfico que hacen referencia a una comunicación concreta y contribuyen a desvelar todo o parte del secreto que protege el art. 18-3 C.E EDL 1978/3879; b) Datos o circunstancias personales referentes a la intimidad de una persona (art. 18-10 C.E. EDL 1978/3879), pero autónomos o desconectados de cualquier comunicación, que caerán dentro del derecho a la protección de datos informáticos o habeas data del art. 18-4 C.E. EDL 1978/3879 que no pueden comprometer un proceso de comunicación. Desde esta perspectiva dicotómica la absoluta equiparación de todo tipo de datos de tráfico o externos o la inclusión de todos ellos dentro del derecho al secreto de las comunicaciones comportaría un auténtico desenfoque del problema, pues incorporaría en el ámbito de la protección constitucional del art. 18-3, circunstancias cuyo tratamiento jurídico no debería separarse del que se dispensa a la protección de datos o al derecho a la autodeterminación informática del art. 18-4 C.E. EDL 1978/3879 (véase por todas S.T.S. nº 249 de 20/5/08 EDJ 2008/90719)".

En el caso concreto se resolvió que "es patente que los datos cuyo obtención se pretende por el Fiscal no tienen relación ni afectan ni

[23] Sentencia nº 247/2010 de TS, Sala 2ª de lo Penal, 18 de marzo de 2010, fallo completo: https://supremo.vlex.es.

interceptan ni descubren ni tratan de descubrir una comunicación concreta, sino que por ser preciso para la acción investigadora el conocimiento del domicilio, número de teléfono o identidad del titular del terminal informático que opera en la Red (I.P.), la solicita a la operadora, al objeto de pedir del juez un mandameinto de entrada y registro con fines indagatorios o de investigación de un posible delito, acerca del que se conocen datos indiciarios".

Esta jurisprudencia, de similar interpretación a la citada anteriormente en Argentina [24], concluye que al no tratarse de datos de tráfico –toda vez que solamente se han solicitado datos identificatorios personales–, no será necesaria la orden judicial para el caso de solicitud de los datos de abonado (nuestro primer escalón), por considerarse que no existe allí una afectación a una comunicación concreta, y por lo tanto, no hay afectación a un derecho constitucional.

Es decir –y ya aquí comenzando con la respuesta a la segunda pregunta planteada–, que sólo ante el análisis positivo sobre si los datos de tráfico solicitados (como suele suceder con el listado de llamadas o los datos de tráfico de un ISP) permitan afectar la inviolabilidad de las comunicaciones y, por lo tanto, el secreto de las comunicaciones, será necesario contar con autorización judicial de juez competente para poder válidamente acceder a este segundo escalón o categoría de datos.

A nivel normativo, esta discusión se encontró resuelta dentro de la Ley Orgánica de Enjuiciamiento Criminal 13/2015, cuyo art. 588 ter b) exige que la resolución judicial habilitante precise el contenido de la intervención de las comunicaciones telemáticas, que puede estar referido a tres conceptos distintos: a) el mensaje comunicado; b) los datos electrónicos de tráfico o asociados al proceso de comunicación, y c) aquellos producidos con independencia del establecimiento o no de una concreta comunicación:

> "La intervención judicialmente acordada podrá autorizar el acceso al contenido de las comunicaciones y a los datos electrónicos de tráfico o asociados al proceso de comunicación, así como a los que se produzcan con independencia del establecimiento o no de una concreta comunicación, en los que participe el sujeto investigado, ya sea como emisor o como receptor, y podrá afectar a los terminales o los medios de comunicación de los que el investigado sea titular o usuario".

Por último, en relación a un adelanto de respuesta de la tercera pregunta sobre la constitucionalidad de la obligación de guarda de esta

[24] Ídem, p. 16.

categoría de datos, informamos al lector que si bien no ahondaremos en todos los argumentos jurídicos que deberían tratarse para hacer un desarrollo adecuado y serio del tema, que por cuestiones de tiempo y espacio que exceden la labor del presente trabajo, citaremos solamente algunos aspectos centrales y medulares de dicha discusión.

En el año 2006 la Unión Europea aprobó la Directiva sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, popularmente conocida como "Directiva de retención de datos"[25], que a lo largo de los años fue gestando normativas internas de los distintos países europeos que regulan sus propias condiciones para la conservación de este tipo de datos.

El objetivo buscado por la normativa general era el de obligar a los proveedores de servicios de comunicaciones electrónicas de acceso público o red pública de comunicación a conservar los datos generados o tratados por los mismos, para garantizar que los datos estén disponibles con fines de investigación, detección y enjuiciamiento de delitos graves, donde cada país determinaba su interpretación de lo que se consideraba delitos graves de acuerdo a su propia normativa penal.

En la práctica, la aplicación de la Directiva implicaba que existía una retención de datos de tráfico de todos los usuarios, por un tiempo determinado (entre 6 meses y 2 años por lo general), independientemente de si los mismos estaban o no siendo parte de una investigación penal que justificaba el acceso a dichos datos y, por lo tanto, la afectación de sus garantías constitucionales.

Sin embargo, esta Directiva no fue siempre aceptada por todos, y ya en su momento había generado una gran polémica y controversia, ya que para algunos sectores su articulado vulneraba la privacidad de los ciudadanos. De hecho, en algunos países nunca fue tenida en consideración para su regulación interna, ya que se entendía que su regulación era inconstitucional. Ya en 2010, el Tribunal Constitucional alemán[26] advirtió (como venía haciendo con otros casos anteriores[27]) el riesgo de que el uso de la tecnología,

[25] Directiva 2006/24/CE, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la directiva 2002/58/CE. https://eur-lex.europa.eu.

[26] "Alemania prohíbe la retención de datos telefónicos y de internet", www.libertaddigital.com.

