Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

Equilibrio entre el derecho a la intimidad y el poder investigativo del Estado en la era digital

Jesica Bernard*

Resumen

Los sistemas de administración de justicia imperiosamente han tenido que actualizar las estructuras existentes e implementar las nuevas herramientas provenientes de las tecnologías de la información y las comunicaciones. La incidencia que pueden tener en las investigaciones penales ha puesto en debate las diversas medidas intromisivas que se proponen en relación a la esfera privada de los ciudadanos. Los organismos encargados de la persecución penal han ampliado los horizontes de búsqueda de información por el acceso a nuevas bases de datos, plataformas y sistemas digitalizados. ¿Hasta dónde es legítimo avanzar en la búsqueda de evidencias criminales, sin lesionar derechos o garantías de la persona investigada, sin violar su privacidad? Se pretende responder a este y otros interrogantes, abordando la problemática en un marco de intereses contrapuestos: la persecución penal estatal y el derecho a la intimidad de los ciudadanos.

Palabras claves: Eficacia punitiva – Garantías constitucionales – Derecho a la intimidad – Evidencias digitales – Valoración probatoria

* Abogada y Especialista en Derecho Procesal Penal por la Universidad Nacional del Litoral, Diplomada en Cibercrimen y evidencia digital por la Universidad Champagnat.

DR © 2021. Universidad de Palermo-Facultad de Derecho
https://www.palermo.edu/derecho/publicaciones/revista_juridica/

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

I. Introducción

Apenas recorridas las primeras décadas del siglo XXI se advierte que la ola de innovación tecnológica es imparable, produciéndose avances a gran escala y en la más variada amplitud de espacios, comprendiendo tanto la ciencia y la medicina, como la política, la economía, el derecho, surgiendo de esta manera nuevos intereses, identidades, espacios personales que son –o deberían ser- amparados por la ley.

Indudablemente, la era digital aporta numerosos beneficios permitiendo a los usuarios experimentar nuevas formas de vincularse socialmente, ofreciéndoles herramientas a las que pueden acceder desde una computadora, un smartphone o cualquier dispositivo que pueda tener una conexión a internet. Toda la actividad que los mismos despliegan deja incontables registros que facilitan la búsqueda y el acceso a los movimientos cibernéticos de quien utilice alguno de los dispositivos referidos.

Para analizar este fenómeno, se optó por comenzar con un análisis de la situación de tensión existente entre las garantías de los ciudadanos y el ejercicio del poder punitivo por parte del Estado, de las características propias del sistema acusatorio, a la luz de la antinomia fundamental del proceso penal que permitirá cohesionar un juego limpio de fuerzas contrapuestas en el marco de las investigaciones penales.

Luego se propone el tratamiento de la normativa constitucional y convencional específica en la materia, como así también se expone el estado actual de las lagunas existentes en la legislación nacional y local que, tal como se expondrá, podría tener una incidencia negativa en el despliegue de ciertas medidas investigativas usadas frecuentemente, a los fines de identificar los modos de producción, su valoración judicial y las posibles vulneraciones que se puedan generar a partir de los incumplimientos de normas establecidas al respecto.

II. Rol del acusador público en el marco de la antinomia fundamental

Desde su origen, el sistema inquisitivo mantenía una concepción de delito como infracción al Estado, la objetivización de las personas sometidas a persecución penal y su correlato en la ausencia de una perspectiva humanitaria que garantice sus derechos, en la criminalización de personas por culpa de un derecho penal de autor que solo buscaba culpables, sirviéndose de torturas para obtener sus confesiones y así poder aplicar castigos. Asimismo, el escriturismo y el secreto de las actuaciones, la persecución y juzgamiento a cargo de un inquisidor -funcionario con delegación de poder estatal- cuya clara parcialidad impedía juzgar a una persona libre de prejuicios, conocimientos previos y vinculaciones que teñían su juicio al momento de pretender iniciar una búsqueda de la verdad histórica, conducían el proceso hacia el único sentido posible: condenar y castigar a quien fuera sometido

DR © 2021. Universidad de Palermo-Facultad de Derecho
https://www.palermo.edu/derecho/publicaciones/revista_juridica/

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

a investigación por un hecho contrario a la voluntad del soberano.

A partir de la Revolución Francesa hubo una fuerte oposición a tales prácticas inhumanas que condujeron a los Estados a introducir reformas en los sistemas de enjuiciamiento penal. Con la sanción del *Code Criminelle 1808* de Napoleón se produjo un quiebre parcial en la ideología reinante que permitió introducir las nuevas ideas que traía la Revolución. El nuevo sistema fue llamado "mixto" puesto que conservaba las bases del sistema inquisitivo. La persecución penal pública y la averiguación objetiva de la verdad histórica como fin del proceso[1] fueron los principales cimientos sobre los cuales se edificaron las pretendidas reformas. La tarea de investigar el acaecimiento de un hecho real en procura de la verdad de lo sucedido aplicando la ley penal no era optativa, debía continuar hasta obtener un pronunciamiento judicial. Ligado al principio de legalidad se impuso al órgano acusador el principio de objetividad, que lo abstrajo de la búsqueda de intereses subjetivos.

Desde aquel momento se empezó a pensar en la necesidad de imponer límites al poder penal del Estado. Durante el siglo XX se produjeron grandes debates acerca de las reformas necesarias a implementar en los sistemas de administración de justicia, pero manteniendo aún intactas las bases inquisitivas. Ante la secuencia de violencia estatal que golpeó a mitad de aquel siglo a las democracias europeas y latinoamericanas, se desarrolló una normativa humanitaria internacional que rápidamente daría el marco jurídico para la protección de derechos humanos básicos, hasta entonces desconocidos y vulnerados en los procesos penales a cargo de los mismos Estados.

Como sostiene Maier, fueron cada vez más numerosos los esfuerzos político-criminales orientados hacia la racionalización del poder penal estatal, abarcando la regulación de la persecución penal[2], siendo una de las principales características del modelo acusatorio la diferenciación de funciones acusatorias y decisorias en la órbita del poder judicial.

El acusador es quien encabeza la investigación desde su inicio en búsqueda de la verdad material de los hechos, la cual se construye en base a evidencias que acrediten tales extremos. El acusador, en ocasiones solo y en otras en conjunto con la parte querellante, ejerce la acción penal litigando frente a su adversario, llevando a cabo una actividad limitada por los controles de la defensa como por el tribunal.

Es importante subrayar que, tanto la acusación como la defensa se encuentran en un pie de igualdad, cuentan con igualdad de armas y posibilidades de probar, alegar, peticionar al juez. El tribunal, por su parte, asume una postura imparcial, imparcial e independiente de los intereses de las partes. Su rol, "totalmente aséptico

1 Maier, J., *Derecho Procesal Penal*, Tomo I, 1° ed., Buenos Aires, AdHoc, 2016, p. 339.
2 Maier, ob. cit., p. 347.

DR © 2021. Universidad de Palermo-Facultad de Derecho
https://www.palermo.edu/derecho/publicaciones/revista_juridica/

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

y descontaminado de todo interés de parte"[3] se circunscribe a controlar el respeto de la legalidad de la investigación y resolver conforme a las pruebas aportadas por las partes en orden a alcanzar un grado de certeza acerca del desarrollo de los hechos sometidos a su consideración.

En cuanto al ejercicio de la acción, el acusador público lo hace de manera oficial y oficiosa[4] en relación a los delitos de acción pública del art. 71 del digesto penal. A su vez, en el Código Procesal Penal de Santa Fe se regula tal procedimiento en el art. 16, estableciéndose que puede actuar de oficio siempre que no dependa de instancia privada, y que tal promoción de la acción será obligatoria respecto a los hechos punibles que lleguen a su conocimiento y sobre los cuales se tenga indicios de su existencia. Tal como lo explican Baclini y Schiappa Pietra:

> [e]l artículo dispone lo que se conoce como el principio de legalidad procesal. Este es el principio rector en la regulación de la acción penal pública y por el cual se obliga al órgano a cargo de la persecución penal a promover la acción penal…

Se dispone una facultad en el ejercicio de la acción, cual es la posibilidad de aplicación de criterios de oportunidad, siempre en el marco de la legalidad dispuesta por la norma como principio rector[5].

En relación a la carga probatoria, estos autores refieren que "quien tiene la carga de la prueba es el Estado, la actividad de probar un hecho tiene su razón de ser cuando se haya constatado una oposición de la Defensa y del imputado sobre la acusación fiscal"[6].

En torno al rol asignado, Mendaña en palabras de González Álvarez, refiere que ello no implica un simple cambio de actores puesto que "No se trata de que los fiscales hagan lo mismo que antes hacían los jueces; se trata de que investiguen de una manera distinta" y en palabras propias, el autor recuerda que

> [l]a investigación de los modelos inquisitivos es una actividad lineal, ritualista, rígida y muy formalizada, todo lo cual impide obtener mayores niveles de eficiencia, lo que se traduce, entre otras cosas, en un alargamiento del tiempo de duración de los sumarios y en un nivel importante de vulneración de derechos de los involucrados[7].

---

[3] Jauchen, E., *Tratado de Derecho Procesal Penal*, Tomo I, Santa Fe, Rubinzal-Culzoni, 2013, p. 76.

[4] Idem. El autor entiende que es consecuencia del carácter oficial del ejercicio de la acción, y que por tal motivo puede promover sin necesidad de excitación de ningún poder extraño. Al tener carácter público, no resulta vinculante el interés del particular para que impulse la acción.

[5] Baclini, J. y Schiappa Pietra, L., *Código Procesal Penal de Santa Fe comentado, anotado y concordado*, Tomo 1, Juris online, Rosario, 2017, p. 74.

[6] Idem, p. 323.

[7] González Álvarez, D., "La Investigación preparatoria del Ministerio Público en el nuevo proceso penal costarricense", en *Revista Pena y Estado*, n° 2, p. 87, cit. por Mendaña, R., "El ministerio

DR © 2021. Universidad de Palermo-Facultad de Derecho
https://www.palermo.edu/derecho/publicaciones/revista_juridica/

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

Por el contrario, en el sistema acusatorio quien debe probar es el fiscal y su tarea será investigar y reunir la mayor cantidad de evidencias que permitan destruir el estado de inocencia del que está investido todo imputado y acreditar su culpabilidad[8] por el hecho mediante la obtención de una sentencia condenatoria.

