Análisis jurídico de la situación de la evidencia digital en el proceso penal en Argentina

Volumen 3

por los Derechos Civiles

Área Digital
Asociación por los Derechos Civiles

Abril 2018
https://adcdigital.org.ar

Este trabajo fue realizado como parte de un proyecto financiado por Ford Foundation. Las opiniones expresadas en este documento son de exclusiva responsabilidad de la autora y no reflejan necesariamente la postura oficial de la Asociación por los Derechos Civiles.

Análisis jurídico de la situación de la *evidencia digital* en el proceso penal en Argentina

Natalia Sergi

Informe realizado para la Asociación por los Derechos Civiles
Febrero 2018

1.Introducción

El desarrollo de internet y el impacto social de las tecnologías de la información y la comunicación (TIC) ha provocado una de las discusiones más profundas de los últimos años en el ámbito del derecho procesal penal.

En principio, la ciencia penal había concentrado sus preocupaciones en lo que se denomina *cibercrimen*, esto es, nuevos hechos delictivos, o formas novedosas de comisión de delitos tradicionales, que utilizan la tecnología, o son su forma de comisión. Ello ha instado modificaciones normativas con el objeto de crear nuevas figuras delictivas y/o prever novedosas formas de comisión de delitos en la ley penal, lo que permitió la tipificación del *cibercrimen,* prevista en la Ley de delitos informáticos, nº 26.388[1].

Conjuntamente, trajeron aparejadas discusiones en el ámbito del derecho procesal penal, con relación a lo que hoy llamamos *evidencia digital o electrónica*. Esto es, elementos probatorios que surgen de medios informáticos, digitales o tecnológicos, y que pueden encontrarse alojados en dispositivos o sistemas informáticos de cualquier índole, incluso pueden más modernamente encontrarse alojados en la *nube* y sólo es accesible a través de estos.

Esta problemática primero fue considerada como propia de los delitos informáticos, o de la *cibercriminalidad*. Sin embargo, la dificultad desde el punto de vista jurídico se ha agravado pues el avance de las tecnologías y la utilización de internet en la vida cotidiana, ha llevado la cuestión informática a cualquier investigación de cualquier tipo de hecho. La evidencia digital —junto sus complicaciones— hoy atraviesa el sistema de manera transversal (cualquier caso menor y simple hasta los más complejos y casos de derecho penal común, como de cuello blanco). Ello es lo que plantea los mayores desafíos desde el examen del derecho procesal penal y la vigencia de las garantías, objeto de este informe.

---

[1] El 4 de Junio del año 2008 el Congreso Nacional sancionó la Ley 26.388 de delitos informáticos que modificó el Código Penal para incluir como conductas típicas la falsificación de documentos electrónicos (CP, art. 77 y 292); ofrecimiento y distribución de pornografía infantil – la tenencia solo fue tipificada cuando tiene fines inequívocos de distribución o comercialización- (CP, art. 128); conductas vinculadas a la violación de secretos y la privacidad que incluyen el acceso ilegítimo a sistemas informáticos ajenos, la intercepción de correspondencia electrónica y otras formas de comunicación, la revelación de secretos y los delitos relacionados con la protección de datos personales (CP, arts. 153, 153 bis, 155, 157 y 157 bis); fraude informático (CP, art. 173, inc. 16); daño informático (CP, arts. 183 y 184); interrupción de comunicaciones (CP, art. 197) y la destrucción de pruebas contenidas en soportes informáticos (CP, art. 255). Sobre los antecedentes de la Ley 26.388 y los problemas dogmáticos de los tipos penales sancionados, ver. Pablo Palazzi, *Los delitos informáticos en el Código Penal. Análisis de la Ley 26.388*, editorial Abeledo Perrot, Buenos Aires, 2009.

Este informe es realizado sobre la base, y por encargo de la Asociación por los Derechos Civiles (ADC), de la propuesta *Cibercrimen y la adaptación del derecho procesal penal, Oportunidades y desafíos para los derechos humanos* y sobre la base de la problemática de la investigación forense informática, que fue desarrollada por el Ing. Gustavo Presman, en enero 2017 para ADC *Estado de la investigación forense informática en Argentina*.

2.Evidencia digital

Aún no existe una definición normativa en las legislaciones procesales sobre el concepto de evidencia digital. Ello ha sido abordado por diversos organismos que han formulado propuestas tomando en consideración sus características más salientes.

Así, la Guía de Prueba Electrónica del Consejo de Europa[2] utiliza la siguiente definición: "La prueba electrónica es aquella información o datos que han sido creados, almacenados o transmitidos a través de dispositivos electrónicos y tienen relevancia en un procedimiento judicial"; la Organización Internacional de Evidencia Computacional -IOCE[3]- en el año 2000 definió la evidencia digital como "toda información generada, almacenada o transmitida a través de medios electrónicos que puede ser utilizado en una corte judicial" y, en un sentido similar, la organización Grupo de Trabajo Científico sobre Evidencia Digital -SWGDE[4]- definió a la evidencia digital como "información de valor probatorio almacenada o transmitida en forma digital". En el ámbito del *CommonLaw*, cabe destacar la definición de Eoghan Casey, cuyo uso se ha extendido ampliamente en la doctrina especializada: "Cualquier dato almacenado o transmitido utilizando computadoras que sustenta o rechaza una teoría sobre cómo ha sucedido un delito o que acredita elementos fundamentales del delito tales como la intención o posibles coartadas"[5].

Desde un punto de vista más estricto, la denominada evidencia digital es en realidad un tipo de evidencia electrónica (concepto más amplio) aunque en muchas ocasiones son utilizados como sinónimos. El término evidencia

---

[2] Data Protection and Cybercrime Division del Consejo de Europa,*Guía de Prueba Electrónica. Guía básica para Fuerzas y Cuerpos de Seguridad, Jueces y Fiscales*, versión en español, Estrasburgo, Francia, marzo del 2013.

[3] International Organization on Computer Evidence, organización internacional creada ya en 1998 con la finalidad de nuclear a agencias de persecución penal de diferentes países a fin de que intercambien información y buenas prácticas en materia de persecución de delitos informáticos y adquisición de evidencia digital. Ver. http://www.ioce.org/

[4]Scientific Working Group on Digital Evidence.https://www.swgde.org/about_us

[5]Eoghan Casey, *Digital Evidence and Computer Crime*. traducción de Marcos G. Salt del texto original.

electrónica incluye forma de datos análogos como fotos, audios o videos que pueden ser digitalizados y asumir formatos digitales aunque en su origen no lo eran. Por este motivo, algunos autores prefieren poner el acento en el concepto más amplio de la evidencia electrónica (incluyendo los datos análogos y digitales que adquieren la forma de datos digitales) como los datos en formato digital que son creados, manipulados, almacenados o comunicados por cualquier dispositivo informático o sistema informático o transmitidos por un sistema de comunicaciones y que tienen relevancia para un proceso[6]. En este informe nos referiremos a la evidencia digital abarcando ambos conceptos.

Las características y diferencias más notables entre los elementos de prueba físicos y los datos informáticos, desarrolladas en el documento sobre tratamiento de la Evidencia Digital del Consejo de Europa[7] son:

- El dato informático no es visible para las personas sin conocimientos y formación técnica especial. De manera tal que requiere algún tipo de traducción tecnológica del formato digital para ser apreciada por los sentidos de los operadores del sistema penal o de cualquier persona. De esta manera, la información almacenada en los dispositivos informáticos no resulta de mucha utilidad para quienes no son especialistas debido a su carácter técnico y a la necesidad de conocimientos específicos para asegurar un tratamiento adecuado que evite alteraciones.
- El dato informático es muy frágil y volátil. En algunos casos, las pruebas electrónicas están almacenadas en dispositivos electrónicos en los que cualquier acción puede alterar su estado. El cambio en la memoria de los dispositivos puede ocurrir por alterar el estado original en el que se encontró un equipo (por ejemplo, apagarlo o encenderlo) lo que genera la necesidad de mecanismos especiales para asegurar la cadena de custodia de los datos.
- El contenido original puede ser alterado o destruido incluso mediante el uso habitual del dispositivo electrónico. El estado de la memoria de los dispositivos electrónicos cambia constantemente, ya sea por voluntad del usuario ("guardar documento", "copiar archivo") o bien automáticamente por el sistema operativo ("asignar espacio para programa", "almacenamiento temporal de datos para intercambio entre dispositivos").
- Masividad de la información digital y dificultad para la búsqueda de la información pertinente para el objeto procesal. La capacidad creciente de

---

[6]Cfr. Salt, Marcos G., *El acceso transfronterizo de datos y las técnicas de acceso remoto a datos informáticos: nuevos desafíos de la prueba digital en el proceso penal*, su tesis doctoral presentada en Córdoba en mayo 2017, p. 18. La información sobre el derecho comparado brindada en este informe surge de dicha tesis.

[7]*Guía de Prueba Electrónica…*, elaborada por la Data Protection and Cybercrime Division del Consejo de Europa, ob. cit, pág. 12 y ss; conclusiones de la International Telecommunication Union en *Manual de Comprensión del Ciberdelito. Fenómenos, Dificultades y Respuestas Jurídicas*, publicación de la versión en Español de Septiembre del año 2012.

almacenamiento de los dispositivos y el bajo costo económico que significa está generando un número cada vez mayor de documentos digitales. Sin perjuicio de las herramientas informáticas que permiten automatizar los procesos de búsqueda, la identificación de la evidencia digital pertinente en un dispositivo o sistema informático que puede transportar millones de documentos constituye un desafío logístico para los investigadores y un desafío para las garantías individuales por la posibilidad de encuentros causales (o no tan casuales) de información indiscriminada muchas veces alejada del objeto de prueba que habilitó una medida.

- La evidencia digital puede *copiarse* sin límites, en realidad, si la operación se efectúa correctamente y con los instrumentos necesarios no se trata propiamente de copias sino de una clonación ya que los nuevos resultados mantendrían todas las características del original. El contenido electrónico puede copiarse infinitas veces y ser exactamente igual al contenido original. Este atributo único permite realizar múltiples copias exactas al contenido original para ser distribuidas y analizadas por diversos especialistas al mismo tiempo (por ejemplo, puede entregarse una copia *bit a bit* a la defensa para que realice su propia pericia). De esta manera una correcta obtención de la prueba digital permite que todas las medidas sean siempre actos de prueba reproducibles, en términos procesales[8].

3.La evidencia digital en el derecho comparado[9]

La *evidencia digital* ha puesto al proceso penal ante una problemática jurídica con relación a la posible adaptación de los medios probatorios tradicionales a las nuevas tecnologías y también enfrenta al proceso penal a la formulación de nuevos medios de prueba, de coerción probatorios, o medidas de investigación —que son comúnmente abarcados por la denominación medios de prueba simplemente por el capítulo de la ley que los establece— (por ejemplo, al acceso transfronterizo de datos, los accesos remotos, o la utilización de software maliciosos por parte del Estado). En una u otra tarea, el examen jurídico es complejo y requiere de discusiones profundas atravesadas siempre por el resguardo de garantías constitucionales (principalmente, el derecho a la intimidad) y por garantizar la certeza del elemento probatorios (cadena de custodia).

[8] Cfr. Salt, Marcos G., tesis doctoral, p. 20.

[9] Cfr. En todo este capítulo seguimos la tesis doctoral de Salt, Marcos G.