[27] BverfG, 1 BvR 370/07, de 27 de febrero de 2008.

a través del acopio y cruce masivo de datos, pueda dar lugar a la creación de los referidos "perfiles de personalidad" de los ciudadanos hasta el punto de llegar a influir de manera determinante en el comportamiento de los individuos, lo cual entiende que no sólo va en detrimento de las posibilidades de desarrollo individual de los individuos, sino también de la comunidad, porque la autodeterminación es una condición funcional elemental de una nación democrática libre, fundada en la capacidad de sus ciudadanos para cooperar y actuar.

Con motivo de un recurso de inconstitucionalidad contra las reformas que tenían por misión incorporar al ordenamiento jurídico germano la directiva europea de retención de datos, el Tribunal Constitucional alemán declaró en su sentencia de 2 de marzo de 2010 [28] que dicha regulación vulneraba dos principios claves: el principio de proporcionalidad (*Verhältnismäßigkeit*) y el principio de determinación jurídica o claridad legal (*Normenklarheit*), pues aunque la efectividad de la persecución criminal, la defensa de la Seguridad y el cumplimiento de las tareas de los servicios de inteligencia son fines legítimos que pueden constituir una injerencia justificada en el secreto de las telecomunicaciones, y aunque tal derecho fundamental no prohíbe cualquier almacenamiento de datos de tráfico, la regulación impugnada suponía un almacenamiento desproporcionado "con una extensión como hasta ahora el ordenamiento no había conocido previamente, pues abarca todo el período de seis meses y prácticamente todos los datos de tráfico de las comunicaciones de todos los ciudadanos sin conexión con una conducta reprochable atribuible, incluso de modo abstracto, a una peligrosidad o una situación cualificada (...). Dependiendo de la utilización de las telecomunicaciones y el futuro de tal aumento de la densidad de almacenamiento, puede permitir la producción significativa de perfiles de personalidad y de movimiento de prácticamente todos los ciudadanos, aumenta el riesgo de los ciudadanos a estar expuestos a mayores y posteriores investigaciones, sin ni siquiera el motivo para el que se ha dado el uso, y evoca un sentimiento de vaga amenaza que puede afectar a un ejercicio imparcial de los derechos fundamentales en muchos ámbitos" [29].

[28] BVerfG, 1 BvR 256/08, que resuelve los procesos BvR 256/08, 263/08 y 586/08.

[29] Ortiz Pradillo, Juan Carlos, "La investigación del delito en la era digital: Los derechos fundamentales frente a las nuevas medidas tecnológicas de investigación", *Estudios de Progreso*, Fundación Alternatives, www.falternativas.net.

Siguiendo esta esta última postura más crítica de la directiva europea, citaremos un importante trabajo de análisis realizado por el fiscal Luis Vázquez Seco [30], quien a modo de resumen de su trabajo, expresa: "ya desde su promulgación, desde instancias tanto privadas como institucionales se alzaron voces poniendo de relieve aspectos de la directiva 2006/24/CE que debían ser modificados. Con el paso del tiempo se constató que lejos de armonizar y acercar las legislaciones de los Estados miembros sobre la materia, provocó todo lo contrario, una diversidad de regulaciones muy discrepantes en aspectos como el principio de proporcionalidad, los niveles de seguridad de los datos, los procedimientos y requisitos para su utilización, etc., que causaron otro efecto no menos importante, cual es que los operadores de telecomunicaciones, según el Estado donde prestaran sus servicios, se veían sometidos a condiciones totalmente dispares que se traducían fundamentalmente en el coste de los servicios ofertados, que a su vez repercutía en los consumidores (los costes de conservar los datos 6 meses son muy inferiores a los generados por la conservación durante 2 años). Y lo mismo en cuanto a la eficacia de las investigaciones policiales, ya que había Estados que permitían utilizar dichos datos para esclarecer prácticamente cualquier delito, mientras otros los restringían a unos pocos, por lo que según el Estado donde se encontraran almacenados los datos, el resultado de la investigación sería muy distinto" [31].

Años más tarde, tras varias declaraciones de inconstitucionalidad a lo largo del viejo continente, finalmente la sentencia del Tribunal de Justicia de la Unión Europea de 8 de abril de 2014, al resolver las cuestiones prejudiciales planteadas respectivamente por la *High Court of Ireland* (Irlanda) y el *Verfassunsgerichtshof* (Tribunal Constitucional de Austria), terminó anulando la directiva 2006/24/CE del Parlamento Europeo, en razón de que si bien las obligaciones de conservación y puesta a disposición de datos sobre comunicaciones a que se refiere son necesarias para posibilitar su utilización en la prevención, detección y persecución de delitos graves, la considera desproporcionada, ya que pese a suponer una injerencia de gran magnitud en los derechos fundamentales a la privacidad y protec-

[30] El Dr. Luis Vázquez Seco es fiscal delegado de Criminalidad Informática en la Fiscalía Provincial de La Coruña, España.

[31] VÁZQUEZ SECO, Luis, "Retención obligatoria de datos de tráfico de las comunicaciones telefónicas y/o electrónicas. Análisis de la sentencia del tribunal de justicia de la unión europea de 8 de abril de 2014 en los asuntos acumulados c-293/12 y c594/12 (Digital Rights Ireland y Seitlinger y otros), www.fiscal.es.

ción de datos de carácter personal, no regula debidamente las garantías que deben servir de contrapeso a tal injerencia.

A modo de resumen, podríamos afirmar que el fundamento jurídico principal por el cual se empezó a declarar la inconstitucionalidad de distintas normativas europeas relacionadas a la retención de datos de tráfico, estriba en la falta de proporcionalidad, la falta de un adecuado equilibrio o balance entre la afectación a los derechos fundamentales que dicha retención de datos provoca, frente a la utilidad que dichos datos representan en las investigaciones de delitos (graves), marcada por los insuficientes controles o requisitos que justifiquen tales avances sobre estos derechos.