En relación a la antinomia fundamental referida en el título del presente capítulo, es un concepto tomado de la obra de Alberto Binder[9] que resulta de suma utilidad para pensar este juego de intereses contrapuestos que se expone, existente tanto en la base del derecho procesal penal como en todas las instituciones que lo componen. Consiste en la contraposición esencial y básica entre la búsqueda de eficacia del poder punitivo del Estado y los límites que se le imponen en defensa de las libertades de los ciudadanos. El choque de ambas fuerzas se produce como una contradicción fundamental que es característica de los sistemas adversariales, donde existen tensiones entre los distintos intereses involucrados, el de castigar y reprimir los delitos y el de defenderse de acusaciones injustificadas y persecuciones infundadas.

Binder propone que los diversos institutos procesales contemplados en la normativa de forma sean analizados a la luz de tales tensiones: una misma norma puede contemplar cierta medida investigativa que pueda regular su procedencia, en respeto de determinados límites, frenos e imponga restricciones formales que no puedan ser traspasadas sin vulnerar derechos de quienes resulten afectados por las mismas. Tal evaluación debe ser llevada a cabo por parte del tribunal interviniente, que resuelve en uno u otro sentido dependiendo del contexto y de las características del caso concreto.

El referido autor considera que la contradicción de fuerzas es necesaria por ser el proceso penal el cauce ineludible para aplicar una pena. De manera coincidente, Jauchen entiende que "se tutelan simultáneamente dos intereses, el de la sociedad que quiere la justa represión del verdadero culpable y al mismo tiempo la exoneración del inocente, y el interés individual por la libertad y la dignidad del hombre" [10].

En cuanto a la eficacia, Binder entiende dicha fuerza concreta el programa punitivo estatal con el fin de absorber la violencia social (mediante el monopolio de la fuerza pública)[11], controlar la criminalidad y lograr la paz social. Impulsa

público y la dirección de la investigación criminal", en *Cuadernos de Derecho Penal*, p. 231.

[8] Maier, J., ob. cit., p. 473, plantea que es una necesidad del proceso afirmar la certeza de la existencia de un hecho, y la prueba de la inocencia no le corresponde al imputado sino al acusador. La regla in dubio pro reo exige que, si no están acreditados los elementos para afirmar la comisión de un hecho, no se destruye de manera cierta la inocencia, el resultado será la absolución porque él se encuentra amparado por una presunción constitucional.

[9] Binder, A., *Derecho Procesal Penal*, Tomo I, Buenos Aires, AdHoc, 2013, pp. 99 y ss.

[10] Jauchen, E., ob. cit., p. 422.

[11] En idéntico sentido Maier, J., ob. cit., p. 442, sostiene que "a la venganza privada (…) le sucede lo que modernamente se conoce por acción procesal o en nuestra materia, persecución penal, ejercida en un primer momento por el ofendido (…) y tiempo después, por el Estado, que expropió ese poder de manos del individuo y monopolizó el poder penal".

DR © 2021. Universidad de Palermo-Facultad de Derecho
https://www.palermo.edu/derecho/publicaciones/revista_juridica/

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

la realización del poder punitivo, busca que no haya impunidad, representando intereses sociales que reclaman seguridad, justicia y cumplimiento de la ley. Este programa punitivo es encabezado por el ministerio público acusador, ente autónomo interrelacionado con las demás autoridades estatales (gestiona intereses generales de la sociedad y de las víctimas en particular pero no es abogado particular de ellas), con el fin de aplicar la ley penal del Estado a los ciudadanos que incurren en transgresiones a la misma[12]. Este poder se encuentra contenido en su avance por el núcleo de garantías del ciudadano, que todo Estado Constitucional de Derecho posee en su favor, y que intentará reducirlo.

En ese sentido, "las garantías" están orientadas a fortalecer los límites al poder penal, a la política criminal. Fueron creadas para proteger a los ciudadanos de las lesiones que pueda ocasionar la política dirigida por el aparato estatal con toda su fuerza y vigor, Binder las define como "el escudo protector del ciudadano frente al poder penal". Representan obstáculos que el Estado debe sortear, frente a los cuales deberá oponer fundamentos válidos y suficientes para su relevamiento, cuando sea necesario priorizar la tutela de un interés de mayor jerarquía en el caso concreto. En ese sentido, "protegen porque tornan más difícil la aplicación de ese poder penal", que no puede actuar arbitrariamente. Se encuentran plasmadas en la Constitución Nacional y los Tratados Internacionales sobre Derechos Humanos, en constituciones y códigos procesales provinciales.

Por su parte, el sistema penal consagra las garantías mediante las formas procesales, que facilitan el cumplimiento y el respeto de un principio determinado[13]. Un ejemplo de ello es lo establecido por el art. 18 de la CN en cuanto a la inviolabilidad de la correspondencia epistolar y los papeles privados, permite preservar el ámbito de intimidad de los ciudadanos[14] en sus comunicaciones, excluyendo intromisiones ajenas injustificadas.

Ambas fuerzas se controlan en un punto de equilibrio -no se suman ni se unen- que no es duradero y que no se produce de la misma manera en todos los casos sino que es inestable porque los planteos de las mismas a lo largo de todo el proceso propician un flujo continuo de intereses que en determinados momentos prevalecen unos sobre otros. Cuando gestionan sus intereses mediante pedidos de autorización

[12] Binder, A., *Derecho Procesal Penal,* Tomo II, Buenos Aires, AdHoc, 2014.

[13] Maier, J., ob. cit., pp. 441-442.

[14] Intimidad como una especie dentro del género privacidad, esta última consiste en el derecho de toda persona a que se proteja su ámbito de reserva sin que sea conocido por terceros, lo que no necesariamente implica que todo lo privado sea íntimo. En idéntico sentido, Baladán F. y Hernández Varela, J., "Intimidad y privacidad frente a las intervenciones de las comunicaciones electrónicas", *16° Simposio Argentino de Informática y Derecho*, 45 JAIIO - SID 2016, p. 118, disponible online en http://sedici.unlp.edu.ar/bitstream/handle/10915/58263/Documento_completo.pdf-PDFA.pdf?sequence=1.

DR © 2021. Universidad de Palermo-Facultad de Derecho
https://www.palermo.edu/derecho/publicaciones/revista_juridica/

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

judicial -ej. interceptación de las comunicaciones, exclusión de puntos de pericia informática por ser impertinentes- exponen sus fundamentos en base a los cuales el tribunal analizará y decidirá la procedencia o no de las medidas (otorgándolas en su totalidad o solo en parte. Es decir, el tribunal dinamiza las controversias que se produzcan entre las partes. Para Maier ello se explica en el marco de la coerción procesal que aplica el Estado en una investigación puesto que

> [l]a coerción procesal es aplicación de la fuerza pública que coarta libertades reconocidas por el orden jurídico, cuya finalidad reside […] en el resguardo de los fines que persigue el mismo procedimiento, averiguar la verdad y actuar la ley sustantiva, o en la prevención inmediata sobre el hecho concreto que constituye el objeto del procedimiento.

Consecuentemente, las medidas de coerción se aplican para llevar a cabo de manera exitosa la actividad probatoria acerca de un hecho, posibilitando el resguardo de la información, los testigos, las evidencias de que se trate en el supuesto fáctico concreto.

Un ejemplo de derecho afectado por los medios de coerción procesal es la apertura o inspección de correspondencia y papeles privados, que en concreto afecta la intimidad de la correspondencia y documentación personal (según el citado art. 18 CN). Maier aclara en este punto que la cosa no es el objeto de la coerción, sí lo es la relación que la persona tiene con ella, privándolo en ese caso de su libre disposición y uso[15].

En efecto, el citado autor entiende que la regulación del derecho a la intimidad en la Carta Magna implica

> [l]a posibilidad de exclusión de terceros de ciertos ámbitos privados, una garantía frente al poder estatal, que reside en prohibir la injerencia de los órganos del Estado, por regla general, y permitirla en los casos y bajo la observancia estricta de las formalidades que la ley prevé al reglamentar racionalmente la garantía.

Ello resulta adaptable a las intervenciones de comunicaciones privadas, al referir que "los medios técnicos que revolucionan hoy las comunicaciones quedan así comprendidos en el derecho a la intimidad"[16].

Ahora bien, el incumplimiento de dichas formalidades y limitaciones legales impuestas en protección de los derechos de los ciudadanos (necesidad de

[15] Maier, J., ob cit., p. 486.

[16] Idem, p. 653. En idéntico sentido Aboso, G., *Derecho Penal Cibernético*, Buenos Aires, BdeF, 2017, p. 143, entiende que es el espacio en el cual la persona tiene garantizada de manera integral su derecho de ejercer un plan de vida determinado con exclusión de la injerencia arbitraria de terceros o del propio Estado.

DR © 2021. Universidad de Palermo-Facultad de Derecho
https://www.palermo.edu/derecho/publicaciones/revista_juridica/

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

autorización judicial, presencia de testigos de procedimiento, filmación, constancias escritas, fotografías, registración y codificación, cadenas de custodia, etc.) puede conducir a que no se admitan determinados elementos de prueba que fueran obtenidos en violación a estas pautas, o bien, si hubieran sido admitidos, a que no sean valorados por el tribunal al momento del dictado de la resolución, auto o sentencia de que se trate.

La prohibición de valoración probatoria tiene como resultado que "la decisión contraria al interés del portador de la garantía no puede ser fundada en elementos de prueba obtenidos mediante su inobservancia o con violación de las formas previstas en resguardo de la garantía"[17]. Significa que no puede ser valorado por el juez aquello que fue obtenido violando formas procesales establecidas para su producción, en consonancia con el principio de que el fin –de obtener la verdad real, objetiva de los hechos- no puede justificar los medios prohibidos[18].