La *Convención Europea Sobre Delitos Informáticos* (Convención de Budapest)[10] es presentada como un hito fundamental por propiciar la regulación de instrumentos procesales especiales que permitan la investigación de los delitos informáticos y extender estas reglas procesales, a la investigación de cualquier delito. Esto es, que los medios de prueba especiales previstos para la obtención e incorporación al proceso de las pruebas digitales se apliquen no sólo en la investigación de los delitos informáticos sino, de manera general, en todos los procesos penales en los que resulte necesaria la obtención de evidencia digital[11]. Prevé los siguientes medios de prueba:

- Aseguramiento de datos: este medio de prueba consiste en la facultad otorgada a las autoridades que llevan adelante una investigación penal concreta de ordenar a los titulares o administradores de sistemas informáticos que tengan alojados datos informáticos que pueden ser de utilidad para la investigación, que los preserven por un tiempo determinado (en general las legislaciones prevén un plazo que oscila entre los 30 y 90 días)[12], ello es para evitar que sean borrados o alterados durante el tiempo que demande para obtener las autorizaciones necesarias de acuerdo a los requisitos y garantías previstos en la legislación procesal para su obtención e incorporación al proceso. En términos más sencillos, ordenar al encargado o titular de un sistema informático (sea persona física o jurídica, privada o pública) que determinados datos queden asegurados mediante mecanismos informáticos por un tiempo determinado sin posibilidad de que sean borrados o alterados. Ello evita el borrado automático de datos por parte del sistema informático en el que los datos están alojados que es de práctica

---

[10]Consejo de Europa, *Convention on Cybercrime* (CETS 185), firmada en Budapest el 23/11/2001 que entró en vigencia el 1/7/2004. Ver texto completo en español: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/ETS_185_spanish.PDF

[11] Ver Artículo 14 de la Convención y los puntos 131 y ss. del reporte explicativo de la convención: "131. Los artículos de esta Sección describen algunas medidas procesales que deben adoptarse a nivel nacional con el fin de facilitar la investigación penal de los delitos establecidos en la Sección 1, otros delitos cometidos por medio de un sistema informático y la obtención de pruebas en formato electrónico relativas a un delito penal…".

[12] Art. 16 de la Convención de Budapest: "Conservación rápida de datos informáticos almacenados. 1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para permitir a sus autoridades competentes ordenar o imponer de otra manera la conservación rápida de determinados datos electrónicos, incluidos los datos sobre el tráfico, almacenados por medio de un sistema informático, en particular cuando existan razones para creer que los datos informáticos resultan especialmente susceptibles de pérdida o de modificación. 2. Cuando una Parte aplique lo dispuesto en el anterior apartado 1 por medio de una orden impartida a una persona para conservar determinados datos almacenados que se encuentren en posesión o bajo el control de dicha persona, la Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a esa persona a conservar y a proteger la integridad de dichos datos durante el tiempo necesario, hasta un máximo de noventa días, de manera que las autoridades competentes puedan conseguir su revelación. Las Partes podrán prever que tales órdenes sean renovables…"

habitual. En general, en estos supuestos el borrado se debe a cuestiones de costos económicos por el almacenamiento, comerciales o, en algunos casos, de políticas de protección de datos personales.

- La orden de presentación de datos: otorga la facultad a las autoridades de ordenar a los proveedores de servicios de internet o los titulares de cualquier sistema de alojamiento de información en formato digital que entregue o informe determinados datos que obren en su poder[13]. Se refiere a los datos almacenados o existentes en un momento determinado y, por lo tanto, excluye a los datos de tráfico o contenido todavía no generados que implican supuestos de intercepción de datos.
- El registro y secuestro de datos informáticos: esta medida tiende a habilitar, en el marco de una investigación penal concreta, el registro de dispositivos o sistemas informáticos con el fin de copiar o secuestrar "datos" que puedan resultar útiles y pertinentes para el objeto procesal[14].
- Con relación al Acceso Transfronterizo[15] la Convención de Budapest reguló el tema de acuerdo a los consensos que los representantes de los países redactores pudieron alcanzar en el momento de su redacción y posterior aprobación. El texto de la Convención toma parte de las propuestas de la Resolución R (95) del Comité de Ministros del Consejo de Europa y de las discusiones y propuestas de los demás foros internacionales. Sin embargo, al momento de establecer normas con carácter vinculante para los Estados, limita las situaciones en las que admite las posibilidades de los Estados de acceder a datos en extrañas jurisdicciones (art. 19). La norma es clara en expresar que se trata de la posibilidad de acceder a un sistema informático conectado siempre que se pueda determinar que el sistema al que se accede desde el dispositivo original se encuentre también ubicado en el mismo territorio, lo que parece excluir la posibilidad de que la medida habilite una intervención transfronteriza. En el capítulo dedicado a la cooperación internacional, aunque de manera limitada, la Convención es el primer texto normativo internacional vinculante que logra plasmar situaciones de acceso transfronterizo de datos como excepciones al principio de territorialidad que, de acuerdo al texto de la propia convención internacional, prevé como criterio general de asignación de los poderes procesales (art. 22 y 25). Los redactores del texto advirtieron con razón que en el futuro resultaría

---

[13] Artículo 18 de la Convención, en las partes pertinentes: "ordenar: a) A una persona que se encuentre en su territorio que comunique determinados datos informáticos que posea o que se encuentren bajo su control, almacenados en un sistema informático o en un medio de almacenamiento de datos informáticos; y b) a un proveedor de servicios que ofrezca prestaciones en el territorio de esa Parte que comunique los datos que posea o que se encuentren bajo su control relativos a los abonados en conexión con dichos 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…"

[14] Cfr. Salt, Marcos G., tesis doctoral, p. 22.

[15] Cfr. Salt, Marcos G., tesis doctoral, p. 225.

necesario ampliar los criterios que lograron plasmar y de hecho dejaron abierta la posibilidad de nuevos supuestos legítimos de acceso a los datos en extraña jurisdicción[16]. La norma que prevé expresamente la posibilidad del acceso transfronterizo a datos es claramente una solución de compromiso, de alcances limitados, que no permite solucionar todos los problemas que pueden generarse hoy con el avance tecnológico. El texto regula dos supuestos habilitantes del acceso transfronterizo de datos en el artículo 32[17]: "Acceso transfronterizo a los datos informáticos almacenados, con consentimiento o de libre acceso. Cualquier Estado podrá sin autorización de otro: a. acceder a los datos informáticos almacenados de libre acceso al público (fuentes abiertas), independientemente de la localización geográfica de esos datos; o b. acceder a, o recibir a través de un sistema informático situado en su territorio, los datos informáticos almacenados situados en otro Estado, si se obtiene el consentimiento legal y voluntario de la persona autorizada para divulgarlos a través de ese sistema informático". De esta forma, habilita el acceso transfronterizo de datos: cuando estos sean de acceso público; cuando se obtiene consentimiento lícito y voluntario de la persona legalmente autorizada a revelarlos. El primer supuesto no ha generado inconvenientes en su interpretación. El segundo supuesto, por el contrario, ha generado en su aplicación práctica dudas de interpretación en

---

[16] Las explicaciones de los redactores expresadas en el punto 293 del reporte explicativo son indicativas de las dudas que el tema generaba y aún genera: "La cuestión de si una Parte puede acceder de forma unilateral a los datos informáticos almacenados en otra Parte sin solicitar la asistencia mutua fue una cuestión que examinaron detenidamente quienes redactaron el Convenio. Hubo un examen detallado de los casos en los cuales puede ser aceptable que los Estados actúen de manera unilateral y aquellos en los que puede no serlo. En última instancia, quienes redactaron el Convenio determinaron que no era posible todavía elaborar un régimen completo y vinculante desde el punto de vista legal que regule este campo. En parte, esto se debió a la falta de experiencias concretas respecto de este tipo de situaciones hasta la fecha, y, en parte, esto se debió a que se consideró que la solución adecuada a menudo es resultado de las circunstancias concretas de cada caso, lo que hace difícil formular normas generales. En última instancia, los redactores decidieron sólo enunciados en el artículo 32 de la Convención de las situaciones en las que todos coincidimos en que la acción unilateral es admisible. Acordaron no regular otras situaciones hasta el momento en que la experiencia ha ido obteniendo más y más debates pueden celebrarse a la luz de la misma. En este sentido, el Artículo 39, párrafo 3 establece que no se autorizan ni se excluyen otras situaciones.". Este último párrafo de la nota ha sido interpretada como una indicación expresa de los redactores de que no excluían otras formas de acceso transfronterizo.

[17] Ver nota 294 del Reporte Explicativo: "El Artículo 32 (Acceso transfronterizo a datos almacenados, con consentimiento o cuando sean accesibles al público) aborda dos situaciones: primero, cuando los datos a los que se ha de acceder sean accesibles al público y segundo, cuando una Parte ha accedido a datos o recibido datos ubicados fuera de su territorio a través de un sistema informático de su territorio y ha obtenido el consentimiento legal y voluntario de la persona que tiene autoridad legal para revelar los datos a la Parte a través de ese sistema. La cuestión de quién está "legítimamente autorizado" a revelar datos puede variar dependiendo de las circunstancias, la naturaleza de la persona y la ley aplicable de que se trate. Por ejemplo, el correo electrónico de una persona puede estar almacenado en otro país por un proveedor de servicios, o una persona puede deliberadamente almacenar datos en otro país. Estas personas pueden recuperar los datos y, siempre que tengan la autoridad legal, pueden voluntariamente revelar los datos a los agentes del orden o permitir a esos funcionarios acceder a los datos, según lo dispuesto en el artículo".

la jurisprudencia de los países miembros de la Convención sobre quién es la persona autorizada a brindar el consentimiento. ¿Se trata del titular de los datos o puede brindar el consentimiento la empresa proveedora de servicios en la que los datos están alojados[18]? También subsisten las dudas y conflictos sobre la posible afectación del principio de territorialidad y soberanía que puede generar el hecho de que, aun en estos supuestos limitados y otras formas de acceso transfronterizo que se han dado en la práctica de las investigaciones, no se otorga ningún tipo de intervención al Estado nacional en el que se encuentra el servidor que aloja la información que es obtenida por las autoridades de otro Estado. Todo ello ha generado un trabajo intenso de los miembros del Comité de la Convención (TC-Y) para intentar alcanzar soluciones de fondo, ya sea profundizando la utilización de los artículos vigentes de la convención e, incluso la posibilidad de promover reformas para introducir nuevas normas que solucionen las situaciones prácticas a las que se enfrentan las investigaciones. Es fácil advertir que el tema ha pasado a ser prioritario para el Comité de trabajo del Convenio de Budapest (unidad de aplicación de la Convención Europea sobre delitos informáticos) que ha generado grupos de trabajo *ad hoc* para realizar estudios y proponer alternativas de solución. Así se creó primero el grupo *ad hoc* de expertos sobre acceso transfronterizo de datos y jurisdicción (año 2011) y, posteriormente, cuando este grupo culminó su tarea, un nuevo grupo de trabajo sobre justicia penal y acceso a evidencias almacenadas en la nube (diciembre de 2014). El primer grupo de trabajo culminó el 9 de abril del año 2013 un documento con propuestas para un posible protocolo adicional a la Convención de Budapest introduciendo posibles habilitaciones para nuevos supuestos de acceso transfronterizo de datos que no logró consenso como para alcanzar un texto normativo vinculante y culminó sus tareas en Diciembre del año 2014 con un documento final de informe en el que se mantienen las propuestas de un protocolo adicional que habilite nuevas formas de acceso transfronterizo de datos[19], dando paso a la conformación del segundo grupo especial de trabajo antes mencionado que

---

[18] Sobre este tema ver la Nota explicativa elaborada por el Grupo especial de Trabajo del TC-Y, *Nota de orientación sobre el acceso transfronterizo de datos (artículo 32) adoptada por la 12 sesión Plenaria del TC-Y*, publicada en español en libro editado por el Consejo de Europa, *Convención sobre la Ciberdelincuencia. Informe Explicativo y Notas de Orientación*, pág. 294 y ss. El texto de la Nota propone criterios de interpretación que resultan de suma importancia tratando los temas que habían generado dudas en la jurisprudencia de los países miembros como la noción del consentimiento o la persona legitimada para permitir el acceso a los datos o revelarlos.