4.3. El tercer escalón: los datos de contenido

Hemos llegado al tercero y último escalón en nuestra construcción jurídica, que consiste en los datos de contenido y que es, desde el punto de vista de la afectación de los derechos, el nivel más alto de intromisión en las garantías constitucionales.

Si bien su concepto no se encuentra definido de forma directa en la Convención de Budapest, podremos ensayar uno a través de la comparación con los propios datos de tráfico. Un reciente estudio sobre "Retención y privacidad de datos"[32] los compara afirmando que "al realizar un envío por correspondencia los datos de tráfico o metadatos son el sobre y las direcciones del remitente y destinatario, mientras que los datos de contenido son la carta misma". Debemos entender entonces por datos de contenido a la comunicación en sí misma, al propio mensaje que un emisor envía a uno o más receptores, independientemente del medio utilizado (carta, fax, llamada telefónica, whatsapp o correo electrónico). Es decir que ya no son datos relativos a la comunicación en sí, ya no es el continente sino el contenido –concepto jurídico si los hay–.

No encontramos aquí discusiones sobre que nos estamos en presencia del nivel de afectación más profunda que podría pensarse a nivel jurídico, superando todas las barreras a la intimidad del titular, accediendo y conociendo sus comunicaciones, donde se supone que el Estado ha considerado indispensable, a los fines de la averiguación de la verdad de los hechos –y que no existe otra vía menos invasiva–, la necesidad de acceder y conocer el contenido de esas comunicaciones privadas.

[32] The Social Engineering Unit, "Retención y privacidad de datos: algunas lecciones derivadas de las diversas prácticas internacionales", http://the-siu.net.

Todos los derechos repasados al comenzar este artículo son afectados en este último nivel: El derecho a la intimidad, la privacidad, el secreto de las comunicaciones, en el fondo, todos derivados del derecho humano a la dignidad. En consecuencia de los niveles de afectación de los derechos que representa, no queda lugar a dudas sobre la necesidad de autorización judicial –debidamente fundada– para poder acceder a los datos de contenido como última categoría de información.

En la práctica y en concordancia con lo expuesto en la guía internacional para la obtención de evidencia [33], además de la necesidad de una resolución judicial que ordene al proveedor de servicios de comunicación aportar esta categoría de información, las empresas también solicitan que exista lo que se considera *causa probable*, que en Estados Unidos es el nivel mismo de exigencia jurídica que se requiere para poder –por ejemplo– solicitar una orden de allanamiento a un domicilio.

No debe considerarse *a priori* que estos requisitos son un capricho de las empresas privadas –al menos de forma genérica–, sino más bien de una exigencia derivada de un mandato constitucional agregado en la cuarta enmienda de la Constitución de los Estados Unidos, en el cual se afirma:

> "El derecho de los habitantes de que sus personas, domicilios, papeles y efectos se hallen a salvo de pesquisas y aprehensiones arbitrarias, será inviolable, y no se expedirán al efecto mandamientos que no se apoyen en un motivo verosimil, estén corroborados mediante juramento o protesta y describan con particularidad el lugar que deba ser registrado y las personas o cosas que han de ser detenidas o embargadas" [34].

Es decir, las órdenes deben mencionar una causa probable, ratificada mediante juramento o declaración, y deben describir minuciosamente el lugar donde se realizará la pesquisa y los objetos que se secuestrarán.

Podría aquí el lector hacerse una nueva serie de preguntas: *¿Puede intervenirse cualquier tipo de comunicación? ¿Existen límites a tener en cuenta, o bien podría el Estado intervenir cualquier comunicación que considerara pertinente? ¿Es posible emplear en un proceso penal medios probatorios no regulados en la ley procesal?*

[33] Ídem, p. 12.

[34] Texto extraído de la versión de la Constitución de Estados Unidos traducida en www.constitutionfacts.com.

Para dar respuesta a tales interrogantes, avanzaremos en una breve pero muy importante sección dedicada a los principios y límites a tener en cuenta en las medidas de investigación.

5. Principios y límites en las medidas de investigación

Desde el punto de vista de las garantías constitucionales, la *causa probable* que describíamos al finalizar la última sección aparece como una sana exigencia sobre la necesidad de contar con la existencia de determinados elementos o indicios, que apuntalen de forma sólida los fundamentos por los cuales se hace indispensable acceder al nivel más invasivo y crítico de información de una persona.

En esta línea, entre los principios más importantes aceptados a nivel internacional podemos encontrar los principios de proporcionalidad, idoneidad, excepcionalidad y necesidad. España ha comprendido la importancia de la regulación clara de estos requisitos jurídicos, y ha dedicado un artículo a su incorporación y descripción en la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica [35]:

> Art. 588 bis a: Principios rectores
>
> 1. Durante la instrucción de las causas se podrá acordar alguna de las medidas de investigación reguladas en el presente capítulo siempre que medie autorización judicial dictada con plena sujeción a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida.
>
> 2. El principio de especialidad exige que una medida esté relacionada con la investigación de un delito concreto. No podrán autorizarse medidas de investigación tecnológica que tengan por objeto prevenir o descubrir delitos o despejar sospechas sin base objetiva.
>
> 3. El principio de idoneidad servirá para definir el ámbito objetivo y subjetivo y la duración de la medida en virtud de su utilidad.
>
> 4. En aplicación de los principios de excepcionalidad y necesidad sólo podrá acordarse la medida:
>
> a) cuando no estén a disposición de la investigación, en atención a sus características, otras medidas menos gravosas para los derechos fundamentales del investigado o encausado e igualmente útiles para el esclarecimiento del hecho, o

[35] L.O. 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica (B.O.E. de 6 de octubre).

b) cuando el descubrimiento o la comprobación del hecho investigado, la determinación de su autor o autores, la averiguación de su paradero, o la localización de los efectos del delito se vea gravemente dificultada sin el recurso a esta medida.