III. Evidencia digital y su regulación a nivel internacional

Debido a los atentados terroristas acaecidos en 2001 en Estados Unidos, las preocupaciones de los Estados europeos por la protección de su seguridad y orden interno se incrementaron notablemente. La facilidad con que se transmiten datos a través de medios digitales o informáticos tanto para fines lícitos como para la comisión de delitos, su carácter transnacional que no reconoce fronteras, la recolección de evidencias digitales ubicadas en distintos países y la falta de normas de cooperación internacional para el abordaje de tales delitos pusieron de manifiesto la necesidad de establecer un marco regulatorio común.

En el año 2001 el Consejo de Europa reunido en Budapest suscribió el Convenio sobre Ciberdelincuencia[19]. En su preámbulo marcó la imperiosidad del respeto por los derechos humanos reconocidos por diversos tratados internacionales, contemplando explícitamente el respeto a la privacidad para todas las personas y la protección de sus datos personales y comunicaciones, exigiendo que haya un "equilibrio adecuado" entre los mismos. En su capítulo II, impone el compromiso de las Partes en adoptar medidas legislativas procesales y aplicarlas a la recopilación de pruebas informáticas en la investigación de un delito (art. 14), velando por la más amplia aplicación.

Dispone que el ejercicio de las facultades concedidas a las Partes y los procedimientos que se regulan en el Convenio no podrán ser aplicados en detrimento en la protección de los derechos humanos y libertades de los ciudadanos. Para ello se establece que según el tipo de medida o procedimiento de que se trate, se deberá

[17] Maier, J., ob cit., p. 655.
[18] Ello remite al análisis de la teoría de los frutos del árbol envenenado (*poisonous tree*).
[19] Convenio sobre la Ciberdelincuencia, disponible online https://rm.coe.int/16802fa403

DR © 2021. Universidad de Palermo-Facultad de Derecho
https://www.palermo.edu/derecho/publicaciones/revista_juridica/

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

contar con autorización judicial, ser motivada, y limitada en cuanto a su alcance y duración, evaluando la posible afectación de intereses legítimos de terceros. Ello significa permitir la intromisión estatal en la esfera de los derechos y libertades en cuanto manifieste un interés concreto y razonable.

Regula la conservación de datos informáticos almacenados en sistemas informáticos y la divulgación parcial de datos de tráfico para permitir su rápida conservación (*quick freeze*), imponiendo a la entidad que conserva dicha información el deber de preservar y mantener la integridad de los datos bajo confidencialidad, en el plazo que se establezca. Respecto a los datos de tráfico, se propone su conservación para garantizar su rápida divulgación a la autoridad interviniente que intente identificar proveedores de servicios y la ruta que se siguió en una determinada comunicación. El problema que se plantea en este punto está vinculado a la discrecionalidad con que se pueden servir los Estados de esa información, que puede ser utilizada en una o más investigaciones, situación agravada por la falta de regulación al respecto en muchos países.

Contempla la garantía de acceso a sistemas informáticos y datos almacenados por cada Estado parte, pudiendo tomar medidas específicas para proteger los datos informáticos de interés (disponiendo su incautación o aseguramiento, copia). Lo dispuesto supone una libertad de actuación para disponer de información privada que queda a merced de lo que las autoridades estatales dispongan, sin vislumbrarse limitaciones específicas en el tiempo, cantidad de información y la conservación o eliminación de tales datos.

Posteriormente trata la recopilación de datos informáticos en tiempo real -de tráfico- vinculados a comunicaciones que se hayan producido en su territorio asegurando en todos los casos la confidencialidad del procedimiento. Si se tratara de delitos graves los Estados podrán permitir que sus autoridades recopilen o registren datos de contenido en tiempo real.

Es posible afirmar que se otorgan amplias facultades a los Estados en el marco de sus investigaciones a fin de garantizar la eficacia en la recopilación de datos a nivel interno y transfronterizo, asegurada por la obligación de conservarlos, entregarlos cuando sean solicitados y mantener la confidencialidad en dichos pedidos.

Al respecto cabe formular algunas precisiones. Tal como sostiene Ferreyra, estas medidas "tienen el potencial de afectar gravemente la privacidad de las personas, ya que implica que una gran cantidad de información personal estará a disposición de las autoridades y las fuerzas de seguridad"[20]. Se habilita a los Estados

[20] Ferreyra, E. "La Convención de cibercrimen de Budapest y América Latina. Breve guía acerca de su impacto en los derechos y garantías de las personas", *Asociación por los Derechos Civiles*, marzo 2018. Disponible en https://adc.org.ar/wp-content/uploads/2019/06/035-la-convencion-de-cibercrimen-de-budapest-y-america-latina-vol-1-03-2018.pdf

DR © 2021. Universidad de Palermo-Facultad de Derecho
https://www.palermo.edu/derecho/publicaciones/revista_juridica/

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

a la intromisión en las comunicaciones individuales y deja librado a su criterio la ampliación de las solicitudes, los datos que se recolectan.

Se advierte que, con facilidad, se puede vulnerar la privacidad de las personas investigadas si se realizan pedidos de información indiscriminados, en base a sospechas fundadas en datos sensibles como orientación política, religión, raza, etc., que podrían conducir incluso a prácticas que atenten contra el derecho a la igualdad y el ámbito de reserva de cada ciudadano.

Por otra parte, cabe tener en cuenta que en el proceso penal uno de los criterios para la producción de la prueba es su pertinencia respecto al hecho. La mayoría de las evidencias que se obtienen de medios informáticos tienen alto nivel de injerencia en la personalidad, por ende, deben ser autorizadas en aquellos casos en que se justifique tal intromisión.

En Argentina mediante Ley 27.411 se ratificó el Convenio y se formularon reservas a algunas de sus cláusulas vinculadas a delitos informáticos, a cuestiones de jurisdicción, entre otras.

Por otro lado, en el año 2013 en el ámbito de la Asamblea General de Naciones Unidas se emitió la Resolución N° 68/167 acerca del derecho a la privacidad en la era digital, indicando que nadie será objeto de injerencias arbitrarias e ilícitas en este ámbito[21]. Reconoce que Internet posee una naturaleza "global y abierta", que el avance de las TIC ha generado un efecto positivo hacia el desarrollo en diversas formas y afirmando que los derechos de las personas "también tienen que estar protegidos en Internet". Es una regulación de mayor especificidad que impone límites más nítidos que lo expuesto hasta el momento, que permite llevar a cabo la tarea del Estado dentro de un marco legal y protectorio de derechos de los ciudadanos.

En cuanto a regulaciones específicas europeas, son dables de mencionar las establecidas por España y Alemania. En el derecho español, la Legislación de Enjuiciamiento Criminal[22] se caracteriza por la precisión y el tratamiento detallado de las evidencias que sean recolectadas en medios informáticos: 1) interceptación de comunicaciones telefónicas y telemáticas (para delitos dolosos con determinada pena cometidos en el marco de organización criminal, terrorismo o mediante instrumentos informáticos o de comunicación, de direcciones IP o números de IMEI), 2) la captación y grabación de comunicaciones orales mediante dispositivos electrónicos, 3) el uso de dispositivos de seguimiento, localización y captación de la imagen, 4) el registro de dispositivos de almacenamiento de información y 5) registro remoto sobre equipos informáticos. Asimismo, identifica los principios

[21] Resolución N° 68/167 de 18 de diciembre de 2013, emitida por la A.G. de Naciones Unidas, disponible online https://digitallibrary.un.org/record/764407?ln=es

[22] Ley de Enjuiciamiento Criminal española disponible en https://boe.vlex.es/vid/ley-organica-13-2015-583908674

DR © 2021. Universidad de Palermo-Facultad de Derecho
https://www.palermo.edu/derecho/publicaciones/revista_juridica/

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

rectores que determinan la validez de las medidas mencionadas: vinculadas con un delito concreto (especialidad); circunscriptas a un ámbito objetivo y subjetivo y su duración preestablecida (idoneidad); ser imprescindibles, por no existir otras medidas de menor gravedad e injerencia en los derechos humanos fundamentales (excepcionalidad y necesidad). Por último, el caso del descubrimiento casual y la orden de borrado y eliminación de los registros una vez que el procedimiento fue concluido, asegurando que toda información extraída de pericias informáticas o intervenciones de comunicaciones será eliminada y no podrá ser consultada ni utilizada en ninguna otra ocasión.

Por su parte, el Tribunal Constitucional Federal alemán acuñó la denominación "*derecho a la autodeterminación informativa*" como derivación del derecho a la intimidad, entendiendo que

> El libre desarrollo de la personalidad presupone en las modernas condiciones para el procesamiento de datos, la protección de los individuos frente a la ilimitada recolección, archivo, empleo y retransmisión de sus datos personales […]. Este derecho a la "autodeterminación de la información" no se garantiza ilimitadamente. El individuo no tiene un derecho en el sentido de un señorío ilimitado, absoluto, sobre "sus" datos […] El individuo debe admitir ciertas restricciones a su derecho a la autodeterminación de la información, principalmente en aras del interés general preponderante[23].

Se advierte cómo se imponen limitaciones en orden a la proporcionalidad de la medida procurando un equilibrio entre los intereses generales y los individuales.

Por último, cabe hacer mención de lo previsto en la norma ISO/IEC N° 27037:2012 referida al análisis forense de la prueba digital. Impone tres principios como condiciones previas para los expertos informáticos respecto a la evidencia digital, a saber: 1) relevancia, que la medida sea apta para probar una hipótesis planteada alrededor de los hechos; 2) confiabilidad, a fin de lograr la repetibilidad y la auditabilidad de las pericias (asegurando que cualquier interesado en revisar el proceso de obtención de los resultados pueda hacerlo repasando todos los pasos hasta llegar a la información obtenida); 3) suficiencia, en relación a que las pruebas informáticas sean completas para fundar tales hallazgos[24].

Como corolario de lo expuesto, el desarrollo internacional alcanzado en la materia bajo análisis permite indicar un camino hacia una regulación completa y detallada, llenando los vacíos legislativos para evitar las injerencias indebidas en

[23] Tribunal Constitucional Federal Alemán, Sentencia de la Primera Sala –1 BvR 209, 269, 362, 420, 440, 484/83– del 15 de diciembre de 1983, disponible online https://www.kas.de/c/document_library/get_file?uuid=0a66a4a6-1683-a992-ac69-28a29908d6aa&groupId=252038

[24] Norma ISO/IEC N° 27037:2012 , disponible online https://www.iso.org/standard/44381.html.