[19] Disponible en http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2014)16_TBGroupReport_v17adopted.pdf

produjo ya diversos informes y propuestas[20]. Lo cierto es que hasta la fecha no se ha alcanzado el consenso como para lograr reformar el texto de la convención o promover un protocolo adicional[21]. Durante las actividades de ambos grupos especiales conformados por el T-CY del Consejo de Europa se celebraron audiencias públicas, reuniones con empresas del sector privado y encuentros con autoridades a cargo los organismos de protección de datos personales (estos últimos en general, se han manifestado en contra de muchas de las opciones de accesos transfronterizos en el marco de las causas penales que requieren los organismos de persecución penal[22]). Estos contrapuntos dejaron en evidencia la necesidad de encontrar fórmulas de mayor coordinación entre los intereses jurídicos en juego (investigación penal/protección de datos personales[23]).

A. En *Latinoamérica,* la Convención de Budapest, así como reformas procesales que contemplen nuevos medios tecnológicos, no tienen la extensión que pueda establecer estándares con relación a las discusiones jurídicas profundas que estas nuevas tecnologías deberían provocar en los sistemas procesales. Tanto es así que en términos genéricos los organismos internacionales del sistema americano no se han ocupado profundamente del problema que plantea la evidencia digital en los procesos penales.

---

[20] Entre ellos destaca el informe *Criminal Justice Access to data in the cloud: Challenges* del 26 de mayo de 2015 y *Criminal Justice Access to electronic evidence in the cloud. Informal summary of issues under consideration by the cloud evidence group* del 17 de febrero del 2016, ambos disponibles en http://www.coe.int/en/web/cybercrime

[21] Ver los elementos de un posible protocolo adicional propuestos por el grupo especial de trabajo en https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680 2e70b6

[22] Muchas de las posturas aparecen como irreconciliables con las necesidades de investigación de los Estados en materia penal. Cfr. A modo de ejemplo, Article 29 Data Protection Working Part (European Union): Opinion 05/2012 on cloud computing (aprobado el 1 de julio del año 2012).

[23] Los documentos de ambos grupos de trabajo están disponibles en http://www.coe.int/en/web/cybercrime/tb. Especial interés reviste la reciente modificación de la normativa europea de protección de datos personales (abril del año 2016) que tendrá gran influencia en las resoluciones que se adopten en relación a la Convención de Budapest y en la legislación interna de los diferentes países. Ver resumen de prensa en http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm

En el ámbito de la *OEA* , el Grupo de Trabajo en Delito Cibernético[24] y el Portal Interamericano de Cooperación en Delito Cibernético[25], constituyen dos de los principales desarrollos emanados del proceso de Reuniones de Ministros de Justicia u otros Ministros, Procuradores o Fiscales Generales de las Américas (REMJA), para fortalecer la cooperación internacional en la investigación y persecución del delito cibernético, facilitar el intercambio de información y de experiencias entre sus integrantes y formular las recomendaciones que sean necesarias para mejorar y fortalecer la cooperación entre los Estados miembros de la OEA y con otras organizaciones o mecanismos[26].

No obstante, a pesar de las continuas corrientes de reformas procesales en toda la región ello no ha implicado que se desarrollen nuevas normas de medios tecnológicos, ni que se resuelvan normativamente los problemas que la aplicación de los medios probatorios tradicionales mediante el principio de libertad probatoria.

Algunos países se encuentran avanzando en regular leyes de cibercriminalidad integrales, esto es, que contienen normas penales como procesales para adaptarlas a la Convención. Puesto que suelen ser tratadas tipificaciones penales, las normas suelen ser minuciosas en definiciones y previsiones de medios probatorios[27]. Ello puede resultar a corto plazo obsoleto pues la evolución tecnológica prontamente creará nuevos medios más eficaces no previstos y nuevas cuestiones que excedan el marco de dicha definición detallada.

Así *Colombia*, que ha modificado su código procesal penal (Ley 906 del 2004), contiene Orden de Presentación en su art. 236; Registro y Confiscación de datos informáticos almacenados, art. 236 y 244. *Guatemala* se encuentra tratando un

---

[24] Está integrado por los expertos gubernamentales, con responsabilidades en este campo o en materia de cooperación internacional para la investigación y persecución del delito cibernético, de los Estados Miembros de la OEA.

[25] Este Portal fue creado para facilitar y hacer más eficiente la cooperación y el intercambio de información entre los expertos gubernamentales de los Estados miembros de la OEA con responsabilidades en materia de delito cibernético o en cooperación internacional en la investigación y persecución de este delito. En dicho portal es posible relevar la legislación de los miembros de la OEA con relación a la cibercriminalidad.

[26] A excepción *Estándares para una Internet Libre, Abierta e Incluyente Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos*, donde se refiere a la protección de ámbitos de privacidad y de datos personales en las comunicaciones en internet; http://www.oas.org/es/cidh/expresion/docs/publicaciones/INTERNET_2016_ESP.pdf.

[27] De hecho, es más frecuente que países, por ejemplo, Perú, Argentina y Paraguay, hayan reformado su ley penal, más la reforma procesal aún no ha sido posible.

proyecto de ley en el Congreso[28], en el capítulo sobre medidas cautelares procesales y procedimentales prevén: el aseguramiento de datos, orden de presentación, registro de secuestro de datos, interceptación de comunicaciones (art. 26 a 29 del proyecto)[29]. *Chile*, en su CPP, tiene previsto el registro y confiscación de correspondencia electrónica, art. 217 y 218, que seguramente en un futuro debe adecuar su legislación en virtud de la ratificación de la Convención. *Panamá*, en el Código Judicial tiene previsto el registro y confiscación de datos informáticos almacenados (art. 2178), obtención en tiempo real de datos sobre el tráfico (art. 16 – Ley 16/2004), y la interceptación de Datos sobre el Contenido (art. 16 – Ley 16/2004). *República Dominicana* en su Ley sobre Crímenes y Delitos de Alta Tecnología (53-07) tiene prevista la conservación rápida de datos informáticos almacenados (art. 54(b)), conservación y revelación parcial rápidas de datos sobre el tráfico (art. 56), orden de presentación (art. 54(a)), registro y confiscación (art. 54(b), (e), (f) y (j)), obtención en tiempo real de datos sobre el tráfico (art. 54(k), e (i)) y obtención en tiempo real de datos sobre el contenido (art. 54(l)). *Costa Rica*, tiene previsto el registro y confiscación en los artículos 198 y 199 del código procesal penal y artículo 1 de la ley sobre registro, secuestro y examen de documentos privados e intervención de las comunicaciones y la interceptación de datos sobre el contenido: artículo 9 de la ley sobre registro, secuestro y examen de documentos privados e intervención de las comunicaciones.

A pesar de la importancia internacional de la Convención, *pocos países han ratificado la Convención en Latinoamérica: Panamá, República Dominicana y recientemente Chile*. A pesar de ello, el Consejo de Europa (hayan o no ratificado la Convención) interviene, promueve la formación de operadores del sistema, envía expertos, etc., a los diferentes países donde se producen modificaciones legislativas, de manera tal que, con diferencias menores, las normas suelen contener las previsiones de la Convención (que excede los 15 años de antigüedad).

Los países en Latinoamérica (países en desarrollo) no siempre tienen los recursos para no encontrarse inducidos por la Cooperación Internacional que, en realidad, tiene su propia agenda (unificar normas, incorporar las redes 24/7[30], flexibilizar normas de cooperación internacional, etc.). Las medidas que proponen son presentadas como atractivas, y supuestamente eficaces, y en muchos aspectos beneficiosas para el país, sin embargo, su incorporación a la

---

[28] Es posible acceder al textohttp://old.congreso.gob.gt/archivos/iniciativas/registro5254.pdf.

[29] El proyecto, principalmente, vinculado con tipificación de hechos delictuales, fue objeto de una Nota Técnica por parte de la Relatoría Especial para la libertad de expresión, con fecha 8 de mayo de 2017.

[30] Incluso apoya formación jurídica de ministerio públicos en Argentina.

legislación interna debe ser minuciosamente estudiada para encontrar límites adecuados de protección de los derechos de sus ciudadanos y respectar la soberanía. En este sentido, la situación de la discusión en Latinoamérica no se encuentra más avanzada ni resulta diferente a la de Argentina que debe estar atenta a este equilibrio, como lo hacen los países centrales.

B. La Convención hoy por hoy es el instrumento que mayor consenso internacional ha alcanzado. Ha provocado reformas procesales en diversos países de gran influencia en nuestro medio jurídico: Alemania, Francia, España, Italia y Portugal, y es en dichos países donde se han producido las discusiones jurídicas más profundas que nos incitan a reflexionar sobre los reales problemas del moderno derecho procesal penal que en modo alguno se agotan, ni finalizan con la Convención ni la adaptación a su normativa, que incluso a esta altura puede no resultar novedosa. En este sentido, la normativa procesal penal en Argentina será realmente novedosa y moderna en tanto prevea la evolución tecnológica que resulta mucho más veloz que las reformas normativas.

A modo de ejemplo trataremos aquí dos casos de nuevas tecnologías en el derecho comparado, lo que permite relevar las decisiones jurídicas y también judiciales en el examen de esos nuevos medios probatorios.

> **I.** La utilización de software especial de acceso remoto a datos en el derecho comparado[31]

Lo habitual hasta hoy ha sido que el registro y secuestro de datos informáticos a los fines de ser utilizados como evidencia en una causa penal requiera, previamente, de un acceso al soporte físico en el que los datos están alojados (computadoras, teléfonos móviles, discos rígidos externos, pen drive, cámaras digitales, consolas de juegos, etc.). Así, la búsqueda de datos informáticos a los fines de su posterior *aseguramiento, copia o secuestro* se realiza en la generalidad de los casos, luego de secuestrar o tener acceso material al soporte físico en el que los datos útiles para la investigación están alojados, ya sea que se los encuentre de alguna manera en el lugar en el que el delito sucedió[32] o en una inspección de un lugar o se obtenga a través de una requisa personal o del allanamiento de una morada. Es decir que, tanto para realizar una búsqueda simple de documentos u otro tipo de datos previamente determinados que están

---

[31] Salt, Marcos G., tesis doctoral, p.58.