5. Las medidas de investigación reguladas en este capítulo sólo se reputarán proporcionadas cuando, tomadas en consideración todas las circunstancias del caso, el sacrificio de los derechos e intereses afectados no sea superior al beneficio que de su adopción resulte para el interés público y de terceros. Para la ponderación de los intereses en conflicto, la valoración del interés público se basará en 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 con la restricción del derecho.

Si bien todos los principios tienen su radical importancia, por cuestiones de espacio abordaremos sólo el principio de proporcionalidad, que de acuerdo a nuestra consideración quizá sea el que observamos más aplicable a la luz de lo que se pretende abordar en este artículo.

De acuerdo al Dr. Cianciardo[36], este principio de proporcionalidad supone el ejercicio razonable del poder político que desde una perspectiva constitucional pretende resguardar las libertades fundamentales atendiendo a que la intervención pública que se ejecuta sea idónea, indispensable y proporcionada; esto es, que el medio elegido sea adecuado al fin y resulte el más moderado dentro de aquellos igualmente eficaces.

No obstante el reconocimiento genérico en la exigencia del cumplimiento de estos principios fundamentales, la normativa española citada avanza y regula una serie de requisitos jurídicos especiales, aplicables de acuerdo a cada una de las medidas, entre los que podemos encontrar[37]:

Art. 588 bis b. *Solicitud de autorización judicial*: Establece todos los elementos que deberán formar parte de una solicitud de autorización judicial para la aplicación de algunas de las medidas reguladas.

Art. 588 bis c. *Resolución judicial*: Establece el plazo que tendrá el juez para resolver le pedido de autorización, así como todos los

[36] CIANCIARDO, Juan, *El conflictivismo en los derechos fundamentales*, Eunsa, Pamplona, 2000.

[37] Para ver los textos completos de los artículos citados, remitimos al lector a acceder a la norma L.O. 13/2015, de 5 de octubre.

extremos que deberán constar en dicha autorización (identidad de los investigados, extensión de la medida, duración, unidad a cargo, finalidad perseguida, entre otros).

Art. 588 bis d. *Secreto*: Establece que la solicitud y las actuaciones posteriores se sustanciarán de forma separada y secreta, sin necesidad de que se establezca expresamente el secreto.

Art. 588 bis e. *Duración*: Establece que la medida podrá ser prorrogada, mediante auto motivado, por el juez competente, de oficio o previa petición razonada del solicitante, siempre que subsistan las causas que la motivaron.

Art. 588 bis f. *Solicitud de prórroga*: Establece los requisitos necesarios y condiciones para pedir una prórroga de la medida previamente autorizada.

Art. 588 bis g. *Control de la medida*: Establece la obligación de mantener informado al juez de instrucción sobre el desarrollo y resultados de la medida.

Art. 588 bis h. *Afectación de terceras personas*: Establece que aun en el caso de afectarse a terceras personas, se podrán autorizar las medidas, en las condiciones autorizadas.

Art. 588 bis i. *Utilización de la información obtenida en un procedimiento distinto y descubrimientos casuales*: Remite al art. 579 bis para establecer qué sucede con los llamados descubrimientos casuales.

Art. 588 bis j. *Cese de la medida*: Establece en qué casos podrá el juez ordenar el cese de las medidas autorizadas.

Art. 588 bis k. *Destrucción de registros*: Establece las medidas que deberán tomarse sobre la información una vez finalizada la utilidad en la investigación.

Como podemos observar y celebrar, España ha realizado un importante trabajo al momento de regular, de la forma más detallada posible, los distintos requisitos jurídicos que se consideran necesarios para fundamentar las medidas de prueba solicitadas.

Diferente situación en materia procesal penal existe en Argentina –así como en otros tantos países latinoamericanos–, donde aún persiste una ausencia importante de esta clase de regulación en relación a las medidas de investigación tecnológica.

Impecable abordaje y opinión sobre este tópico realiza el Dr. Marcos Salt en el prólogo de un libro sobre prueba electrónica[38], en el cual afirma "Es por ello que desde hace tiempo venimos llaman-

[38] Salt, Marcos, Prólogo al libro *Vigilancia electrónica y otros modernos medios de prueba*", de Carlos Christian Sueiro, Hammurabi, Buenos Aires, 2017. www.libreriahammurabi.com.

do la atención sobre la urgente necesidad de analizar las implicancias jurídicas que el uso de la tecnología informática tiene para el proceso penal. Especialmente, la necesidad de regular en los códigos procesales penales 'medios de prueba' que tengan en cuenta las características especiales de las distintas formas de evidencia digital y sus marcadas diferencias con la evidencia física. Sólo de esta manera será posible dejar atrás la tendencia de nuestros tribunales a utilizar acríticamente el principio de 'libertad probatoria' para incorporar al proceso penal evidencia digital usando normas pensadas para la prueba física. Resulta a esta altura evidente que la tecnología informática aporta poderosas herramientas de investigación y prevención del delito que difieren de manera sustancial de lo que las legislaciones procesales vigentes en nuestro país previeron al regular los medios de prueba tradicionales".

Expresamos una absoluta adhesión a las palabras expresadas por el Dr. Salt, destacando sobre todo la importancia y necesidad de una regulación procesal penal que permita no sólo preservar a los ciudadanos de posibles medidas abusivas por parte del Estado, sino además de evitar que bajo el impreciso (y por lo tanto bastante flexible) principio de la libertad probatoria se realicen medidas de investigación de forma desproporcionada, injustificada y sin controles.