DR © 2021. Universidad de Palermo-Facultad de Derecho
https://www.palermo.edu/derecho/publicaciones/revista_juridica/

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

ámbitos privados de las comunicaciones por medios informáticos. Ello demuestra, por un lado, cierta complejidad en la producción de evidencia digital que determina la exigencia de constantes actualizaciones de los sistemas de administración de justicia, que deben acompañar las modificaciones tecnológicas que se van generando. En este punto es oportuno resaltar que existe una vinculación entre el derecho a la información almacenada en soportes informáticos, de acceso privado y las medidas investigativas llevadas a cabo por el órgano persecutor en razón de la disputa generada por la búsqueda de la realización del derecho penal en el caso concreto y los límites impuestos por el respeto a la dignidad humana.

Tal como sostiene Aboso, los datos almacenados en medios tecnológicos son alcanzados por la tutela constitucional del derecho a la intimidad y la expectativa que tienen los ciudadanos a su privacidad, en cuyo caso cualquier intrusión arbitraria de las autoridades públicas podrá conducir a la nulidad de toda fuente u objeto de prueba utilizado en contra de quien resulte afectado, siendo imperioso en estos casos la habilitación judicial[25]. Vale decir que, para cualquier medida que se intente llevar a cabo que pueda afectar la intimidad del encartado se deberá contar con la venia judicial, una evaluación del caso concreto a la luz del principio de razonabilidad, la pertinencia y necesariedad.

El derecho a la privacidad personal origina un deber de dos caras para el Estado: por un lado, de abstenerse de cometer cualquier injerencia arbitraria en el ámbito de la vida personal de los ciudadanos; por el otro, debe actuar de modo proactivo para asegurar el ejercicio razonable de ese derecho"[26].

IV. Regulación procesal local y el problema de las lagunas normativas

En Santa Fe no existe una legislación que contemple de manera acabada las medidas investigativas en entornos digitales. Si bien sería de gran utilidad contar con una regulación actualizada constantemente y que acompañe los avances que se van produciendo en este tema, no hay que perder de vista que las tecnologías avanzan mucho más rápidamente que la legislación.

La existencia de lagunas podría traducirse -en algunos casos- como una vulneración a los derechos a la intimidad y la privacidad de los ciudadanos que entrarían en riesgo cuando nuevas medidas no legisladas se llevan a cabo de manera indiscriminada. Ferrajoli, citado por Binder, ilustra la preocupación sosteniendo que

[25] Aboso, G., ob cit., cita su propio trabajo "La inconstitucionalidad de la requisa y el examen sin autorización judicial de datos personales almacenados en dispositivos celulares de personas detenidas – Breve reseña de los fallos 'Riley vs. California' (2014) y 'United States vs Brima Wurie (2012) de la Corte Suprema de Justicia de los Estados Unidos", *elDial.com*, 31/7/14.

[26] Aboso, G., ob. cit., p. 68.

DR © 2021. Universidad de Palermo-Facultad de Derecho
https://www.palermo.edu/derecho/publicaciones/revista_juridica/

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

> las deficiencias propias del derecho positivo (lagunas) o de justiciabilidad (debilidad del poder judicial) son defectos de hecho del sistema político constitucional que deben ser reparados a través de la obligación constitucional de los órganos correspondientes de dotar cuanto antes a esos derechos de la plenitud de sus garantías primarias y secundarias.

Para evitar, precisamente, que esa inexistencia de normas específicas se traduzca en la escasez de garantías, es conveniente recurrir a la normativa genérica existente en la actualidad, a los principios rectores en materia probatoria y al análisis jurisprudencial en casos concretos.

El artículo 159 del CPPSF refiere al principio de libertad probatoria admitiendo cualquier medio de prueba que refiera, de manera directa o indirecta, al objeto de averiguación. Al respecto, Baclini y Schiappa Pietra sostienen que "el principio de libertad probatoria habilita la posibilidad de recurrir al encuadramiento legal del medio probatorio análogo cuando el que se pretenda utilizar no esté expresamente regulado en la ley[27]".

Ahora bien, cuando se trata de evidencia digital se suele remitir a las normas que regulan la evidencia física haciendo una interpretación amplia de las mismas[28]. A pesar de ello, no es posible soslayar que la evidencia digital posee características propias que ameritan un tratamiento diferenciado.

La única medida que se encuentra legislada, en cumplimiento del mandato constitucional, es la interceptación de correspondencia e intervención de comunicaciones (art. 171)[29], que para su procedencia debe realizarse mediante un pedido fundado al tribual para obtener su autorización.

En función de la citada amplitud probatoria, medidas como la conservación de datos informáticos y la extracción de datos de servidores podrían ser llevadas a cabo mediante solicitud dirigida al tribunal oficiando al prestador de servicios de telecomunicaciones, aportando información completa y suficiente para su procedencia. Tal proceder sería acorde a la manda constitucional de la "orden de autoridad competente".

Sería importante diseñar una regulación específica de las evidencias digitales[30], para que su utilización legítima, incuestionable y eficiente.

---

[27] Baclini, J. y Schiappa Pietra, L., ob. cit. p. 328.

[28] Existe doctrina que se opone a la aplicación analógica de normas en materia de medidas de coerción. Vázquez Rossi, J., *Derecho Procesal Penal*, Tomo II, Santa Fe, Rubinzal-Culzoni, 1997, p. 242, sostiene que las medidas de coerción, al estar previstas de manera expresa en el ordenamiento procesal, no pueden aplicarse fuera de los límites legales.

[29] En el ámbito del Ministerio Público de la Acusación de Santa Fe existe la Res. FG N° 470/17 que establece una Guía de actuación sobre intervención de comunicaciones, contempla diversas medidas a los fines de obtener datos de abonado, tráfico y contenido.

[30] Muchas provincias de nuestro país han generado protocolos de actuación al respecto (Mendoza, Buenos Aires, Corrientes, Neuquén Río Negro y CABA).

DR © 2021. Universidad de Palermo-Facultad de Derecho
https://www.palermo.edu/derecho/publicaciones/revista_juridica/

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

V. Diferentes medidas investigativas y sus alcances

Por evidencia se entiende todo aquel dato o elemento recolectado por las partes durante la etapa de investigación que permita acreditar las proposiciones fácticas que forman parte de la teoría del caso elaborada en torno al hecho delictivo que se investiga, sea de consistencia física o no, que pueda ser utilizado para fundar una atribución imputativa de un delito, una eventual acusación que conduzca a juicio.

La evidencia digital presenta caracteres propios: es intangible (no tiene consistencia corporal, para su obtención, análisis, visualización y reproducción es imprescindible la utilización de un soporte electrónico físico); su contenido está compuesto por diversos códigos que permiten su identificación en el medio digital y determinan su existencia y veracidad (ej. código hash); es relativamente más vulnerable[31] (es imprescindible recurrir a técnicas para su preservación y resguardo hasta tanto sea extraída); está constituida por los datos e información que se almacenan, transmiten o reciben en un dispositivo informático. Es entendida como prueba informática[32] por alguna doctrina.

Delbono [33] sostiene que evidencia digital es un elemento resguardado en un medio digital como una computadora, que contiene un disco rígido interno, permite almacenar evidencias de la más variada índole (ej. cookies, archivos ocultos, historial de navegación, *spool* de impresión, archivos temporales, etc.), un dispositivo con control de acceso, cuyo recurso material puede ser un pen drive o una tarjeta de proximidad o de datos biométricos, que contiene datos identificatorios del usuario, niveles de acceso y permisos, configuraciones, una tarjeta de memoria, que puede contener imágenes, documentos, fotos, programas o aplicaciones, un celular, cuya memoria interna o tarjeta de memoria permite al usuario conservar fotografías, correos electrónicos, videos, notas de voz, servicio de mensajería.

A continuación, se mencionarán algunas medidas que son utilizadas en la actualidad por los organismos estatales en el marco de las investigaciones.

[31] Logrando acceder de forma remota a una computadora o teléfono celular desde una cuenta de usuario –ej. Google- se puede borrar evidencia digital de relevancia para una investigación, de manera irreversible, perdiéndose toda la información de utilidad.

[32] Es la postura que sostiene Sain, Gustavo, "La estrategia gubernamental frente al cibercrimen: la importancia de las políticas preventivas más allá de la solución penal", en *Cibercrimen y delitos informáticos*, Parada, R. (coord.), Buenos Aires, Erreius, 2018, p. 15, se reproduce como cita, pero se sostiene la necesidad de separar los conceptos por las razones expuestas.

[33] Delbono, P., "Investigación Forense sobre medios digitales", en *Cibercrimen y delitos informáticos*, Parada, R. (coord..), Buenos Aires, Erreius, 2018, p. 160.

DR © 2021. Universidad de Palermo-Facultad de Derecho
https://www.palermo.edu/derecho/publicaciones/revista_juridica/

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

1. Obtención de direcciones IP

La dirección IP es un conjunto de números decimales que identifican la interfaz de un dispositivo dentro de una red que utilice el Protocolo IP (*Internet Protocol*). Sirve para que la información circule en la red, ya sea de manera estática (IP única e inmutable) y de forma dinámica (cambia al reconectarse). Un proveedor de acceso a Internet que tiene un contrato con un abonado a Internet normalmente mantiene ficheros históricos con la dirección IP (fija y dinámica) asignadas, el nro. de identificación de cada suscriptor, la fecha, hora, y duración de la asignación de dirección; al igual que las compañías telefónicas que también conservan esta información[34].

En el marco de una investigación obtener la dirección IP puede configurar un indicio útil estableciendo personas potencialmente identificables. Sin embargo, tal tarea se puede ver frustrada por la utilización de sistemas que impiden la identificación de la dirección IP (ej. la red TOR), evitando su detección mediante una conexión cifrada y segura. No obstante, existen técnicas para trazar el tráfico de información que se genera desde una determinada conexión[35].