[32] Por ejemplo, un teléfono celular o una tablet hallada a simple vista en el lugar en que se cometió un robo o un homicidio.

almacenados informáticamente[33], como para ejecutar tareas de informática forense más complejas para la búsqueda de la información relevante en la investigación[34] y proceder posteriormente a su *copia, aseguramiento o secuestro* en el caso que resulten útiles como evidencia en un proceso penal determinado, los investigadores y peritos trabajan sobre el soporte físico en el que los datos están alojados (por ejemplo una computadora) que ha sido secuestrado o requisado en un procedimiento. En otros supuestos, realizan las operaciones necesarias para la búsqueda de los datos informáticos útiles para la investigación trabajando sobre una copia forense de los datos informáticos contenidos en dichos soportes realizada o supervisada por el encargado de la

[33] Supongamos, verbigracia, búsquedas simples de los archivos informáticos que contienen los resúmenes de cuenta de determinadas personas en el servidor de una institución bancaria o planillas de la contabilidad de una empresa en su computadora o fotos almacenadas en el teléfono celular de un sospechoso.

[34] Supongamos, como ejemplos de tareas de informática forense más complejas, que resulta necesario identificar evidencia relevante para una investigación que suponemos está alojada en un soporte informático que contiene, además, gran cantidad de información que nada tiene que ver con el objeto procesal de la causa y puede incluso afectar la intimidad de terceras personas ajenas a la investigación por lo que resulta necesaria la utilización de programas de informática forense especiales que utilizan para la búsqueda en cúmulos importantes de información palabras claves o imágenes como patrones de búsqueda, o casos en los que la información relevante ha sido borrada por el usuario y es necesario utilizar herramientas de informática forense para recuperar estos archivos o buscar archivos de imágenes o video ocultos en el sistema en formatos de almacenamiento diferentes, etc. También puede resultar necesario utilizar técnicas especiales para obtener claves de acceso a archivos.

ejecución del allanamiento o la requisa[35] pero, en ambos casos, siempre con acceso físico al soporte (computadora, pen drive, teléfonos móviles) en el que la información está alojada. Una vez obtenido el acceso al dispositivo informático en el que se supone está alojada la evidencia pertinente para la investigación (o a la copia forense), los investigadores o peritos utilizarán las diferentes técnicas de búsqueda forense[36].

De esta manera, hasta ahora, lo usual ha sido que la obtención de evidencia digital para un proceso penal requiera, previamente, la necesidad de tener acceso de manera *legítima* al soporte físico (*hardware*) donde la información

---

[35] Usualmente, lo que sucede en la práctica es que al momento de realizar un allanamiento en el que está involucrada la necesidad de registrar y secuestrar datos contenidos en soportes digitales, los funcionarios a cargo del allanamiento se encuentran frente a una disyuntiva que resulta más difícil de resolver día a día en la medida en que aumenta la cantidad de información digital almacenada y la utilización cada vez mayor de soportes susceptibles de almacenar información digital en todos los ámbitos (domicilios personales, empresas, instituciones públicas, etc.). Pensemos por ejemplo en un allanamiento a un banco o una empresa en la que se encuentran cien computadoras. Una posibilidad que tienen los investigadores es secuestrar todos los elementos físicos susceptible de contener evidencia digital (o sea, en el ejemplo, las cien computadoras sin efectuar en el lugar del allanamiento análisis alguno sobre su contenido) para que posteriormente el registro y eventual secuestro de datos sea realizado por los peritos en un laboratorio forense. En este caso, en los hechos, la medida tendrá las formas y deberá respetar los requisitos habituales del secuestro de cualquier prueba física (en este caso las computadoras). Resultará necesario adoptar las medidas de aseguramiento de los elementos secuestrados para garantizar la cadena de custodia de manera bastante similar a las que se adopta en el secuestro de otras *cosas* como documentos o armas (sin perjuicio de algunas medidas técnicas especiales para evitar que los datos informáticos puedan ser borrados u alterados). Sin embargo, como el lector advertirá, esta medida puede resultar perjudicial en términos de eficiencia para la administración de justicia (enormes costos para el depósito de las computadoras y un colapso de los laboratorios forenses) y perjudicial para terceros que pueden ver paralizada la actividad de una empresa cuando quizá la evidencia buscada estaba en una sola computadora y podía obtenerse con una medida de menor coerción. Otra posibilidad es realizar copias seguras de los datos contenidos en los diferentes soportes físicos para evitar tener que secuestrar las máquinas e incluso de esta forma evitar causar mayores perjuicios a terceros (medida que puede ser costosa y demandar mucho tiempo de trabajo). Una tercera posibilidad "intermedia" entre el secuestro de todo el material y la copia forense, hoy muy utilizada y que ha demostrado ser beneficiosa en términos prácticos, es el proceso técnico denominado *triage*que permite utilizar herramientas especiales de informática forense para hacer búsquedas simples para determinar cuáles de los soportes informáticos pueden contener datos de relevancia para la investigación y así evitar tener que secuestrar mayor cantidad de elementos de los necesarios. Esta última metodología puede generar algún tipo de duda sobre su legitimidad al no estar prevista expresamente en la legislación procesal. Según creo, no existiría inconveniente si esta técnica es utilizada solamente como una forma de búsqueda o registro sencilla de datos. El problema legal aparece si lo que se inicia como una simple búsqueda se transforma, en los hechos, en una verdadera operación técnica que por sus características constituye un acto pericial en el que no se respetan las normas previstas en el ordenamiento procesal, especialmente la participación de la defensa. Para evitar este problema (que no trato en profundidad porque excede los objetivos de la presente investigación), resulta aconsejable trabajar con técnicas de bloqueo de escritura sobre los medios de almacenamiento de información para garantizar que no se altera el contenido del soporte físico que es objeto de análisis a fin de garantizar que frente a cualquier duda o impugnación la medida sea un acto reproducible en términos procesales.

[36] O sea que la verdadera tarea de búsqueda se realizará en un laboratorio y no en el lugar en que se encontró el dispositivo que se secuestra. Esta diferencia ha llevado a que, en la práctica, los límites entre las operaciones técnicas de registro y la pericia se tornen más difusos.

está alojada. Generalmente esto requerirá el allanamiento de un lugar físico (domicilio particular, oficina, etc.) o el secuestro de un soporte de almacenamiento digital luego de una requisa personal conforme a las normas procesales que lo regulan para luego poder realizar un análisis forense sobre los soportes informáticos así obtenidos. Es quizá por este motivo que a veces existe una confusión entre los supuestos procesales de habilitación del allanamiento y requisa pergeñados para el espacio y elementos físicos y el posterior registro y secuestro de datos alojados en los soportes físicos a los que el Estado accede mediante estas habilitaciones legales. Cuando en realidad se trata de dos pasos diferentes, por un lado, la obtención del soporte físico donde los datos están alojados (por ejemplo, el secuestro de una computadora o un disco rígido en el marco de un allanamiento) y, por el otro, las tareas de búsqueda y secuestro de datos en los soportes secuestrados, tarea que incluso puede ser que se realice en un laboratorio forense tiempo después y no en el mismo acto del allanamiento[37].

Sin embargo, este esquema de obtención de datos informáticos en dos etapas diferenciadas que comprenden 1. El secuestro del soporte físico o la copia forense realizada con acceso directo al soporte físico y 2. posterior búsqueda de datos mediante técnicas de informática forense aplicadas sobre el soporte previamente secuestrado o la copia forense obtenida durante el allanamiento, parece ingresar en un proceso de cambio siguiendo nuevas posibilidades que ofrecen las tecnologías informática y de las telecomunicaciones (TIC). Así han surgido nuevos instrumentos tecnológicos de búsqueda y secuestro de evidencia digital que permiten obtener importantes pruebas ya sea accediendo a distancia a información almacenada en diferentes equipos informáticos o capturando información que circula en internet sin necesidad de tener contacto o acceso físico a los elementos de almacenamiento (o sea sin que ningún funcionario esté presente en el lugar donde se encuentra el soporte físico donde los datos están almacenados). Consisten en programas informáticos capaces de interceptar en tiempo real y grabar datos transmitidos o recibidos a través de diferentes medios de comunicación electrónica (ello puede incluir tanto datos de contenido como datos de tráfico de comunicaciones e, incluso datos de geo-localización que permitan la ubicación geográfica de un dispositivo). Estos novedosos programas permiten también obtener *a distancia* datos de archivos almacenados en la memoria de los equipos sometidos a una medida de investigación sin necesidad de tener ningún tipo de contacto físico con ellos. Estos nuevos programas implican un cambio sustancial en la forma de obtener datos que se encuentran alojados en un soporte informático que ponen en crisis la aplicación para estos supuestos de las normas tradicionales previstas en los códigos procesales penales tanto para el registro y secuestro de cosas físicas como para la intercepción de comunicaciones. Se trata de un nuevo mecanismo

---

37 Ver el trabajo de Kerr, Orin S., *Searches and Seizures in a Digital World*, publicado en Harvard Law Review, nro. 119, año 2005, págs. 531-585.

de acceder a la información contenida en soportes informáticos que, por sus características tecnológicas, parece no encajar en ninguna de las normas que prevén los medios de prueba tradicionales lo que ha llevado a algunos autores a caracterizarlos como medios de investigación *híbridos*[38].

Esta posibilidad de recurrir a estas herramientas de análisis forense a distancia, es considerada por diversos órganos de investigación en el mundo que reclaman eficacia de las investigaciones, poder acceder a evidencia digital de manera remota y, fundamentalmente, secreta. Es por ello que las fuerzas de seguridad (autoridades policiales especializadas en investigaciones en entornos digitales y organismos especiales de investigación de delitos complejos como unidades antiterroristas u organismos de inteligencia) como algún sector de la doctrina y la jurisprudencia, han intentado justificar la viabilidad de su utilización, incluso sin regulación legal específica que las prevea, generalmente asimilándolas a la intervención de comunicaciones o bajo el resguardo del allanamiento de domicilio.

Estos argumentos han sido esgrimidos para *eludir* los límites impuestos por las garantías constitucionales de los diferentes países y aceptados universalmente en las convenciones internacionales de Derechos Humanos más importantes. Lo que ha provocado un intenso debate que ha estado presente en la agenda de organismos internacionales y que generó algunos antecedentes normativos y también jurisprudenciales en países en los que se conoció formalmente la utilización de estos mecanismos de investigación[39].

a) Organismos internacionales

➢ *Unión Europea*

La idea de implementar estos medios de investigación está presente en recomendaciones y resoluciones adoptadas en el seno de la Unión Europea. En el año 2008, el Consejo de Ministros de la UE adoptó un documento de Estrategias para fortalecer las reglas para la lucha contra los delitos informáticos que contenía la recomendación de adoptar diversas medidas procesales para fortalecer las investigaciones en los delitos informáticos. Entre ellas recomienda una mejor cooperación entre las policías de los diferentes países y las empresas del sector privado sobre mecanismos de investigación, una respuesta rápida a los requerimientos de cooperación y recursos y herramientas para accesos remotos. Sin embargo, el anuncio oficial no estuvo

[38] Salt, tesis doctoral, p. 35.

[39] Tratados por Salt, Marcos G. en su tesis doctoral, que seguimos en este capítulo.

acompañado de un detalle de a qué medidas concretas se refiere ni en qué supuestos se utilizaría.

Posteriormente en la Directiva 2011/92/EU, del Parlamento Europeo y el Consejo de Ministros de la Unión Europea[40] sobre el combate contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil, se prevén una serie de fuertes medidas procesales entre las que se incluyen las técnicas de vigilancia electrónica encubierta que ha permitido a un sector de la doctrina interpretar que alcanzan a las técnicas de *remote forensic* a las que hacemos referencia en este capítulo de la investigación[41].