Para evitar este tipo de excesos en el uso del poder coercitivo por el Estado, es precisamente que desde la teoría dura del derecho penal siempre ha existido la aplicación del principio *nulla coactio sine lege*. Este principio, vinculado también al principio de legalidad o de reserva, refiere a todas aquellas actividades del Estado –entre las que se encuentra la actividad probatoria en el marco de los procesos penales– que impliquen una injerencia en los derechos fundamentales de los ciudadanos, y tienen como condición de validez una autorización legal previa.

Es decir que, para poder autorizar la realización de una medida de investigación, que afectará siempre –en mayor o menor medida– algún derecho constitucional del ciudadano, la misma deberá estar basada o fundamentada en alguna norma procesal penal previa que establezca, al menos con un mínimo de regulación, las condiciones para llevar a cabo la medida.

Mucho mejor desarrollo sobre este principio expresa el Dr. Gustavo Bruzzone[39], quien siguiendo una línea de pensamiento del

[39] BRUZZONE, Gustavo, "La *nulla coactio sine lege* como pauta de trabajo en el proceso penal", *Estudios sobre Justicia Penal.* Homenaje al Profesor Julio B. J. Maier, Ed. Del Puerto, Buenos Aires, 2005.

ilustre profesor Dr. Julio Maier, trabaja sobre la necesidad de elaborar una teoría general de las medidas de coerción, que establezca mejores bases desde lo jurídico para trabajar sobre la pertinencia o proporcionalidad de algunas medidas.

En este contexto, Bruzzone explica que al momento de imponerse una medida de coerción se debería seguir un procedimiento similar al que utilizamos para concluir en la imposición de una pena o una medida de seguridad. Así como hablamos de una tipicidad penal, también deberíamos comenzar a pensar en la existencia de determinados presupuestos que permitan hablar de una "tipicidad procesal" o, más precisamente, de los tipos de las medidas de coerción. Un riesgo latente, explica Bruzzone, es la facilidad para confundir los medios de prueba en general con medidas de coerción a través de las cuales se puede incorporar elementos de prueba. En relación a los medios de prueba, en Argentina tenemos un sistema abierto, toda vez que se encuentra reconocido el principio de libertad probatoria. Como explica el autor, "Si bien existe *numerus apertus* en materia probatoria, no ocurre lo mismo con las medidas de coerción que suponen la incoporación de pruebas, de aquellas que sólo tienden a la obtención de los fines del proceso y que, sólo en forma mediata, responden a una finalidad probatoria".

A nuestro criterio –y como anteriormente ya expresaba el Dr. Salt–, la advertencia realizada es de extrema importancia, toda vez que suele pensarse que el principio de libertad probatoria funciona como una especie de comodín que habilita a llevar adelante cualquier tipo de diligencia investigativa (medidas de coerción o de injerencia), que como ya hemos afirmado suponen –salvo casos ya explicados en la base de nuestra escalera– una afectación directa en contra de una garantía o de un derecho.

En un informe de 2018 dedicado a la regulación en cibercrimen publicado por la Comisión de Prevención del Crimen y Justicia Criminal de Naciones Unidas [40], se puede observar las diferencias existentes entre los avances en la regulación penal de fondo en cibercrimen, sobre la regulación de los aspectos procesales penales.

De acuerdo a este informe, "la legislación específica, consistente con los requisitos de los derechos humanos y el Estado de derecho, es la base para las acciones de justicia criminal sobre cibercrimen y evidencia electrónica. Muchos gobiernos de todo

[40] *Cybercrime: the state of legislation: UN Commission for Crime Prevention and Criminal Justice, Side-event* - Vienna International Centre, 15 May 2018, Conference Room M3.

el mundo han emprendido reformas legales durante los últimos cinco años, utilizando muchas veces la Convención de Budapest sobre Ciberdelincuencia como una guía. La aprobación de legislación sustantiva para tipificar como delito los delitos contra las computadoras y por medio de computadoras, así como la regulación de las facultades procesales para permitir la recopilación de pruebas electrónicas, suele ser el punto de partida para construir las capacidades de desarrollo. Se observa un progreso mensurable y se pueden extraer lecciones importantes de esta experiencia".

Ese progreso mensurable está basado en unas estadísticas que han realizado en relación al avance en los distintos continentes sobre la regulación penal en cibercrimen, tanto sobre derecho penal sustantivo como sobre las reglas de derecho procesal penal aplicables a la evidencia electrónica o digital.

Comparativamente, en estadísticas relacionadas al nivel de normativización entre la regulación del derecho penal de fondo y el derecho penal de forma, aquellas del primer grupo siempre son superiores a las segundas, toda vez que es normal que en el proceso de regulación primero se priorice la tipificación penal de la acción considerada delictuosa, y posteriormente (y a veces demasiado posteriormente) se piensa en las regulaciones de ajuste o adaptación de las normas procesales penales necesarias para avanzar en la ejecución práctica de esas investigaciones penales que permitan combatir los delitos anteriormente tipificados.

Si bien el estudio es mucho más complejo, a los fines de este artículo sólo citaremos los datos publicados en relación a las normativas procedimentales sobre la evidencia electrónica, donde es posible observar que los países americanos se encuentran en tercer lugar sobre los 5 continentes, siendo Europa la referencia con los países de mayor desarrollo.

Como aspecto positivo, destacamos que es motivo de celebración el avance general en las regulaciones de materia procesal relativas a la evidencia electrónica, que es observable en todos los continentes al comparar los estudios de 2013 y 2018.

A modo de cierre de esta sección, y como hemos adelantado en varias oportunidades, nuestra postura adhiere a la necesidad (en Argentina) de una adecuada regulación sobre el aspecto procesal penal, que establezca –similar al modelo español y de otros países– por un lado las distintas medidas de investigación con las que el fiscal y las fuerzas de seguridad pueden contar, y por el otro, con el mayor nivel de detalle posible, los requisitos y límites jurídicos que deberán aplicarse para la autorización y ejecución de dichas medidas.