2. Dispositivos para geolocalizar personas y comunicaciones

La utilización de GPS[36] o antenas utilizadas por el dispositivo informático, permiten dar con la ubicación concreta de una persona en tiempo real, o diferido, o bien con lugares que frecuenta. Joyanes Aguilar sostiene que "el seguimiento electrónico de los movimientos de un sospechoso mediante el uso de artefactos, dispositivos o simplemente satélites hace posible conocer los movimientos habituales de una persona, establecer sus relaciones sociales y preferencias religiosas o políticas

[34] Hay dos tipos de conexiones a internet: mediante dirección de IP pública (un único dispositivo conectado a Internet tiene una dirección IP pública diferente al resto de los demás dispositivos conectados a Internet en todo el mundo para ese momento determinado. Cuando ese dispositivo se desconecta de internet, la dirección IP pública puede ser liberada y usada por otro dispositivo que necesite realizar una conexión a Internet) y dirección IP privada (se usa para identificar equipos o dispositivos dentro de una red doméstica o privada, son usadas en redes que no sean la propia Internet y utilicen su mismo protocolo).

[35] La ventaja de este tipo de red es la protección a la intimidad, garantiza a los usuarios no dejar huellas de su conexión puesto que TOR no revela las ubicaciones exactas. En 2016 hubo un caso en Buenos Aires de una persona, Iván Barrera Oro, usuario de la red Tor y nodo de salida, en 2013 alguien utilizó su nodo para distribuir pornografía infantil y por tal motivo Barrera fue allanado, detenido y acusado de poseer dicho material, hasta que se comprobó que el usuario era otra persona que se había servido de su nodo para cometer el delito.

[36] Los GPS son sistemas de posicionamiento mediante vía satelital, ofrecen información tridimensional sobre un objeto posicionado, nombre de calles o la demarcación de algún recorrido mediante el uso de mapas en 2 o 3 dimensiones.

DR © 2021. Universidad de Palermo-Facultad de Derecho
https://www.palermo.edu/derecho/publicaciones/revista_juridica/

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

mediante la infiltración a distancia en su computadora personal"[37].

3. Videovigilancia electrónica, reconocimiento facial

Las filmaciones y grabaciones en espacios públicos y privados están reguladas por la Disposición N° 10/2015 de la Dirección Nacional de Protección de Datos Personales, en el ámbito del Ministerio de Justicia y Derechos Humanos de la Nación, la cual establece que, conforme a lo dispuesto por la Ley 25326 una imagen o registro fílmico es considerado un dato personal en tanto permite identificar a una persona y, al estar digitalizada, facilitar su búsqueda. Por ese motivo, la procedencia de las medidas desplegadas por cuestiones de seguridad pública está supeditada al cumplimiento de condiciones como el consentimiento previo e informado del titular del dato a través de carteles que indiquen la existencia de cámaras, la finalidad con la que se registran. Es interesante la limitación que impone al Estado, al disponer que la información deberá ser adecuada, pertinente y no excesiva en relación a la finalidad para la que se obtuvo. El objetivo es salvar el derecho a la privacidad, evitando intromisiones en la intimidad de las personas.

Otra medida que actualmente se implementa en el marco de investigaciones penales es la utilización de *sistemas aéreos no tripulados* en tareas de inteligencia, como *drones*, que pueden contener cámaras de alta resolución para capturar imágenes y videos en tiempo real, realizar reconocimiento facial, referencias en terreno (rastros, ubicaciones, predios urbanizados o rurales), cámaras infrarrojas o térmicas para identificar objetos o puntos a partir de calor, lectores de patentes de vehículos terrestres, geolocalización de teléfonos celulares, determinación de ubicación geográfica por GPS, análisis de vulnerabilidades de una red *Wi-Fi* para ingresar a la misma e identificar los dispositivos conectados[38].

Los drones, por sus características físicas, tienen la capacidad de servir en tareas subrepticias, permitiendo a los usuarios observar movimientos de individuos. Captan imágenes, videos y sonidos para su procesamiento y almacenamiento de todo lo que se encuentre dentro de su rango operativo[39].

En cuanto al reconocimiento facial, la Resolución N° 398/19 del Ministerio de Justicia y Seguridad de Buenos Aires creó un Sistema de reconocimiento facial

[37] Joyanes Aguilar, L., "Introducción. Estado del arte de la ciberseguridad", en *Revista Pensamiento Penal*, disponible online http://www.pensamientopenal.com.ar/system/files/2015/01/doctrina38717.pdf, p. 23.

[38] Información extraída del documento titulado "Alto en el cielo. exploración sobre tecnologías de vigilancia aérea en Argentina", *Área Digital de la Asociación de Derechos Civiles de Argentina,* disponible online https://adc.org.ar/wp-content/uploads/2019/06/033-alto-en-el-cielo-12-2017.pdf

[39] La disposición 20/15 de la Dirección Nacional de Protección de Datos Personales regula la materia, disponible online http://www.jus.gob.ar/media/2898655/disp_2015_20.pdf

DR © 2021. Universidad de Palermo-Facultad de Derecho
https://www.palermo.edu/derecho/publicaciones/revista_juridica/

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

de prófugos que se sirve de información obtenida de cámaras de videovigilancia instaladas en diferentes puntos de la ciudad y que permiten escanear los rostros arrojando una identificación de cada una de las personas[40]. El riesgo que presenta este tipo de medida en primer lugar es el margen de error, que puede conducir a detenciones ilegales, afectaciones mayores a la privacidad, generando un temor a ser perseguido e identificado injustificadamente.

4. Allanamiento remoto

Consiste en el registro de dispositivos informáticos mediante la instalación de un software (es un malware, o también denominado "troyano judicial") que permite examinar a distancia los datos informáticos que los mismos contienen. Es una medida innovadora en la materia que aún no ha sido implementada en Argentina, no obstante, existen algunos proyectos de ley que impulsan su aprobación a nivel provincial, imponiendo como requisito la autorización judicial y limitando su utilización para casos en que la vida o integridad física o sexual de una persona estén en grave peligro. Su aplicación debe ser cautelosa puesto que habilita el acceso a incontable cantidad de información personal, incluyendo información que no corresponda a lo que se está buscando. Contar con una regulación permitiría restringir la cantidad y el tipo de información a recolectar, que sea vinculada a la investigación en el marco de la cual se lleva a cabo la medida.

5. Agente encubierto digital

Agente encubierto, tal como lo define la Ley de Delitos Complejos 27.319 que actúa como un testigo o persona civil, pero con la diferencia de que la identidad que muestre en Internet no podrá revelar su pertenencia a una fuerza de seguridad. Esta actuación excluye la provocación o inducción al delito[41].

[40] Solicitud de información pública presentada por la *Asociación de Derechos Civiles* "Con mi cara no", disponible en https://adc.org.ar/2019/05/23/con-mi-cara-no-reconocimiento-facial-en-la-ciudad-de-buenos-aires/

[41] A nivel internacional, está regulado por la LECrim Española, circunscribe su ámbito a la delincuencia organizada.

DR © 2021. Universidad de Palermo-Facultad de Derecho
https://www.palermo.edu/derecho/publicaciones/revista_juridica/

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

6. Pericias de dispositivos electrónicos

Consiste en la búsqueda, recolección[42], extracción y análisis de datos informáticos contenidos en dispositivos electrónicos físicos.

Acerca de la recolección de información existen determinados requisitos de procedencia regulados en la normativa procesal local: debe estar fundada en base a la evidencia que se intenta obtener, detallar los puntos de pericia y el contenido específico a buscar[43]. Desde el momento del secuestro del dispositivo informático el procedimiento debe estar registrado para su posterior auditabilidad y verificación como así también para la reproducción ante los tribunales, en el eventual supuesto que se deba acreditar el contenido de la pericia en un juicio.

La pericia informática arroja información obtenida de dispositivos y se plasma en un informe que presenta características propias[44], que lo diferencian de una evidencia documental clásica precisamente por su soporte.

La preservación de los medios debe realizarse mediante cadena de custodia[45], con ciertas condiciones de guardado que impidan vulnerar los equipos. En cuanto a la información relevada corresponde distinguir el tipo de datos de que se trate, el lugar del que fueron extraídos (dispositivo, programa, nube) o si son volátiles.

La información que se puede obtener es variada, comprende desde el historial de ubicaciones y direcciones, marcadores de navegación de Internet y su historial completo, configuraciones de usuario, contenidos multimedia como fotografías

[42] Darahuge, M. E. y Arellano González, L., *Manual de informática forense II (Prueba indiciaria Informático Forense)*, Buenos Aires, Errepar, 2012, pp. 247 y ss. Existen dos variantes de recolección de datos: lógica, extrae la información almacenada o asignada; física, permite obtener datos que han sido eliminados e información del sistema de archivos, es llevada a cabo mediante un hardware que se conecta al dispositivo o mediante software y obtienen una imagen física de todas las particiones de datos, proveyendo acceso al sistema de archivos y permitiendo una copia completa de todos los archivos lógicos.

[43] Existen numerosas Guías de buenas prácticas a nivel nacional e internacional que regulan la materia, algunas como la Guía de UFECI, Protocolo guía de obtención, preservación de evidencia digital, Convenio 88/16 del Ministerio de Seguridad de la Nación al que Santa Fe se encuentra adherido, Protocolo para levantar evidencia – PURI disponible en http://www.jus.gob.ar/media/3262247/Protocolo%20unificado.pdf),

[44] Darahuge, M. E. y Arellano González, L., ob cit., pp. 19 y 20. Los autores refieren que la prueba documental informática posee características propias: 1) principio de identidad atípico (la copia digital de un archivo no se puede distinguir del original); 2) posibilidad de modificación por medios locales o remotos; 3) divisibilidad del documento; 4) esta prueba lleva implícita la prueba pericial informática forense. Frecuentemente necesita su convalidación con una prueba de informes solicitada al ISP que corresponda.

[45] Darahuge, M. E. y Arellano González, L., ob. cit., p. 163, la cadena de custodia "*es el conjunto de medidas que deben adoptarse a fin de preservar la identidad e integridad de objetos o muestras que pueden ser fuente de prueba de hechos criminales, para su total eficacia procesal*".