➢ *El proyecto de legislación modelo de los países del Caribe*

El proyecto HIPCAR denominado "Por una mayor competitividad en el Caribe a través de la armonización de las políticas de TIC, Legislación y Procedimientos Regulatorios" fue lanzado en diciembre de 2008 por la Unión Internacional de Telecomunicaciones (UIT) y la Unión Europea y contó también con la colaboración de CARICOM Secretaría de la Comunidad del Caribe y la Unión de Telecomunicaciones del Caribe (CTU). El proyecto incluyó entre sus actividades la elaboración de recomendaciones para una legislación modelo sobre la ciber-delincuencia, modelo normativo que incluye tanto normas de derecho penal de fondo como de proceso penal tendente a la obtención de evidencia digital. El resultado alcanzado por el proyecto ha sido reconocido por la doctrina como uno de los modelos normativos más completos sobre la materia[42].

Entre sus propuestas en materia procesal prevé la utilización de técnicas de *remote forensic* como herramientas de investigación. Así, en la Sección 27, sugiere a los países la adopción de una norma a nivel nacional que prevea estas técnicas de investigación previendo la excepcionalidad de la medida y un uso restrictivo atendiendo a la potencialidad de afectación a la intimidad que

---

[40] Directiva del Parlamento Europeo 2011/92/EU del 13 de Diciembre del año 2011, disponible en español en http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32011L0093&from=ES

[41] Artículo 27: "Los responsables de la investigación y del enjuiciamiento de las infracciones contempladas en la presente Directiva deben disponer de unos instrumentos de investigación eficaces. Entre estos instrumentos podrán figurar la interceptación de comunicaciones, la vigilancia discreta, incluida la electrónica, el control de cuentas bancarias y otros medios de investigación financiera, teniendo en cuenta, entre otras cosas, el principio de proporcionalidad y la índole y gravedad de las infracciones que se estén investigando. Cuando proceda y de conformidad con el Derecho nacional, entre dichos instrumentos podrá encontrarse también la posibilidad de que los servicios de seguridad utilicen una identidad oculta en Internet"

[42] Texto completo de la propuesta normativa en su idioma original disponible en https://www.itu.int/en/ITU-D/Cybersecurity/Documents/HIPCAR%20Model%20Law%20Cybercrimes.pd

significa su uso[43]. De hecho, advirtiendo la resistencia que este tipo de medidas puede provocar por su fuerte intromisión en garantías individuales, prevé que la norma propuesta en el modelo normativo regional sea facultativa para los países[44].

Asimismo, la ley modelo, prevé que este tipo de medidas sean aplicables solamente a un grupo de delitos que deja librado a la decisión de cada país, la necesidad de autorización judicial, el requisito de justificar que no es posible obtener los datos buscados mediante otros mecanismos procesales y una duración limitada de la medida.

b) La discusión en países centrales

➢ *EEUU*

Un primer antecedente que fue objeto de análisis por parte de la jurisprudencia norteamericana (cubierto ampliamente por los medios de prensa) se refiere a la utilización en una investigación penal de un dispositivo (compuesto de *hardware* y *software*) de los denominados *keyloggers* que permitía grabar toda

---

[43] 27. (1) Si, … un [juez] [magistrado] considera que en la investigación de un delito enumerado en el párrafo 5 infra existen motivos razonables para creer que no pueden recabarse pruebas fundamentales por medio de otros instrumentos indicados en la Parte IV, y que dichas pruebas son razonablemente necesarias para la investigación penal, el [juez] [magistrado] [podrá/ deberá] autorizar, previa solicitud, a utilizar software forense con la finalidad específica que requiera la investigación e instalarlo en el sistema informático del sospechoso con el fin de obtener las pruebas pertinentes. La solicitud deberá contener la siguiente información: (a) identificación del sospechoso del delito, con nombre y domicilio si resulta posible, (b) una descripción del sistema informático que será objeto del procedimiento, (c) una descripción del objetivo de la medida, su alcance y duración (d) motivos que justifican recurrir a este procedimiento.
(2) En el marco una investigación de estas características, es necesario garantizar que la modificación del sistema informático que es objeto de la medida se limita a lo estrictamente necesario para la investigación y que dicha modificación pueda ser revertida una vez concluida la investigación. Durante la investigación se habrá de registrar: (a) el mecanismo técnico utilizado y la hora y fecha de su aplicación; (b) la identificación del sistema informático y las modificaciones introducidas en el marco de la investigación; y c) toda la información obtenida
La información obtenida mediante este software debe protegerse contra cualquier alteración, supresión o acceso no autorizados.
(3) la duración de la autorización estipulada en la sección 27 1) se limita a [3 meses]. Si se dejaran de cumplir las condiciones de la autorización, se detendrá inmediatamente el procedimiento.
(4) la autorización de instalar el software comprende el acceso a distancia al sistema informático del sospechoso.
(5) Si el proceso de instalación requiere el acceso físico, se habrán de cumplir lo estipulado en la sección 20.
(6) En caso de resultar necesario … (el encargado de la medida) podrá, en virtud de la orden judicial concedida, solicitar que al juez que exija la colaboración del proveedor de servicios en el proceso de instalación.
(7) [Lista de delitos]
(8) El país podrán tomar la decisión de no aplicar la sección 27

[44] ver punto 8 de la Sección 27 citada en nota anterior.

la actividad del teclado de la computadora del sospechoso y enviar la información al sistema del FBI. Los hechos del caso, sucintamente, fueron los siguientes: El FBI investigaba a un sospechoso de integrar la mafia y dedicarse a actividades de juego ilegal. Los investigadores tenían información de que el acusado tenía en su computadora información relevante de las actividades ilícitas pero que los archivos informáticos estaban encriptados y resultaba imposible acceder a ellos sin contar con la clave de desencriptación que, con un alto grado de posibilidad, sólo el acusado conocía (de hecho los investigadores habían obtenido con anterioridad una orden judicial que permitió revisar la computadora pero fue imposible acceder a la información buscada debido a las medidas de seguridad adoptadas por el sospechoso). Por ese motivo, el FBI solicitó al juez autorización para instalar un dispositivo (*hardware* y *software*) que permitiera grabar subrepticiamente la actividad del sospechoso en el teclado de la computadora para de esta manera obtener las claves de encriptación que protegían los archivos necesarios para la investigación. El juez emitió la orden que permitió realizar la medida de vigilancia y obtener finalmente las claves para acceder a los datos que, posteriormente, permitieron alcanzar una sentencia condenatoria. Se trató de un caso de un dispositivo instalado físicamente entre la computadora y el teclado y no de un caso de programa malicioso enviado vía internet.

La dificultad que puede presentar la instalación *física* de estos dispositivos sumado a las crecientes posibilidades de internet dio paso a mecanismos más sofisticados que permitieron la instalación de programas espías a distancia (sin necesidad de acceder físicamente al *hardware*). Así, ya en el año 2001 fue ampliamente discutido el caso del denominado *proyecto linterna mágica* del FBI. Consistía en un programa espía para investigaciones en internet que permitía grabar todo lo que marca un usuario en los teclados de computadora que eran objeto de investigación. El programa puede ser instalado subrepticiamente y a distancia mediante internet ya sea por la apertura de un archivo enviado adjunto a un mail o aprovechando vulnerabilidades de seguridad en del sistema informático que es objeto de investigación.

En el año 2007, el tema de la utilización de programas espías por parte del Estado fue puesto en el tapete nuevamente en EEUU por un proyecto continuador del anterior. La herramienta denominada CIPAV (*Computer and Internet Protocol Address Verifier*) permite el rastreo de comunicaciones en las que se utilizan mecanismos diseñados para permitir el anonimato. Como el programa es secreto, sólo existe información limitada tanto sobre sus alcances y objetivos como sobre sus especificaciones técnicas. Sin embargo, se conocen los casos en los que el *programa espía* fue utilizado con autorización judicial que requirió, previamente, que las solicitudes del FBI incluyeran descripciones de funcionalidades del programa CIPAV lo que permite identificar muchas de sus

características y los datos informáticos que el programa permite obtener en la computadora que es objeto de registro. Así ha sido admitido que el programa malicioso permite obtener datos[45], de acuerdo a una declaración jurada realizada por el FBI para obtener la orden judicial que permitió su utilización en un caso (según la publicación WIRED News -traducción propia-). Una vez recopilados los datos, el CIPAV comienza un monitoreo secreto del uso de la computadora, registrando cada dirección IP a la que se conecta la máquina. Toda esta información se envía a través de Internet a un ordenador del FBI en Virginia, probablemente ubicado en el laboratorio técnico del FBI en Quantico. Esta información, de acuerdo a lo informado por el FBI, en ningún caso implicaría el acceso al contenido de las comunicaciones por lo que fue aceptado jurisprudencialmente que la expectativa de privacidad sobre estos datos es menor y es posible obtenerlo sin los mismos requisitos necesarios para la intervención del contenido de comunicaciones.

En la doctrina norteamericana, autores importantes[46] han sostenido la posibilidad de utilizar válidamente programas de acceso remoto de datos siempre que se cumpla con los requisitos de la cuarta enmienda[47], esto significa que han entendido que pueden aplicarse por *analogía* las normas y jurisprudencia que regula el registro y secuestro tradicional permitiendo órdenes de *allanamiento* (registro y secuestro de datos) que prevean la obtención de datos a través de estos mecanismos de acceso remoto a computadoras.

El FBI ha insistido siempre en la necesidad de políticas de uso más agresivas de estas tecnologías que permiten el acceso remoto a datos informáticos, especialmente la posibilidad de que estas medidas se puedan aplicar de forma transfronteriza (o sea, sin respetar los límites territoriales que delimitan la jurisdicción del juez que ordena la medida) y sin necesidad de identificar de manera concreta el dispositivo informático que es objeto de la medida. Ha realizado diferentes propuestas y presentado casos prácticos en los cuales la imposibilidad de usar este tipo de herramientas ha significado perdida de

---

[45] Dirección IP, Dirección MAC, Una lista de puertos TCP y UDP abiertos, Una lista de programas en ejecución, El tipo de sistema operativo utilizado y su versión y número de serie, El navegador de Internet utilizado y su versión, El usuario registrado en el sistema operativo y el nombre de empresas registradas, en su caso, el nombre del usuario que ha iniciado la sesión, La última URL visitada.

[46] Citados por Salt, Marcos G. en su tesis doctoral, p. 65, quienes no sólo analizan la relación con la garantía sino también el acceso interjurisdiccional estatal con diferentes estándares.