6. Medidas o técnicas de investigación tecnológica

Dedicaremos la parte final de este artículo a realizar una descripción de diferentes medidas y técnicas de investigación tecnológica que actualmente son utilizadas, estableciendo sus relaciones con su posible afectación de derechos y garantías constitucionales, de acuerdo a los criterios jurídicos previamente desarrollados.

Desde un punto de vista metodológico, realizaremos sólo una breve descripción de la técnica o medida de investigación en sí, categorizando dicha medida de acuerdo al tipo o clase de información a la que es posible acceder como resultado de su ejecución.

Entre otras consideraciones, debemos advertir que abordaremos un listado de técnicas y medidas de investigación tecnológica genérica, independientemente de si existe o no una adecuada regulación jurídica para la misma, lo cual nos obligaría a analizar la normativa de un país en particular, perdiéndose la generalidad buscada en el artículo. Tampoco abordaremos en el análisis la necesidad o no de autorización judicial, aspecto jurídico cuya discusión también ya ha sido abordada en este trabajo.

En general, intentaremos concentrarnos en la medida de investigación, que es en definitiva la que deberá solicitar el fiscal o juez competente en el marco de una causa determinada. Sin embargo, en algunos casos, indicaremos la técnica utilizada (que es como muchos lectores podrán reconocer la medida en sí). El ejemplo claro es, en el caso de la realización de OSINT[41] (técnica de investigación sobre fuentes abiertas), que desde el punto de vista jurídico puede encontrarse con distintos nombres, como un informe de inteligencia criminal, investigación preliminar o preparatoria, etc.

A modo preliminar, y desde un punto de vista teórico, es posible realizar un agrupamiento de las medidas o técnicas de investigación tecnológica, identificando aquellas que tienen por objetivo la identificación del delincuente, sobre aquellas cuyo objetivo principal es la obtención de evidencia útil para la imputación del delito. Sin embargo, a los fines buscados, listaremos a todas juntas independientemente de la finalidad buscada, que en última instancia su funcionalidad dependerá del caso concreto.

Con finalidad pedagógica de repaso sobre los aspectos ya analizados, y con la intención de aportar un elemento gráfico que sea de utilidad al lector para intentar resumir los niveles de afectación de los derechos de acuerdo al tipo información accedida a través de las medidas de investigación tecnológica, brindamos el siguiente

[41] OSINT: *Open Source Intelligence.*

gráfico y tabla comparativa, con la clasificación que utilizaremos para esta etapa final del trabajo.

Categorías de información:
Nivel 0 – Datos de acceso público e irrestricto
Nivel 1 – Datos de abonado o de identificación
Nivel 2 – Datos de tráfico o transaccionales
Nivel 3 – Datos de contenido

Con respecto a la aplicación práctica de las categorías y a modo de ejemplo, supongamos el abordaje de la clásica medida de intervención de comunicaciones telefónicas, la misma será de categoría 3, toda vez que el resultado de la medida será el acceso a las conversaciones que la persona investigada tenga con terceros, siendo estos claramente datos de contenido.

Sin embargo, no en todas las medidas será tan simple su categorización, ya que en algunos casos podrá ser de categorías mixtas o compartidas. Por ejemplo, ante el caso de la intervención de comunicaciones electrónicas, sería posible a través de un ataque "*Man in the Middle*" (MiM), capturar los paquetes que circulan por la red. Ahora bien, en el caso de que las comunicaciones se encuentren cifradas (por ejemplo un chat de Whatsapp), no será posible acceder a su contenido, pero sí a parte de sus datos de tráfico. En cambio, en esa misma captura, sobre comunicación efectuada por un protocolo sin cifrar, será posible acceder a todo su contenido en texto plano. En conclusión, en este caso práctico, la categorización podría ser compartida en los niveles 2 y 3.

Sin más preámbulos, a continuación listamos las medidas y técnicas de investigación tecnológicas, con su breve descripción y la categorización en la afectación de derechos de acuerdo a nuestro criterio, buscando organizarlas desde las menos invasivas hasta aquellas que más injerencia provocan sobre los derechos del sujeto investigado.

6.1. Inteligencia de fuentes abiertas (OSINT)

Descripción: Las técnicas de investigación en fuentes abiertas son cada vez más utilizadas en todo tipo de investigación, basado en que las personas voluntariamente hacen públicos cada vez más aspectos de su vida privada. Esta técnica se concentra en la identificación, recolección, procesamiento y entrega de información sobre un determinado objetivo (en nuestro caso, una persona), utilizando fuentes de información abierta (buscadores de internet, redes sociales, foros, etc).

Categoría de información obtenida: Nivel 0 – Datos de acceso público o irrestricto

Nivel de afectación de derechos: Nulo

6.2. Ciberpatrullaje

Descripción: Esta medida de investigación consiste en el acceso, análisis y procesamiento masivo de información pública disponible en internet, buscando detectar comportamientos criminales en línea que, en caso de reunirse algunos indicios o elementos, podrían dar lugar al inicio de una investigación penal concreta. De todas las medidas listadas, esta es la única que no refiere a la investigación de un delito concreto, sino que es una actividad de prevención que suele ser cada vez más realizada por distintas fuerzas alrededor del mundo [42].

La diferencia entre el ciberpatrullaje y el agente encubierto digital (otras de las medidas listadas) es que en este último la fuerza de seguridad que oculta su identidad lo hace con un objetivo concreto –la obtención de información útil para una investigación ya en curso–. En cambio, en el ciberpatrullaje es una etapa previa, donde ni siquiera es necesario ocultar la identidad del agente de seguridad, toda vez que estamos ante casos cuya exposición pública (sin límites de privacidad) permite un acceso irrestricto a la información por cualquier usuario.