DR © 2021. Universidad de Palermo-Facultad de Derecho
https://www.palermo.edu/derecho/publicaciones/revista_juridica/

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

con su ubicación y metadatos[46], correos electrónicos, caché o cookies, claves, aplicaciones o programas descargados, redes de Wifi utilizadas, contactos, notas, existentes y borrados del aparato, tanto en la memoria del mismo como en las tarjetas de memoria o micro SD.

7. Redes sociales

Son plataformas de intercomunicación social en las que el usuario puede crear un perfil con elementos de representación de su realidad física pero en el ciberespacio, a través del cual vivir experiencias sociales de amistad y demás en Internet[47]. En el ámbito de las investigaciones se presentan como fuentes sumamente útiles por el caudal de datos que se pueden recolectar y de vinculaciones que se pueden obtener[48], ofrecen información actualizada y que, sumada a otras evidencias, puede constituir un elemento más que direccione la identificación de personas, lugares, etc. Respecto a la solicitud de información de perfiles de usuario se deberá previamente obtener autorización judicial y luego oficiar a dichas empresas cuyas sedes, por lo general, se encuentran en otros países. En este punto toma relevancia la cooperación internacional para requerir a las empresas que aporten la información requerida (direcciones IP, nombres de usuario, números de teléfono asociados o cuentas de correo electrónico). Asimismo, se pueden efectuar solicitudes de preservación de información para evitar su eliminación para lo cual no es necesario contar con autorización judicial debido a que no existe una injerencia en los derechos del usuario.

[46] Los metadatos son los "datos del dato", comprenden fecha de creación del archivo, tamaño, fecha de modificación, autor, lugar de creación. En el caso de los correos o emails contiene información de emisor y receptor en los encabezados del mismo, la dirección IP del remitente, etc.

[47] Miró Llinares, F., *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*, Madrid, Marcial Pons, 2012, disponible online https://www.marcialpons.es/media/pdf/9788415664185.pdf

[48] Cámara Federal de Casación Penal, Sala IV "Caso Bejarano Alexis s/Rec de Casación", 04 de diciembre de 2015 disponible online https://www.cij.gov.ar/nota-19281-La-C-mara-Federal-de-Casaci-n-Penal-confirma-condena-por-homicidio-cometido-con-alevos-a.html. En el caso se pudo determinar la identidad de dos personas que mataron a otra en un incendio a partir de un apodo aportado por vecinos del lugar, y la posterior búsqueda en Facebook, lo cual permitió el reconocimiento en función de que su perfil de usuario se encontraba abierto al público general, sin grado de privacidad, por lo tanto el tribunal entendió que no se encontraba vulnerada la correspondencia epistolar porque no hubo afectación a la garantía constitucional del art. 18 CN. Disponible online https://www.cij.gov.ar/nota-19281-La-C-mara-Federal-de-Casaci-n-Penal-confirma-condena-por-homicidio-cometido-con-alevos-a.html

DR © 2021. Universidad de Palermo-Facultad de Derecho
https://www.palermo.edu/derecho/publicaciones/revista_juridica/

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

VI. Niveles en la extracción de información y de afectación a la intimidad y privacidad

Por empezar, no todos los datos personales son sensibles y no toda solicitud de información vulnera garantías constitucionales. Hay distintos niveles de afectación que van desde una mínima intromisión a una de mayor gravedad y para su procedencia se impone el cumplimiento de determinadas condiciones. Partiendo de la base de que los derechos no son absolutos, es posible ir avanzando en la recolección de datos sin lesionar otros intereses hasta tanto sea necesaria la intervención de un juez que decida el límite a partir del cual se ingresa en la esfera privada del individuo.

1. Datos de abonado, informes a empresas prestatarias de servicios de telefonía e internet

El Convenio de Cibercrimen los define como la información básica contenida en forma de datos informáticos o cualquier otra forma que esté en poder de un proveedor de servicios, vinculada a los suscriptores de sus servicios -que no sean de tráfico o de contenido- y por la cual se puede establecer el tipo de servicio utilizado, las provisiones técnicas adoptadas, identidad del cliente, dirección, número de teléfono, datos de facturación y pago, y toda información relativa al lugar donde se encuentran los equipos de comunicación. Comprende también a los datos de usuario de redes sociales (nombre y apellido, correo electrónico o teléfono asociados a la cuenta, dirección, sexo, fecha de creación de la cuenta, localidad, nombre de usuario) y de páginas comerciales (ej. Mercado libre, Amazon, OLX, etc.) que son requeridos para la registración.

Como se indicara anteriormente, este nivel es el de menor gravedad puesto que son datos personales comprendidos en la protección legal (Ley 25326) que identifican a la persona. Se entiende que es válida la solicitud de información a las empresas prestatarias de servicios de comunicación o internet -sin obtener previamente el consentimiento del usuario- puesto que encuadra dentro de las facultades que puede ejercer el Estado en sus investigaciones.

2. Datos de tráfico. Necesidad de autorización judicial y primer límite constitucional

Consisten en aquella información producida sobre en el contexto de una comunicación que se llevó a cabo por medio de un sistema informático o electrónico, aportando datos que permiten identificarla. Fernández Rodríguez lo explica claramente sosteniendo que "los datos de tráfico, o metadatos, en una comunicación son los datos que rodean el mensaje que se transmite, pero que no forman parte de

DR © 2021. Universidad de Palermo-Facultad de Derecho
https://www.palermo.edu/derecho/publicaciones/revista_juridica/

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

dicho mensaje. Son un subproducto de las conexiones, que se concretará en función del tipo de comunicación"[49].

Su contenido permite ubicar en tiempo y espacio a alguien, en un momento determinado, el intercambio de comunicaciones que mantuvo en ese lapso de tiempo, conociendo la cantidad de comunicaciones que entabló como así también los interlocutores. Las direcciones IP asignadas a una conexión, los números de llamadas entrantes y salientes registrados en los "listados sábana"[50] de todas las comunicaciones, las celdas en las cuales impactaron dichas llamadas, la ubicación geográfica, números de IMEI sobre los que impactaron las líneas desde las cuales se realizaron las comunicaciones, las titularidades respectivas, todos datos que permiten constatar la existencia de tales comunicaciones.

Siguiendo el orden de afectación constitucional expuesto, implican una intromisión más notable en la esfera íntima de una persona. En apariencia no refieren ninguna información determinante para una investigación, pero pueden aportar indicios que, sumados a otras evidencias o pruebas, sean de gran utilidad en las investigaciones penales. Es acertada la opinión de Fernández Rodríguez al sostener que

> [h]ay datos de tráfico que integran el derecho al secreto de las comunicaciones y otros que simplemente afectan a la intimidad, la protección de datos o la libertad de circulación. Entre los primeros se halla la identidad de los interlocutores de la comunicación. En cambio, la duración de la llamada o la localización de los interlocutores estarán en el ámbito del derecho a la intimidad[51].

Ello permite escindir la cuestión según el espacio de intimidad que afecte la medida y verificar si en el caso concreto ha generado una afectación al derecho del que se trate.

A nivel nacional la Ley de Telecomunicaciones 25.873[52] en su artículo 2º, impone

---

[49] Fernández Rodríguez, J., "Los datos de tráfico de comunicaciones: en búsqueda de un adecuado régimen jurídico que elimine el riesgo de control permanente", *Revista Española de Derecho Constitucional*, *año* 2016, p. 96, disponible online en https://recyt.fecyt.es/index.php/REDCons/article/view/54343

[50] Tribunal Supremo de Justicia español, Sentencia N° 444/14, en la cual sostuvo que, respecto a los listados de llamados entregados por las compañías de teléfonos a la policía también es necesario obtener autorización judicial. Disponible online https://supremo.vlex.es/vid/516232138

[51] Ibidem, p. 102.

[52] Ley modificatoria de la Ley N 19.798, reglamentada mediante Decreto N° 1563/2004, cuya aplicación fue suspendida por el Decreto N° 357/2005, disponible online http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=31922 En el precedente "Halabi" la CSJN declaró la inconstitucionalidad de la ley 25873 porque contenía previsiones vagas y no surgía de las mismas en qué medida podían las prestatarias captar el contenido de las comunicaciones sin la debida autorización judicial, en el punto 26 del fallo estableció que "*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"*, disponible online http://www.saij.gob.ar/corte-suprema-

DR © 2021. Universidad de Palermo-Facultad de Derecho
https://www.palermo.edu/derecho/publicaciones/revista_juridica/

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

a las empresas prestatarias de servicios de telecomunicaciones la obligación de registrar y sistematizar datos de abonado y de tráfico para ser consultados por el poder judicial o el ministerio público, con el deber de conservación y guarda[53] de los mismos por el plazo de diez años. Se puede advertir la existencia de un riesgo latente de uso indiscriminado por ser un plazo tan exiguo durante el cual la información se encuentra a disposición de organismos estatales que pueden acceder sin que refieran a investigación alguna si no con fines meramente persecutorios, atentando contra la intimidad de los ciudadanos que desconocen dichas intromisiones.

Por lo general este tipo de información es requerida sin mediar autorización judicial con fundamento en el ejercicio de las potestades persecutorias otorgadas a los organismos encargados de la persecución penal. Ante la importancia que poseen tales datos y la influencia que pueden tener para establecer conexiones entre personas que podrían estar involucradas en un delito, sería lógico imponer algún límite a su solicitud ya sea circunscribiendo su procedencia a determinado tipo de delitos que por su gravedad o complejidad ameriten la solicitud de dicha información, o bien exigiendo fundamentos de tales pedidos, impidiendo de tal manera el avance discrecional del Estado.

3. Datos de contenido. Interceptación de las comunicaciones, límites legales y constitucionales

Son aquellos referidos 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, ya no son datos relativos a la comunicación en sí, ya no es el continente sino el contenido[54]. Una de las principales medidas para la obtención de datos de contenido son las interceptaciones de comunicaciones. Siguiendo a Jauchen, el art. 18 de la Constitución Nacional no contempla específicamente la inviolabilidad de las comunicaciones telefónicas o por otros medios, puesto que a la época de la sanción de la misma no existían este tipo de medios. No obstante, como el espíritu de la

justicia-nacion-federal-ciudad-autonoma-buenos-aires-halabi-ernesto-pen-ley-25783-dto-1563-04-amparo-ley-16986-fa09000006-2009-02-24/123456789-600-0009-0ots-eupmocsollaf#

[53] Suprema Corte de Justicia de Irlanda, "Digital Rights Ireland Ltd (C-293/12) y otros (C-594/12) c/ Ireland", 8 de abril de 2014, disponible online http://curia.europa.eu/juris/document/document.jsf?docid=153045&doclang=ES mediante el cual el máximo tribunal irlandés admitió el recurso de inconstitucionalidad contra determinadas disposiciones de la Ley federal de telecomunicaciones 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 declaró que la misma era inválida.