[47] Enmienda 4: "El derecho del pueblo a la seguridad en sus personas, casas, documentos y efectos contra perquisiciones y secuestros irrazonables no será violado, y no se expedirá ningún mandamiento sino en virtud de causa probable apoyada por juramento o afirmación y que describa con precisión el lugar que debe ser registrado y las personas o cosas que deben ser detenidas o secuestradas."

eficiencia de la investigación (por ejemplo, casos de pornografía infantil). Conforme a ello, el Departamento de Justicia, inició políticas formales para lograr los cambios normativos necesarios para habilitar que las órdenes judiciales que permiten utilizar programas de registro remoto de datos resulten válidas no solamente para la jurisdicción en las que se obtienen, sino que sirvan también para obtener datos en diferentes distritos como una manera de lograr mayor eficiencia en la persecución de delitos en internet. En el año 2013, el Departamento de Estado presentó una propuesta de modificación de la Regla 41 del procedimiento federal. Durante el año 2014, esta propuesta logró un avance significativo al obtener el apoyo del Comité de reglas y procedimientos de la conferencia Judicial de EEUU, lo que aumentaba las posibilidades de que fuera aprobado por la Corte Suprema y, si resultara necesario, por el Congreso. Finalmente, luego de un largo proceso de audiencias, la Corte Suprema de Justicia anunció en abril de 2016 la aprobación de la modificación de la Regla 41 (en vigencia en diciembre 2016) solicitada por el Departamento de Justicia, entendiendo que se trata sólo de una cuestión procedimental (motivo por el cual no requeriría el paso previo por el parlamento). Ello provocó oposición en organizaciones de la sociedad civil preocupadas por la defensa de los derechos en internet y la protección de datos personales y de importantes empresas del sector[48] que se han manifestado en contra de esta ampliación de las facultades del Estado, claramente peligrosas para las garantías individuales que pueden tener incluso problemas de ribetes internacionales en la medida en que signifiquen el envío de programas maliciosos o el acceso a computadoras ubicadas fuera de los EEUU. Las organizaciones protectoras de las libertades civiles han manifestado públicamente su rechazo resaltando que la medida permitirá a las autoridades encarar operaciones masivas de vigilancia con muy limitado control judicial pudiendo afectar la seguridad e intimidad incluso de

---

[48] Teóricamente, el mecanismo que permite modificar las normas a las cortes federales se limita a cuestiones meramente procesales. Quienes critican la resolución de la Corte han señalado que la modificación a la Regla 41 está lejos de ser una mera modificación procedimental y, antes bien, se trata de un cambio sustancial con implicancias en garantías constitucionales. Así ha sido resuelta la cuestión en el derecho norteamericano frente a medidas intrusivas de la intimidad como la intervención de comunicaciones. Las Organizaciones no gubernamentales preocupadas por la defensa de las libertades en internet han iniciado múltiples campañas para intentar frenar la entrada en vigencia del nuevo texto normativo. Ver a modo de ejemplo, la convocatoria pública de un grupo de organizaciones destinado a firmar solicitudes en contra de la modificación: "TAKE ACTION The U.S. government wants to use an obscure procedure—amending a federal rule known as Rule 41— to radically expand their authority to hack. The changes to Rule 41 would make it easier for them to break into our computers, take data, and engage in remote surveillance.These changes could impact any person using a computer with Internet access anywhere in the world. However, they will disproportionately impact people using privacy-protective technologies, including Tor and VPNs. The U.S. Congress only has until December 1st to stop the changes from taking effect. We need to speak out. Sign our petition and join our day of action".
Ver asimismo y a modo de ejemplo, el documento presentado por la empresa GOOGLE cuestionando la iniciativa remarcando tanto los problemas constitucionales como de geopolítica que estas medidas puede conllevar, file:///C:/Users/Marcos%20Salt/Downloads/13Feb2015_Google_Inc_Comments_on_the_Proposed_Amendment_to_Federal_Rule_of_Criminal_Procedure_41.pdf

personas totalmente ajenas a la comisión de un delito (además señalan que tal como está redactada la medida podría afectar también a los equipos informáticos de las víctimas y no sólo a los de los posibles autores.).

De acuerdo al texto normativo aprobado, un juez de una jurisdicción en la que ocurrió un delito podría dictar una orden de acceso remoto que podría alcanzar a sistemas informáticos en otras jurisdicciones (supuesto de acceso transfronterizo de datos) en dos supuestos: cuando no se conozca el lugar en el que la información está alojada por la utilización de algún software especial que permite la utilización de internet de manera anónima; en los casos de ataques a sistemas informáticos (18U.S.C 1030 (a) 5) que afecten a computadoras ubicadas geográficamente en cinco o más distritos. La modificación permite también que los jueces puedan reunir en una sola orden numerosas computadoras, aunque estén ubicadas en diferentes jurisdicciones evitando la necesidad que hasta ahora tenían los investigadores de identificar cada computadora particular que era objeto de la medida.

El nuevo texto de la Regla 41 agrega un requisito de *notificación* a la persona que es objeto del allanamiento a distancia, similar a la notificación prevista en los casos de allanamientos a espacios físicos. Así prevé en un agregado al artículo referido a la orden de allanamiento que, en los supuestos de ordenes en las que se prevea la utilización de software de acceso remoto para buscar, secuestrar o copiar información, el oficial a cargo de la medida debe realizar *esfuerzos razonables* para entregarle una copia de la orden de allanamiento a la persona cuya propiedad fue allanada o su información secuestrada o copiada. Sin embargo, llama la atención que el Comité que evaluó el tema decidiera no tratar el tema de los problemas constitucionales que esta nueva modalidad de allanamientos a distancia presenta, especialmente todo lo atinente a la vinculación con la cuarta enmienda de la Constitución de EEUU. Antes bien, expresamente señaló que los requisitos que debe tener este tipo de órdenes de allanamientos y los demás planteos constitucionales que el tema pueda implicar, se vayan resolviendo por el desarrollo de líneas jurisprudenciales, perdiendo de esta forma, una buena posibilidad de dotar de mayor certeza a la aplicación de estas medidas de prueba excepcionales.

- *Alemania. El nuevo derecho constitucional a la confidencialidad e integridad de los sistemas informáticos*

La cuestión de la utilización por parte del Estado de accesos remotos a sistemas informáticos como nueva técnica de investigación y obtención de evidencia para un proceso penal fue también objeto de análisis en Alemania, tanto en el ámbito académico como jurisprudencial, con precedentes judiciales de gran trascendencia tanto para el derecho interno de este país como para el derecho

comparado, especialmente en los países con sistemas jurídicos de tradición europea continental, como es el caso de nuestro país.

Sin perjuicio de que la doctrina ya había advertido sobre la utilización de estas formas de investigación que habían sido aceptadas por la jurisprudencia de tribunales inferiores, el primer precedente de importancia sobre el tema fue dictado por la Corte Federal el 31 de enero del año 2007[49]. Para el momento en que la Corte adoptó esta decisión, parte de la doctrina había postulado que resultaba posible utilizar legítimamente en el proceso penal estas técnicas de *registros* a sistemas informáticos mediante accesos remotos, básicamente, que era posible utilizar de manera analógica las disposiciones que regulan en el Código de Proceso penal alemán el registro y allanamiento de lugares físicos (art. 102 del CPP AlemánStPO). La Corte Federal, por el contrario, estableció en su resolución que, con las normas sobre registro y secuestros vigentes en aquel momento en Alemania, no resultaba válida la utilización de *software* de registro y secuestro de datos a distancia. En definitiva, reconoce que la utilización de estos mecanismos sin estar expresamente legislados resultaba ilegítima y desechó la posibilidad de aplicar por analogía tanto las normas previstas para el registro y secuestro de elementos físicos como las normas previstas para la intercepción de comunicaciones. Aunque no señala que estos mecanismos de investigación sean de por sí y de manera categórica contrarios al texto constitucional. Antes bien, deja abierta la posibilidad de que una regulación legal que cumpla con los requisitos constitucionales pueda habilitar la utilización de estos mecanismos de investigación en el futuro.

El caso se desarrolló de la siguiente manera: en el año 2006 un fiscal federal que llevaba adelante una investigación por terrorismo solicitó una orden judicial que le permitiera a la policía instalar de manera secreta un programa de vigilancia similar a un troyano en la computadora de un sospechoso. La solicitud pretendía obtener una orden judicial para realizar un registro y secuestro de datos de una computadora sin que sea necesario un allanamiento del domicilio en la que la computadora se encontraba físicamente. Esto es, realizar la medida *a distancia* valiéndose de las posibilidades de internet. El fiscal proponía utilizar una herramienta informática que se instalaría en la computadora objeto de investigación y permitiría copiar los datos almacenados para luego transferirlos mediante internet hasta la computadora de los investigadores para su posterior evaluación forense; el programa permitiría también copiar los datos existentes en la *memoria de trabajo de la computadora* con la finalidad de obtener claves y metadatos de comunicaciones que, de otra forma, se perderían cuando la computadora se apagara (por ejemplo, si se realizaba un allanamiento de morada tradicional), permitiría también copiar y enviar el

[49] Bundesgerichtshof. Corte Federal de justicia de Karlshrure. Cf. http://www.bundesgerichtshof.de, BGH, NJW, 2007, 930

tráfico de mails y la información sobre las páginas *web* visitadas. El fiscal argumentó que la información resultaba crucial para la investigación y presentó los elementos de sospecha que le permitían justificar que la información necesaria para su investigación podía estar almacenada en la computadora del sospechoso.

El juez rechazó el pedido del fiscal y éste presentó un recurso ante la Corte Federal. El eje central del recurso fiscal fue que los artículos 102[50] y 110[51] del Código procesal penal alemán –StPO-, aplicados por analogía, permitían realizar la medida solicitada, argumentando que existían similitudes entre el allanamiento para posterior registro y secuestro de cosas en espacios físicos y el acceso remoto a un sistema informático del sospechoso para su registro y secuestro de datos. Estas similitudes, según el fiscal permitían utilizar los programas de acceso remoto de datos aplicando los recaudos y garantías previstos en los arts. 102 y 110 como base legal.

La Corte confirmó la resolución que denegaba el pedido fiscal de utilizar el programa espía, sosteniendo que *la orden de registro no podía ser concedida ya que no estaba prevista en el ordenamiento procesal vigente la utilización de herramientas de análisis remoto forense de datos* (de lo que se colige que una modificación legislativa permitiría la utilización de estos programas). Se rechazó la posibilidad de analogía entre el registro tradicional de espacios físicos y los registros clandestinos de computadoras. Claramente, estableció que sin una ley procesal que expresamente prevea este tipo de medidas de investigación, no era posible ordenarlas sin incurrir en una extra limitación de poder.

Sin embargo, la resolución jurisprudencial más trascendente sobre el tema fue dictada por la Corte Federal Constitucional Alemana[52] el día 27 de febrero del año 2008, precedente de fundamental importancia tanto en Alemania como por su potencial influencia en el derecho comparado. En esta resolución reconoce un nuevo derecho fundamental constituido por la garantía a la *confidencialidad e integridad de la información en sistemas informáticos* como una derivación del derecho a la personalidad y la dignidad. Este nuevo derecho fundamental se orienta a la protección de los derechos de privacidad y personalidad de los ciudadanos en el ámbito de los sistemas informáticos y de comunicaciones.

Para la misma época en la que se producía el debate doctrinario y jurisprudencial al que hacíamos referencia en los párrafos anteriores, el Estado

---

[50] Regula el registro de espacios físicos

[51] Regula el registro y secuestro de documentos y dispositivos digitales.

[52] Bundes verfassungsgericht , BVerfG, NJW 2008, 822

de Nordrhein-Westfalen introdujo modificaciones en la denominada *Ley de la protección de la Constitución*[53]. Estas modificaciones legislativas reforzaban los poderes del servicio secreto denominado "Oficina federal de Protección de la constitución" creando una agencia especial para realizar tareas de inteligencia y otorgándole facultades para realizar accesos encubiertos a sistemas informáticos y monitoreo secreto de las comunicaciones en internet (búsquedas e intercepciones de comunicaciones realizadas vía internet). La modificación se introdujo en el artículo 5.2 numeral II de la mencionada Ley. Así el texto normativo otorgaba facultades para la observación y la investigación secreta en Internet, especialmente la intercepción secreta de comunicaciones a través de Internet y el acceso secreto a sistemas informáticos tanto mediante programas que permiten la vigilancia a distancia como autorizando el uso de dispositivos físicos que permiten acceder y obtener datos de manera subrepticia del sistema informático que se quiere investigar. El texto normativo preveía dos habilitaciones legales diferenciadas. Por un lado, la posibilidad de realizar tareas de monitoreo e intercepción de datos en las comunicaciones normales de internet, datos de chats *on line*, acceder a páginas restringidas mediante contraseñas obtenidas previamente, etc., por el otro, medidas directas de acceso a sistemas informáticos mediante programas troyanos; *troyanos federales*, instalados a distancia o logrando un acceso físico subrepticio directo en las computadoras investigadas (o sea casos de infiltración técnica aprovechando fallos de seguridad del sistema que es objeto de investigación o instalando programas espías). La enmienda legislativa daba, de esta manera, la base legal para las búsquedas secretas *a distancia* en la computadora de un sospechoso por parte de la denominada Agencia de Protección Constitucional. Así, parecía que podía superarse el escollo planteado en la sentencia a la que antes hicimos referencia ya que una ley formal autorizaba la utilización de estos novedosos medios de investigación superando las objeciones sobre la posible aplicación por analogía de las normas sobre registro y secuestro de espacios físicos.