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

Categoría de información obtenida: Nivel 0 – Datos de acceso público o irrestricto

Nivel de afectación de derechos: Nulo

6.3. Identificación por huella digital (*browser fingerprinting*)

Descripción: Esta técnica consiste en la recolección, procesamiento y análisis de un conjunto de información pública que expone un sistema determinado al conectarse a un servidor controlado (sistema operativo, versión, navegador, *plugins* instalados, fuentes instaladas, resolución de pantalla, entre otros). La técnica (usualmente conocida por el funcionamiento de las *cookies*) consiste en el agrupamiento de este conjunto de datos, generando una "huella digital" de dicho usuario, que podrá ser de utilidad para determinar la identificación –con cierto nivel de precisión– de un usuario.

Esta tecnología es de uso cotidiano por distintos portales y servicios web, para identificar a un usuario y observar su comporta-

[42] "Se relanzó la Policía Federal con su nueva función de 'ciberpatrullaje'", *Clarín*, www.clarin.com.

miento en línea, para posteriormente poder "ajustar" el servicio a sus preferencias. Es decir, permitiría identificar a un mismo usuario, aunque el mismo cambiara de dirección IP cada 5 minutos. Hace años que desde la *Electronic Frontier Foundation* (EFF), a través del proyecto Panopticlick[43], advierten sobre los peligros de la utilización de este tipo de técnicas de identificación de usuarios por empresas privadas (uso comercial).

De acuerdo con un estudio realizado por la EFF[44], en los navegadores compatibles con Flash o Java, es posible que en promedio se recolecte al menos 18.8 bits de información de identificación, logrando un porcentaje de exactitud en la identificación del 94,2%.

Categoría de información obtenida: Nivel 0 y 1 – Datos de acceso público y datos de identificación o abonado

Nivel de afectación de derechos: Bajo

6.4. Acceso y análisis de datos identificatorios provistos por CSP

Descripción: Esta medida consiste en el acceso, análisis y procesamiento de datos de personales de un usuario determinado, que permitiría como resultado obtener la identificación de la persona –en principio– detrás del servicio utilizado –o de la conexión a la red–. Remitimos al desarrollo sobre el primer escalón realizado en este trabajo, referente a datos de identificación o de abonado.

A diferencia de otras técnicas de investigación, el acceso a este tipo de información requiere la colaboración y cooperación de la empresa proveedora del servicio (CSP tales como Facebook, Google, o un ISP local, entre otros).

Categoría de información obtenida: Nivel 1 – Datos identificatorios o de abonado

Nivel de afectación de derechos: Bajo

6.5. Acceso y análisis de datos provistos por fuentes cerradas

Descripción: Esta medida consiste en el acceso, análisis y procesamiento de datos (personales o no) de un usuario determinado, a través de la consulta a fuentes cerradas (de acceso restringido), que permitiría obtener la identificación de la persona.

A diferencia de la medida anterior, donde se solicitaba a una empresa los datos identificatorios de un cliente o usuario de un servicio o plataforma (como un servicio de Internet, Facebook, etc.), en este caso la medida está dirigida a otras fuentes de información cerradas, en

[43] *Electronic Frontier Foundation: Panopticlick*. https://panopticlick.eff.org.

[44] ECKERSLEY, Peter, "How Unique Is Your Web Browser?", Electronic Frontier Foundation. https://panopticlick.eff.org.

cuyas bases de datos puede existir información de interés que haga al sujeto investigado determinable (a través del cruzamiento de datos).

Ejemplos de ello serían consultas aportando el rostro de una persona sobre un sistema que permite reconocimiento facial, consultas a un servicio de taxis sobre los domicilios relacionados con un determinado número de teléfono, consultar el tipo y cantidad de medicación consumida por un cliente a un servicio de farmacias, etc.

Categoría de información obtenida: Nivel 1 – Datos identificatorios o de abonado

Nivel de afectación de derechos: Bajo

6.6. Acceso y análisis de datos de tráfico

Descripción: Esta medida consiste en el acceso, análisis y procesamiento de datos de tráfico de una comunicación electrónica, que permitiría como resultado obtener información de interés para una investigación. Entre ellos podrían ser sitios web visitados, personas con las que tuvo más comunicación por chat, en qué momento del día realizaba sus llamadas telefónicas, qué duración tuvieron las llamadas, entre otros datos de interés que pueden obtenerse de un adecuado análisis de esta categoría de datos.

El acceso a los datos de tráfico de una comunicación electrónica podrá ser brindado por la empresa proveedora del servicio de comunicación, o bien podría ser obtenido de forma "artesanal" por las fuerzas de seguridad a partir de la ejecución de técnicas de intevención de comunicaciones electrónicas –adaptadas a este tipo de datos–.

Categoría de información obtenida: Nivel 2 – Datos de tráfico o transaccionales

Nivel de afectación de derechos: Medio – Alto

6.7. Acceso y análisis de comunicaciones electrónicas

Descripción: Esta medida consiste en la clásica intervención de las comunicaciones, que podrá realizarse por intermedio de un proveedor de servicios de comunicación, como una empresa telefónica o ISP, así como de forma directa por las fuerzas de seguridad.

Vale destacar que desde un punto de vista técnico, es posible que las comunicaciones capturadas en la red intervenida se encuentren cifradas –por ejemplo, una llamada por whatsapp–, obstaculizando el acceso a los contenidos de la comunicación en sí (en esos casos solamente habría acceso a datos de tráfico). En el caso de comunicaciones no cifradas (como las llamadas tradicionales), es posible el pleno acceso a los contenidos del mensaje transmitido por la red.

Categoría de información obtenida: Nivel 2 y 3 – Datos de tráfico y de contenido

Nivel de afectación de derechos: Alto

6.8. Agente encubierto informático o digital

Descripción: Esta medida consiste en la utilización, a través de medios electrónicos, de una identidad supuesta para poder entrar en el ámbito de confianza del sujeto investigado, y desde la cuál se busca obtener información de interés para una causa previamente determinada[45].