[54] Temperini, M., "Delitos informáticos y cibercrimen: Técnicas y tendencias de investigación penal y su afectación a los derechos constitucionales", disponible en https://www.asegurarte.com.ar/articulos

DR © 2021. Universidad de Palermo-Facultad de Derecho
https://www.palermo.edu/derecho/publicaciones/revista_juridica/

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

norma es tutelar y garantizar el derecho a la intimidad del ciudadano -cualquiera sea el medio que utilice para realizar la comunicación- lo hace bajo el entendimiento de que los diálogos o mensajes son solamente conocidos por los involucrados en la comunicación, no estando expuestos a su difusión ni a la escucha involuntaria de terceros. Sostiene que es este el fundamento bajo el cual los ciudadanos confían en la reserva de sus comunicaciones, manteniendo una "razonable expectativa de privacidad" en el desarrollo de su vida[55].

Con el mismo criterio, la Corte Suprema de Justicia de la Nación, mediante Acordada 17/2019 afirmó que

> [e]l balance entre el derecho de toda persona a no sufrir invasiones a su privacidad y el interés estatal en la persecución penal de un posible delito, debe incluir una necesaria ponderación de los instrumentos escogidos y los fines hacia los que se dirige la específica herramienta investigativa dispuesta en la causa, en cuyo marco corresponde tamizar la medida elegida por los filtros de la necesidad, la adecuación y la proporcionalidad[56].

En ese sentido, las medidas que tienen por objetivo recabar datos de contenido de las comunicaciones personales son de excepción por el grado de intromisión en el ámbito de intimidad de los individuos. Forman parte del tercer nivel de afectación porque representan la invasión más grave dentro de la escala de las medidas investigativas descriptas hasta el momento.

Allí, además, estableció los principios rectores bajo los cuales se deben llevar a cabo estas medidas: tienen carácter *instrumental* -son herramientas creadas al servicio de la función jurisdiccional y deben ser utilizadas únicamente para esclarecer delitos y con el objetivo final de afianzar la justicia-, *excepcional y restrictivo* -previo a su autorización se deberá evaluar la razonabilidad de la según el fin propuesto-, deben ser *fundadas* -esgrimir las razones por las cuales se solicitan evitando recurrir a la misma para fines preventivos o genéricos- y son *provisionales* -sujetas a un plazo determinado-.

En el precedente "Quaranta"[57] la Corte volvió a expedirse en cuanto a la autorización judicial para las intervenciones telefónicas será otorgada cuando

> [m]edian elementos objetivos idóneos para fundar una mínima sospecha razonable (...) si el Estado pudiera entrometerse en el secreto de las comunicaciones telefónicas a partir de "sospechas" de la entidad de las

[55] Jauchen, E., ob. cit., Tomo III, p. 247.

[56] Acordada CSJN 17/2019, disponible online http://servicios.infoleg.gob.ar/infolegInternet/anexos/320000-324999/324490/norma.htm

[57] CSJN, "Quaranta, José Carlos s/ inf. ley 23.737 – Recurso de Hecho - causa n° 763C", disponible online en https://sjconsulta.csjn.gov.ar/sjconsulta/documentos/verDocumentoByIdLinksJSP.html?idDocumento=6884191&cache=1614633125277

DR © 2021. Universidad de Palermo-Facultad de Derecho
https://www.palermo.edu/derecho/publicaciones/revista_juridica/

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

descriptas más arriba, el derecho reconocido constitucionalmente resultaría ciertamente de poca o ninguna relevancia…

4. Crítica a las extracciones ilimitadas. Pesca informática. Riesgos de incurrir en violaciones al derecho a la intimidad.

Una idea propia del sistema inquisitivo es la que entiende que el fin justifica los medios[58] y que, en esa inteligencia, se puede proceder vulnerando garantías y derechos de los encartados si el fin es probar la existencia de un delito y restaurar el orden social vulnerado a partir de su comisión. Por el contrario, la búsqueda de información no es ilimitada y debe estar estrechamente vinculada a lo que se quiere probar.

Un problema que se genera con frecuencia en el marco de las investigaciones penales es que la información obtenida de diversas fuentes -dispositivos informáticos, redes sociales, etc.- se encuentra a discreción del personal a cargo de los procedimientos pudiendo incurrir estos en intromisiones indebidas[59]. Es una práctica potencialmente peligrosa que podría generar graves perjuicios en los intereses de quienes las soportan si se accede a información que no se encuentra vinculada a una investigación concreta. Es dable formular una analogía con respecto al allanamiento, medida sumamente intromisiva en la esfera de privacidad del domicilio intervenido, para ser un procedimiento válido debe estar previamente respaldado en una orden judicial que admita cada uno de los puntos solicitados y contemple tiempo en que se llevará a cabo y la extensión de la medida. Es posible aplicar idéntico criterio a la recolección de evidencias digitales. El acceso a una computadora o Smartphone no admite una pesca indiscriminada de información que no se vincule a ninguna investigación concreta, invocando fines de prevención o de seguridad ciudadana.

El Tribunal Supremo Español en la sentencia N° 204/16[60] ilustró dicha situación indicando que

[d]ado que la multifuncionalidad de los datos que se albergan en estos

[58] Lega, P., "Intervenciones telefónicas y control del debido proceso. El necesario límite a la creación de irrazonables excepciones", *Revista de Derecho penal y Criminología*, La Ley, año VI, N° 2, marzo de 2014, p. 23.

[59] Aboso, G., "Técnicas de Investigación y vigilancia electrónicas en el proceso penal y el derecho a la privacidad en la moderna sociedad de la información", Ferrazuolo, V. (coord.), *Era digital. Delito y prevención*, Buenos Aires, Jusbaires, 2019, p. 61, sostiene que "*No cabe duda de que la erosión de la expectativa razonable de privacidad en el uso de estos servicios telemáticos traería como lógica consecuencia la falta de confianza del público sobre el resguardo de sus derechos personalísimos, al permitir o autorizar el registro y tratamiento de datos por parte de las autoridades públicas, lo que sellaría el destino de esta moderna forma de comunicación".*

[60] Tribunal Supremo de Justicia Español, Sentencia N° 204/16, disponible online https://supremo.vlex.es/vid/631962729#section_28

DR © 2021. Universidad de Palermo-Facultad de Derecho
https://www.palermo.edu/derecho/publicaciones/revista_juridica/

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

dispositivos provoca una extrema debilidad de la tutela jurisdiccional del derecho del investigado a la reserva de su propio entorno virtual, pues una vez realizado el acceso al dispositivo, superando la barrera de la contraseña, todos los datos, incluidos los relacionados con el secreto de las comunicaciones están al libre alcance del investigador.

Este ámbito es donde más dudas se generan en torno a la legitimidad de las medidas probatorias de recolección de evidencia en orden a que el hallazgo de información por fuera de lo autorizado judicialmente, para ser utilizado legítimamente debe estar acreditado de qué manera se obtuvo, sin vulnerar garantías constitucionales.

VII. Conclusiones

Como corolario de lo expuesto, se sostiene que el sistema de administración de justicia penal en Argentina ha logrado superar la lógica inquisitiva del proceso en la mayoría de las provincias, y como parte de dicha superación se revisaron numerosas prácticas que se correspondían con modelos de investigaciones secretas y con organismos públicos con poderes discrecionales. Sin embargo, todavía existe un largo camino por recorrer hacia el fortalecimiento del sistema de garantías procesales y la regulación específica en materia de evidencias digitales.

Los medios empleados en las investigaciones criminales no pueden traspasar los límites impuestos por la legalidad, proporcionalidad, y el respeto de las garantías individuales como la intimidad y privacidad. Quien sea perseguido penalmente por un delito debe poder contar con la posibilidad de controlar toda la actividad que realiza el Estado para endilgarle un hecho delictivo y defenderse ante posibles acusaciones infundadas o logradas en base a información de mala calidad, obtenida de manera ilegítima, sin fundamento alguno. La obligación que pesa sobre el Estado, entonces, es la de garantizar transparencia en la actuación de sus organismos y ello se alcanza estableciendo normativa específica sobre este tipo de medidas y controlando su cumplimiento.

Las dificultades y discusiones que se plantean durante las investigaciones en torno a la evidencia digital, en ocasiones, son generadas en razón de la deficiente e inespecífica regulación legal de las nuevas medidas investigativas sobre medios digitales, que conduce a su aplicación analógica, intuitiva, siguiendo la modalidad del caso a caso.

Se sostiene que una solución posible para lograr el equilibrio entre ambas fuerzas opuestas, tomando en consideración el estado actual de la situación en Argentina y la urgencia que presentan ciertas investigaciones de delitos complejos consiste en solicitar -en los casos en que sea procedente por carecer de una regulación específica

DR © 2021. Universidad de Palermo-Facultad de Derecho
https://www.palermo.edu/derecho/publicaciones/revista_juridica/

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

o adecuada a lo que se intenta realizar-, una autorización judicial a los fines de someter la decisión de su procedencia a un tercero imparcial e independiente, quien deberá analizar la situación concreta y los distintos niveles de información a los que se intente acceder. En ese sentido, la jurisprudencia irá marcando una vía constitucional que proteja los derechos de los ciudadanos sin perjudicar la eficacia de las investigaciones llevadas a cabo por el Estado.

VIII. Referencias

1. Bibliográficas

AA. VV., *Informática y Delito. Reunión Preparatoria del XIX Congreso Internacional de la Asociación Internacional de Derecho Penal (ADIP)*, Grupo argentino, Facultad de Derecho, UBA, Infojus, Buenos Aires, 2014, disponible online en http://www.bibliotecadigital.gob.ar/items/show/1643

Aboso, Gustavo, "La inconstitucionalidad de la requisa y el examen sin autorización judicial de datos personales almacenados en dispositivos celulares de personas detenidas – Breve reseña de los fallos 'Riley vs. California' (2014) y 'United States vs Brima Wurie (2012) de la Corte Suprema de Justicia de los Estados Unidos", *elDial.com*, 31/7/14.