Sin embargo, un recurso de amparo constitucional presentado (por personas que no eran investigadas por terrorismo) en contra de esta enmienda[54] motivó

---

53 En su idioma original, "Verfassungsschutzgesetz". La modificación de la ley se sancionó del 30 de diciembre de 2006.

54 La demanda de inconstitucionalidad fue presentada por personas que, si bien no estaban alcanzados por la normativa ya que no estaban siendo investigados por actividades ilegales de terrorismo, podían verse afectados en sus derechos como consecuencia de sus actividades profesionales que podían llevar al Estado a realizar allanamientos en línea de sus computadoras por error. Concretamente, uno de los demandantes es un periodista que por sus investigaciones accedía de manera regular a páginas y chats vinculados a actividades extremistas, otro un miembro de un partido político bajo observación por parte de la oficina a la que la ley otorgaba los poderes especiales y el último un abogado que asistía a asilados políticos, alguno de ellos bajo observación de la oficina de control. En todos los casos, los demandantes alegaron que usaban sus computadoras con fines laborales y personales al mismo tiempo justificando de esta manera la afectación a su ámbito de intimidad personal.

que la nueva ley sea analizada por el Tribunal Constitucional Federal Alemán (Bundesverfassungsgericht).

El Tribunal Constitucional analizó el tema en profundidad atendiendo no sólo a las aristas jurídicas sino también a aquellas cuestiones de índole tecnológica que resultaba importante comprender para resolver los temas constitucionales planteados por los demandantes (lo que acredita la necesidad de análisis multidisciplinario). En este proceso de estudio, el Tribunal celebró audiencias públicas y convocó como expertos a reconocidos académicos tanto del ámbito jurídico como de las ciencias informáticas y especialistas en protección de datos personales, incluso fue convocado un reconocido *hacker* (Andreas Bogk, miembro de Chaos Computer, una de las organizaciones de *hackers* más influyente a nivel mundial).

El Estado alemán, convocado como demandado, presentó dos repuestas diferentes, una por parte del gobierno regional de North Rhine Westphalia del cual había surgido la ley en cuestión y otra del Estado federal. Ambas posturas partían de un argumento común: tratar de asimilar las facultades de utilizar técnicas de *remote forensic* a poderes procesales de investigación policial en el mundo físico y, por ende, afirmar la posibilidad de utilizar por analogía normas existentes para la obtención de evidencia física a la obtención de evidencia digital mediante estas técnicas de acceso remoto. El Estado regional identificó a la garantía de la privacidad de las telecomunicaciones como la más cercana a las medidas en discusión, entendió que las técnicas de acceso remoto son sólo formas de intercepción de comunicaciones y que, por lo tanto, las normas que regulan las garantías para este tipo de intromisión en la esfera de garantías son aplicables para esta nueva modalidad de investigación, pues las medidas de investigación mediante los programas troyanos funcionan siempre con una comunicación de la computadora que es objeto de la medida en internet que permite la transmisión de los datos. El Estado Federal por su parte, argumentó que las normas previstas para garantizar la inviolabilidad de domicilio resultaban las más cercanas y análogas y, por tanto, el marco adecuado para cubrir las garantías necesarias para poder hacer uso de las técnicas de acceso remoto a sistemas informáticos.

El Tribunal Constitucional Federal decidió el 27 de febrero de 2008 que el artículo 5, párrafo II 11 de la Ley de Protección de la Constitución de Nordrhein-Westfalen no estaba de acuerdo con la Constitución y, por lo tanto, resultaba

inconstitucional (BVerfG, NJW 2008, 822)[55]. La resolución fue sorpresiva por sus argumentos, en tanto no estaba basada en la aplicación y extensión de los alcances de los precedentes del alto tribunal sobre registro y secuestros en ámbitos físicos al ámbito digital. En cambio, reconoció (creando de esta manera jurisprudencialmente) un nuevo derecho fundamental que protege la intimidad y los derechos personales de los ciudadanos vinculados a las tecnologías de la información y las comunicaciones. La decisión se basó precisamente en el reconocimiento de este *nuevo* derecho fundamental, el derecho humano a la confidencialidad y la integridad de los sistemas de tecnología de la información. El tribunal en su razonamiento deriva esta nueva garantía, de los derechos fundamentales de la dignidad personal y los derechos de la personalidad reconocidos en los artículos 2 I en relación con el 1 I de la Constitución Federal Alemana (Grundgesetz - GG). La sentencia toma como premisa argumental fundante de su conclusión, que las garantías constitucionales y legales derivadas del *derecho al secreto de las comunicaciones* y aquellas derivadas de la *inviolabilidad del domicilio*, no habían tomado en cuenta la influencia de las tecnologías informáticas con relación a la necesidad de protección de la intimidad, situación que se extiende a la jurisprudencia y que produce una laguna que el tribunal constitucional pretende llenar con su resolución.

El tribunal analizó la insuficiencia de la protección constitucional del domicilio privado para este tipo de medidas de investigación ya que la garantía de inviolabilidad de domicilio resulta inapropiada para una computadora que no entra en el concepto tradicional de domicilio y dejaría limitada la garantía sólo a los casos en los que haya sido necesario ingresar a un domicilio para la instalación de programas espía. Así, el tribunal analizó la garantía de inviolabilidad de domicilio tal como está prevista en la Constitución alemana, como un límite a la intrusión del Estado fijando de manera expresa las condiciones en las que se permite al Estado afectaciones a la garantía, excepciones posteriormente reguladas en las leyes procesales que no pueden apartarse de las pautas fijadas constitucionalmente. El Tribunal Constitucional responde el argumento del Gobierno Federal que pretendía que el registro de una computadora a distancia podía equipararse al registro de un domicilio marcando las características técnicas de estos novedosos programas de investigación que justifican la imposibilidad de una aplicación analógica directa

---

[55]El texto original en alemán disponible en dejure.org/dienste/vernetzung/rechtsprechung?Text=NJW 2008, 822 Cf. El reporte de prensa de la Corte constitucional 22/2008 del 27 de Febrero del 2008, en su idioma original y en ingles: Federal Constitutional Court –press office- "Previsions in the North-RhineWestphaliaConstitutionProtectionAct (VerfassungsschutzgesetzNordrhein-Westfalen) on online searches and o there connaissance of the Internet null and void" disponible en http://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2008/bvg08-022.html. El texto completo del fallo en inglés disponible en http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2008/02/rs20080227_1bvr037007en.html

de estas normas. De esta manera, destacó la importancia del mundo digital para los ciudadanos de hoy y la posibilidad de que los troyanos instalados por el Estado puedan alcanzar a sistemas informáticos fuera del domicilio protegido o, incluso, que una vez instalado un programa espía, registre datos generados fuera del domicilio como podría ocurrir en el caso de que la medida recayera en un dispositivo portátil como una *laptop* o un teléfono móvil inteligente.

De acuerdo con la resolución, tampoco serían aplicables las garantías derivadas del derecho al secreto de las comunicaciones previstas en el artículo 10.1 de la Ley fundamental alemana a la protección a los ciudadanos frente a estas medidas de investigación remota. El fallo destaca que estas medidas de investigación no se dirigen a conocer el contenido de una comunicación particular en curso (o por lo menos, no se limita a ello) sino a penetrar o acceder a distancia un dispositivo informático con el fin de inspeccionar elementos contenidos en él. Admite parcialmente el argumento del Estado regional solamente para los casos en que las técnicas son usadas para interceptar una comunicación, pero no resultan aplicables las normas de garantías previstas para la intercepción de comunicaciones cuando son usadas para registrar un sistema informático y obtener datos almacenados en el sistema informático, aunque una comunicación sea la que permite enviar esos datos a la autoridad que ordenó la medida.

En el fallo resulta también de sumo interés la aplicación del principio de proporcionalidad. En este sentido, la resolución afirma que esta nueva derivación del derecho a la intimidad sólo puede ser restringida cuando otros derechos fundamentales de valor más alto como la vida estén en inminente peligro por lo que el uso de herramientas de investigación como los programas espías a distancia por los organismos encargados de hacer cumplir la ley sólo podría ser utilizado en estos supuestos, siempre con autorización judicial otorgada de manera específica caso por caso y no de manera general y abierta. Aunque el fallo deja abierta la posibilidad de la utilización de los programas para prevenir por ejemplo un ataque terrorista inminente, no podría utilizarse para investigar retrospectivamente uno ya sucedido, ni para la prevención general de los actos de terrorismo, sino existen elementos de prueba suficientes de una amenaza específica, inminente y claramente identificados.

La trascendencia de este fallo del Tribunal Constitucional es indiscutible no sólo para el derecho alemán sino para el derecho comparado en el que la jurisprudencia constitucional alemana tiene gran influencia. De hecho, sentó las bases para la legislación que posteriormente sería sancionada receptando los registros de sistemas informáticos en línea; la Ley Alemana de defensa contra los peligros del terrorismo internacional (25 de diciembre de 2008) que introdujo nuevas potestades de investigación entre las que se encuentra el

acceso secreto y remoto a sistemas informáticos. La ley claramente establece que sólo se podrán utilizar en casos de terrorismo internacional y organizaciones criminales terroristas.

➢ *Italia*

En Italia, aun contando con una legislación procesal moderna que prevé medidas especiales para la obtención de evidencia digital, sancionada para cumplir con los requisitos de la Convención de Budapest, no existe aún una norma procesal expresa que regule de manera clara atendiendo a todas las características técnicas y posibilidades que pueden brindar los programas que permiten la posibilidad de accesos remotos a sistemas informáticos utilizando programas troyanos con fines de investigación. Sin perjuicio de ello, este tipo de técnicas han sido utilizadas e, incluso, han sido avaladas en algunos casos por la Corte de Casación.