La justificación de este tipo de medidas, en muchos casos, se relaciona con el nivel de resguardos técnicos que tiene el ciberdelincuente para ocultar su identidad y ubicación, por lo que esta figura puede volverse de importancia para conseguir información de utilidad referente a su identificación, o bien que permita acreditar la comisión de uno o más delitos por el sujeto investigado.

Más allá de los aspectos técnicos sobre el ocultamiento de la identidad, el agente encargado de dicha tarea generalmente utiliza técnicas de "*ingeniería social*"[46] para lograr engañar a la persona investigada y obtener así la información que se necesita para la investigación.

Categoría de información obtenida: Nivel 3 – Datos de contenido

Nivel de afectación de derechos: Alto

6.9. Registro de dispositivos de almacenamiento masivo

Descripción: Esta medida consiste en la autorización, en el marco de un allanamiento a un domicilio (registro domiciliario), para acceder a realizar el registro (acceso a los datos) de los dispositivos de almacenamiento masivos que se encontraren en el lugar.

Es decir, permitiría lo que en la práctica se denomina "recolección de evidencia en caliente", independientemente de la posibilidad de secuestro de los dispositivos, a fin de que dicha recolección (y posterior análisis) se haga en un laboratorio forense.

Puede ser una medida de utilizada para casos en que, por la volatilidad de la evidencia digital, al momento del allanamiento el agente de seguridad se encuentre con una oportunidad única en relación a la obtención de información de interés para la causa (por ejemplo, porque de secuestrarse los dispositivos estos se encontraran cifrados, o bien el equipo encendido permitiera el acceso a información en la nube).

Categoría de información obtenida: Nivel 3 – Datos de contenido

Nivel de afectación de derechos: Alto

[45] TEMPERINI, Marcelo - MACEDO, Maximiliano, "Nuevas herramientas para la investigación penal: El agente encubierto digital", *Cibercrimen*, Daniela Dupuy ed., BdeF, Montevideo-Buenos Aires, 2017.

[46] ANDERSON, Ross, *Security engineering: a guide to building dependable distributed systems*, Wiley, New York, 2008.

6.10. Registro remoto sobre equipos informáticos

Descripción: Esta medida consiste en la utilización de datos de identificación (credenciales), así como en la instalación de software especializado, que permita de forma remota y telemática el examen a distancia y sin conocimiento de su titular del contenido de un sistema informático.

De todas las medidas y técnicas de investigación tecnológica, probablemente esta sea la más agresiva y peligrosa, por lo que en muchos países [47] su regulación aún se encuentra en debate.

La justificación de una medida de este nivel de injerencia puede estar fundada en motivos similares a los citados para el registro de dispositivos de almacenamiento masivo.

Categoría de información obtenida: Nivel 3 – Datos de contenido

Nivel de afectación de derechos: Alto

A modo de resumen del listado realizado, acompañamos la siguiente tabla con la enumeración de las medidas y técnicas de investigación tecnológica, organizadas de acuerdo al nivel de afectación de derechos.

Nº	**Medida o técnica de investigación tecnológica**	**Tipo de información obtenida**	**Nivel de afectación de los derechos**
1	Inteligencia de fuentes abiertas (OSINT)	Nivel 0	Nulo
2	Ciberpatrullaje	Nivel 0	Nulo
3	Identificación por huella digital del navegador (*browser fingerprinting*)	Niveles 0 y 1	Bajo
4	Acceso y análisis de datos identificatorios provistos por CSP	Nivel 1	Bajo
5	Acceso y análisis de datos provistos por fuentes cerradas	Nivel 1	Bajo
6	Acceso y análisis de datos de tráfico	Nivel 2	Medio - Alto
7	Acceso y análisis de comunicaciones electrónicas	Niveles 2 y 3	Alto

[47] "¿Se viene el 'troyano judicial'?", *Diario Judicial*, www.diariojudicial.com.

8	Agente encubierto informático o digital	Nivel 3	Alto
9	Registro de dispositivos de almacenamiento masivo	Nivel 3	Alto
10	Registro remoto sobre equipos informáticos	Nivel 3	Alto

7. CONCLUSIONES

Queda de manifiesto que la evolución de los ciberdelincuentes hace necesaria una rápida y ágil adaptación de las formas de investigación utilizadas por las fuerzas de seguridad encargadas de la identificación y persecución de los ciberdelincuentes.

Como hemos observado a lo largo de este trabajo, la mayoría de las medidas y técnicas de investigación tecnológica afectan en mayor o menor medida derechos y garantías consagrados constitucionalmente.

Consideramos de importancia destacar la peligrosidad de permanecer en un sistemas penal con nula o escasa regulación sobre las medidas de investigación a través de la tecnología informática, donde a través de una exagerada y abusiva flexibilización del principio de la "libertad probatoria" se justifica la incorporación de elementos de evidencia digital sin que los mismos sean constrastados por un mínimo de controles y principios en resguardo de los derechos del sujeto investigado.

Nuestra postura adhiere a la de otros autores con respecto a la necesidad de visibilizar y avanzar sobre una adecuada regulación del aspecto procesal penal, que establezca una adecuada regulación de los medios de prueba adaptados al escenario digital o electrónico, que permitan a los funcionarios a cargo de la investigación contar con una adecuada "carta" de opciones al momento de solicitar una medida.

En segundo lugar, y no por eso menos importante, cabe destacar la necesidad de regulación, con el mayor nivel de detalle y minuciosidad posible, de los requisitos jurídicos necesarios para solicitar cada una de las medidas probatorias, así como los límites técnicos y jurídicos que deberán observarse al momento de su ejecución.