Aboso, Gustavo, "Técnicas de Investigación y vigilancia electrónicas en el proceso penal y el derecho a la privacidad en la moderna sociedad de la información", Ferrazuolo, Vanesa (coord.), *Era digital. Delito y prevención*, Buenos Aires, Jusbaires, 2019.

Aboso, Gustavo, *Derecho Penal Cibernético*, Buenos Aires, BdeF, 2017.

Baclini, Jorge y Schiappa Pietra, Luis, *Código Procesal Penal de Santa Fe comentado, anotado y concordado*, Tomo 1, Juris online, Rosario, 2017.

Baladán Flavia y Hernández Varela, Jimena, "Intimidad y privacidad frente a las intervenciones de las comunicaciones electrónicas", *16° Simposio Argentino de Informática y Derecho*, 45 JAIIO - SID 2016, p. 118, disponible online en http://sedici.unlp.edu.ar/bitstream/handle/10915/58263/Documento_completo.pdf-PDFA.pdf?sequence=1

Binder, Alberto, *Derecho Procesal Penal*, Tomos I y II, Buenos Aires, AdHoc, 2013/2014.

Darahuge, María Elena y Arellano González, Luis E., *Manual de informática fo-*

DR © 2021. Universidad de Palermo-Facultad de Derecho
https://www.palermo.edu/derecho/publicaciones/revista_juridica/

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

rense II (Prueba indiciaria Informático Forense), Buenos Aires, Errepar, 2012.

Delbono, P., "Investigación Forense sobre medios digitales", en *Cibercrimen y delitos informáticos*, Parada, Ricardo (coord..), Buenos Aires, Erreius, 2018.

De Langhe, Marcela, *Escuchas telefónicas. Límites a la intervención del Estado en la privacidad e intimidad de las personas*, Buenos Aires, Hammurabi, 2009.

Fernández Rodríguez, José Julio, "Los datos de tráfico de comunicaciones: en búsqueda de un adecuado régimen jurídico que elimine el riesgo de control permanente", *Revista Española de Derecho Constitucional*, 2016, disponible online en https://recyt.fecyt.es/index.php/REDCons/article/view/54343

Ferreyra, Eduardo, "La Convención de cibercrimen de Budapest y América Latina. Breve guía acerca de su impacto en los derechos y garantías de las personas", *Asociación por los Derechos Civiles*, marzo 2018. Disponible en https://adc.org.ar/wp-content/uploads/2019/06/035-la-convencion-de-cibercrimen-de-budapest-y-america-latina-vol-1-03-2018.pdf

González Álvarez, Daniel, "La Investigación preparatoria del Ministerio Público en el nuevo proceso penal costarricense", en *Revista Pena y Estado*, n° 2, cit. por Mendaña, Ricardo, "El ministerio público y la dirección de la investigación criminal", en *Cuadernos de Derecho Penal*.

Jauchen, Eduardo, *Tratado de Derecho Procesal Penal*, Tomo I, Santa Fe, Rubinzal-Culzoni, 2013.

Joyanes Aguilar, Luis, "Introducción. Estado del arte de la ciberseguridad", en *Revista Pensamiento Penal*, disponible online http://www.pensamientopenal.com.ar/system/files/2015/01/doctrina38717.pdf.

Lega, Pablo, "Intervenciones telefónicas y control del debido proceso. El necesario límite a la creación de irrazonables excepciones", *Revista de Derecho penal y Criminología*, La Ley, año VI, N° 2, marzo de 2014.

Maier, Julio, *Derecho Procesal Penal*, Tomo I, 1° ed., Buenos Aires, AdHoc, 2016

Miró Llinares, Fernando, *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*, Madrid, Marcial Pons, 2012, disponible online https://www.marcialpons.es/media/pdf/9788415664185.pdf

Sain, Gustavo, "La estrategia gubernamental frente al cibercrimen: la importancia de las políticas preventivas más allá de la solución penal", en *Cibercrimen*

DR © 2021. Universidad de Palermo-Facultad de Derecho
https://www.palermo.edu/derecho/publicaciones/revista_juridica/

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

y delitos informáticos, Parada, Ricardo (coord.), Buenos Aires, Erreius, 2018.

Sueiro, Carlos Christian, *Vigilancia electrónica y otros modernos medios de prueba*, Buenos Aires, Hammurabi, 2019.

Temperini, Marcelo, "Delitos informáticos y cibercrimen: Técnicas y tendencias de investigación penal y su afectación a los derechos constitucionales", disponible en https://www.asegurarte.com.ar/articulos

Vázquez Rossi, Jorge, *Derecho Procesal Penal*, Tomo II, Santa Fe, Rubinzal-Culzoni, 1997.

2. Jurisprudencia

Tribunal Constitucional Federal Alemán, BVerfG, decisión del Primer Senado del 10 de noviembre de 2020, disponible en http://www.bverfg.de/e/rs20201110_1bvr321415.html

Tribunal Constitucional Federal Alemán, Sentencia de la Primera Sala –1 BvR 209, 269, 362, 420, 440, 484/83– del 15 de diciembre de 1983, disponible online https://www.kas.de/c/document_library/get_file?uuid=0a66a4a6-1683-a992-ac69-28a29908d6aa&groupId=252038

Cámara Federal de Casación Penal, Sala IV "Caso Bejarano Alexis s/ Rec de Casación", 04 de diciembre de 2015 disponible online https://www.cij.gov.ar/nota-19281-La-C-mara-Federal-de-Casaci-n-Penal- confirma-condena-por-homicidio-cometido-con-alevos-a.html

Corte Suprema de Justicia de la Nación, "QUARANTA, José Carlos s/ inf. ley 23.737 – Recurso de Hecho - causa n° 763C" disponible online en https://sjconsulta.csjn.gov.ar/sjconsulta/documentos/verDocumentoByIdLinksJS P.html?idDocumento=6884191&cache=1614633125277

Corte Suprema de Justicia de la Nación, "Halabi, Ernesto c/ PEN - ley 25.783 - dto. 1563/04" disponible online http://www.saij.gob.ar/corte-suprema-justicia- nacion-federal-ciudad-autonoma-buenos-aires-halabi-ernesto-pen-ley-25783- dto-1563-04-amparo-ley-16986-fa09000006-2009-02-24/123456789-600-0009- 0ots-eupmocsollaf#

Suprema Corte de Justicia de Irlanda, "Digital Rights Ireland Ltd (C-293/12) y otros (C-594/12) c/Ireland", 8 de abril de 2014, disponible online: http://curia.europa.eu/juris/document/document.jsf?docid=153045&docl ang=ES

DR © 2021. Universidad de Palermo-Facultad de Derecho
https://www.palermo.edu/derecho/publicaciones/revista_juridica/

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

Tribunal Supremo de Justicia Español, Sentencia N° 444/14, disponible online https://vlex.es/vid/516232138

Tribunal Supremo de Justicia Español, Sentencia N° 204/16, disponible online https://supremo.vlex.es/vid/631962729#section_28

3. Legislación

Ley de Enjuiciamiento Criminal española disponible en https://boe.vlex.es/vid/ley- organica-13-2015-583908674

Norma ISO/IEC 27041/2015, 27042/15, 27050/2016 disponible online https://www.iso.org/standard/44381.html

Convenio sobre Ciberdelincuencia disponible online https://rm.coe.int/16802fa403

Resolución N° 470/17 Fiscalía General del Ministerio Público de la Acusación de Santa Fe, disponible en https://mpa.santafe.gov.ar/regulations_files/5a96f81f6ab48_Resoluci%C3%B3n %20N%C2%BA%20470.pdf

Proyecto de ley sobre Allanamiento remoto, disponible en https://www.jorgehenn.com/wp-content/uploads/bsk-pdf- manager/2019/09/Allanamiento-Remoto-de-Dispositivos-Tecnologicos.pdf

Disposición N° 20/15 de la Dirección Nacional de Protección de Datos Personales: http://www.jus.gob.ar/media/2898655/disp_2015_20.pdf

Ley N° 19.798, su Decreto reglamentario N° 1563/2004, y Decreto N° 357/2005 disponible online http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=31922

Decreto N° 1563/2004, disponible online http://servicios.infoleg.gob.ar/infolegInternet/anexos/100000- 104999/100806/norma.htm

Acordada CSJN 17/2019, disponible online http://servicios.infoleg.gob.ar/infolegInternet/anexos/320000- 324999/324490/norma.htm

Resolución N° 68/167 de 18 de diciembre de 2013, emitida por la A.G. de Naciones Unidas, disponible online https://digitallibrary.un.org/record/764407?ln=es

DR © 2021. Universidad de Palermo-Facultad de Derecho
https://www.palermo.edu/derecho/publicaciones/revista_juridica/

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv http://revistas-colaboracion.juridicas.unam.mx

4.Otros Artículos digitales consultados

"Alto en el cielo. exploración sobre tecnologías de vigilancia aérea en Argentina" del Área Digital de la Asociación de Derechos Civiles de Argentina: https://adc.org.ar/wp-content/uploads/2019/06/033-alto-en-el-cielo-12-2017.pdf

"Con mi cara no", disponible en https://adc.org.ar/2019/05/23/con-mi-cara-no-reconocimiento-facial-en-la-ciudad-de-buenos-aires/

Guías de buenas prácticas a nivel nacional e internacional que regulan la materia, algunas tales como la Guía de UFECI, Protocolo guía de obtención, preservación de evidencia digital, Convenio 88/16 del Ministerio de Seguridad de la Nación al que Santa Fe se encuentra adherido, Protocolo para levantar evidencia – PURI (Prot. Unif. para recolección de información, disponible en http://www.jus.gob.ar/media/3262247/Protocolo%20unificado.pdf)

DR © 2021. Universidad de Palermo-Facultad de Derecho
https://www.palermo.edu/derecho/publicaciones/revista_juridica/