Así, en una primera resolución sobre el tema[56], sumamente criticada por la doctrina italiana especializada, la Corte de casación italiana admitió la legitimidad de estas medidas. En la resolución, la Corte confirma la legitimidad de la utilización de un programa espía por parte de la fiscalía sin control judicial previo, ni recaudos especiales que tengan en cuenta el alto poder de intromisión en las garantías individuales. Admite la validez de la utilización de un denominado *software fantasma* para obtener copia de datos digitales almacenados en la computadora de un imputado ubicada en una oficina pública (por ello no se aplicaba la protección del domicilio). Aún peor, en términos de una adecuada protección de las garantías frente a la vigilancia estatal, el programa espía fue instalado de acuerdo a la orden emitida por el Ministerio Público Fiscal sin previa autorización judicial haciendo uso de la habilitación legal prevista en el artículo 234 del código de procedimiento penal pergeñado por el legislador para la obtención de documentos físicos sin necesidad de autorización judicial cuando la legislación italiana cuenta con normas que, si bien no habilitan legalmente la utilización de técnicas de acceso remoto de manera expresa, se acercaban más a su significado técnico al referirse a la intervención de comunicaciones electrónicas (artículo 266 bis) y al registro y secuestro de dispositivos electrónicos. El programa espía instalado permitía la obtención no solamente de los archivos ya existentes sino también de los que se produjeran e ingresaran en el sistema informático en el futuro que el programa podía copiar y enviar periódicamente la información obtenida a los organismos a cargo de la investigación. Lo cierto es que la medida permitió en los hechos la vigilancia subrepticia del sistema informático del sospechoso durante ocho meses sin control judicial. La Corte entendió que no era necesario aplicar las

[56] Cf. Cass. Pen., SezV , 14 de octubre del año 2009. N. 16556 (caso Virrusso).

normas (y garantías) de una intervención de comunicaciones porque solamente tenía por objeto obtener datos ya almacenados en el pasado y, en términos técnicos esto constituía un *flujo de datos en una sola dirección* contenida en los circuitos internos de la computadora. En la misma sentencia, la Corte estableció que la medida no es una medida irreproducible y, por lo tanto, no deben aplicarse las regulaciones y garantías previstas para este tipo de medidas, entendiendo que al estar *copiando los datos* no se produce su alteración y la medida puede reproducirse. De esta manera, para la Corte italiana, la medida podría realizarse sin comunicar ni hacer participar a la defensa ya que de ser necesaria la utilización de la prueba en el proceso podría repetirse la medida en las mismas condiciones.

Sin embargo, en un caso posterior[57], la Corte ratificó la invalidez de evidencia obtenida mediante otra técnica de vigilancia electrónica por permitir la búsqueda de datos de manera indiscriminada, más allá del objeto procesal de causas determinadas.

La doctrina italiana ha resaltado en los últimos años la necesidad de una regulación específica que prevea las diferentes formas en que estos programas espías permiten obtener evidencia para un proceso penal.

➢ *España*

En España, luego de un largo de debate enmarcado en la discusión más amplia sobre la necesidad de reformar la *vieja* Ley de Enjuiciamiento Penal en general y, de manera particular, sobre la necesidad de incorporar normas que regulen la obtención de evidencia digital (obligación asumida por España al adherir a la convención de Budapest), se aprobó una importante modificación en el Código Procesal Penal[58]. El acceso remoto a sistemas informáticos como medida procesal para la investigación en causas penales ya había sido evaluado en proyectos legislativos anteriores sin éxito. Una fuerte resistencia de sectores de la prensa y la sociedad civil había hecho naufragar esta pretensión originada especialmente en pedidos de las unidades especializadas en la persecución penal de los delitos informáticos. Finalmente, la medida de acceso remoto a sistemas informáticos fue incorporada con esta última reforma legislativa surgida, de acuerdo al texto de la exposición de motivos, de la necesidad de modificar aspectos de la Ley de Enjuiciamiento que no pueden esperar la reforma integral que está aún en proceso de discusión.

---

[57]Caso Reynair Cass., sez. IV, 17 Aprile 2012, n. 19618, in Cass. pen., 2013, p. 1523 ss.

[58] Ley Orgánica 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, publicada en el Boletín Oficial del Estado BOE, 239, el 6 de octubre del año 2015

La nueva ley resulta interesante pues ya el título denota la intención (por lo menos la expresada) del legislador: "fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica". La ley es vislumbrada ya desde el título y el texto del Preámbulo como reguladora de garantías antes que como generadora de importantes poderes procesales para el Estado en su rol de persecución penal que, en los hechos, de todas maneras, instituye. Se trata de un interesante enfoque legislativo en el que la regulación es encarada atendiendo especialmente a la jurisprudencia desarrollada por los tribunales superiores españoles y el Tribunal Europeo de Derechos Humanos durante el largo período en el que este tipo de medios de investigación fue utilizado por el Estado sin base legal expresa.

Así el artículo 7 de la ley innova con un Título especial de la Ley de Enjuiciamiento que engloba las medidas de investigación limitativas de los derechos reconocidos en el artículo 18 de la Constitución Española[59]. Regula en conjunto en un Capítulo de la ley[60] aquellas incumbencias permitidas para el Estado (medidas limitativas de los derechos permitidas al Estado) en el ámbito de una persecución penal fijando también los límites y las garantías de los ciudadanos frente a esta actividad estatal en relación a los derechos a la intimidad, inviolabilidad de domicilio, secreto de las comunicaciones e intimidad y honor frente al tratamiento de datos informáticos.

En lo que respecta al tema de esta parte de la investigación, el artículo 13 de la ley crea un nuevo capítulo dedicado especialmente a establecer disposiciones comunes que regulen la interceptación de las comunicaciones telefónicas y telemáticas, la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, la utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen, el registro de dispositivos de almacenamiento masivo de información y *los registros remotos sobre equipos informáticos*.

El capítulo comienza con un artículo que establece condiciones generales para todas las medidas que contiene, estableciendo condicionamientos generales

---

[59] Artículo 18:
"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".

[60] Título VIII del Libro II "De las Medidas limitativas de los derechos reconocidos en el artículo 18 de la constitución".

para admitir la limitación de los derechos contenidos en el artículo 18 del texto constitucional. Así prevé la necesidad de autorización judicial mediante resolución en la que se fundamente adecuadamente el cumplimiento de los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida[61]. Los puntos siguientes del mismo artículo, regulan de manera minuciosa los requisitos que deben reunir las solicitudes de este tipo de medidas que realice la policía judicial o el ministerio público (art. 588 bis b.), el contenido de la resolución que las acuerde o deniegue (588 bis c.), el secreto de las actuaciones en las que se discute la habilitación de las medidas (588 bis d.), duración de las medidas y posibles prórrogas como así también la posibilidad de que el juez decida el cese de la medida cuando cambien las circunstancias que determinaron su orden o no esté dando resultados esperados (588 bis e, f y j), control general judicial de la ejecución de la medida (588 bis g), la posibilidad de que alguna de estas medidas afecte a terceras personas ajenas a la investigación (588 bis h) y todo lo atinente a la destrucción de los registros cuando finalice la tramitación de la causa (588 bis k). Especial mención merece la norma que prevé la utilización de datos obtenidos durante la ejecución de estas medidas en otras investigaciones, o sea los datos obtenidos que nada tienen que ver con el objeto procesal que habilitó la medida pero que proveen información sobre la posible comisión de otro delito que, conforme a lo regulado, se podrán utilizar previo analizar la

---

61 "Artículo 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
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."

legitimidad de la injerencia en el proceso original y la razonabilidad del encuentro casual[62].

En lo que se refiere específicamente al registro remoto de equipos informáticos, la ley enmarca esta nueva forma de investigación en la regulación más amplia del registro de dispositivos informáticos de almacenamiento masivo. Sin embargo, advirtiendo su mayor alance y potencial vulneración de la intimidad personal[63], genera mayores recaudos y garantías especiales frente a esta medida procesal. En primer lugar, la nueva Ley prevé que la medida sólo podrá ser utilizada en la investigación de un grupo limitado de delitos:

Artículo 588 septies a. Presupuestos.1. El juez competente podrá autorizar la utilización de datos de identificación y códigos, así como la instalación de un software, que permitan, de forma remota y telemática, el examen a distancia y sin conocimiento de su titular o usuario del contenido de un ordenador, dispositivo electrónico, sistema informático, instrumento de almacenamiento masivo de datos informáticos o base de datos, siempre que persiga la investigación de alguno de los siguientes delitos:
a) Delitos cometidos en el seno de organizaciones criminales.
b) Delitos de terrorismo.
c) Delitos cometidos contra menores o personas con capacidad modificada judicialmente.
d) Delitos contra la Constitución, de traición y relativos a la defensa nacional.
e) Delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación.
Llama la atención el inciso *e)* del artículo ya que de la simple lectura de su texto parece desprenderse que puede habilitar la utilización de esta medida en la investigación de delitos de menor envergadura sólo por el hecho de que sean

---

[62] Art. 588 bis con remisión al art 579 sobre correspondencia epistolar y telegráfica: Artículo 579 bis: Utilización de la información obtenida en un procedimiento distinto y descubrimientos casuales.
1. El resultado de la detención y apertura de la correspondencia escrita y telegráfica podrá ser utilizado como medio de investigación o prueba en otro proceso penal.
2. A tal efecto, se procederá a la deducción de testimonio de los particulares necesarios para acreditar la legitimidad de la injerencia. Se incluirán entre los antecedentes indispensables, en todo caso, la solicitud inicial para la adopción, la resolución judicial que la acuerda y todas las peticiones y resoluciones judiciales de prórroga recaídas en el procedimiento de origen.
3. La continuación de esta medida para la investigación del delito casualmente descubierto requiere autorización del juez competente, para la cual, éste comprobará la diligencia de la actuación, evaluando el marco en el que se produjo el hallazgo casual y la imposibilidad de haber solicitado la medida que lo incluyera en su momento. Asimismo, se informará si las diligencias continúan declaradas secretas, a los efectos de que tal declaración sea respetada en el otro proceso penal, comunicando el momento en el que dicho secreto se alce"

[63] Ver preámbulo BOE 239, pág. 90197: "…Por lo que afecta al registro remoto (diligencia ya presente en buena parte de las legislaciones europeas) el intenso grado de injerencia que implica su adopción justifica que incluso se refuerce el ámbito objetivo de la medida, para lo que se han acotado con un listado numerus clausus los delitos que la pueden habilitar, y a que se limite la duración temporal…"

cometidos a través de medios informáticos. Esta posible interpretación, tal como ha quedado redactada la norma, podría llevar a desvirtuar el espíritu limitador planteado por el legislador de que una medida procesal de tal injerencia en el ámbito de protección de garantías constitucionales sólo sea admisible para la investigación de delitos de especial gravedad (como posible derivación del principio de proporcionalidad). Hoy en día prácticamente cualquier delito puede ser cometido por medios tecnológicos y esto no significa de por sí un aumento de la gravedad del delito (no existen razones que justifiquen que el uso de la tecnología signifique una mayor gravedad del delito).

La nueva ley prevé también una regulación exhaustiva del contenido que debe tener la resolución judicial que autoriza la medida previendo la necesidad de que la resolución establezca diferentes recaudos acerca de la forma de ejecución, incluyendo el *software* que se autoriza a utilizar y los recaudos técnicos que se adoptaran para garantizar la cadena de custodia de los datos obtenidos[64].

La ley prevé también la posibilidad de extender la medida cuando los datos buscados estén alojados en otro sistema informático: "Cuando los agentes que lleven a cabo el registro remoto tengan razones para creer que los datos buscados están almacenados en otro sistema informático o en una parte del mismo, pondrán este hecho en conocimiento del juez, quien podrá autorizar una ampliación de los términos del registro". La norma, sin embargo, no aclara ni se hace cargo del problema que plantea la posibilidad de que la extensión del registro remoto signifique un acceso transfronterizo de datos en la medida en que el sistema al que se accede este ubicado físicamente en extraña jurisdicción, cuestión que seguramente generará debates jurisprudenciales para su definición, especialmente vinculados a la admisibilidad de la evidencia así obtenida.

La nueva legislación prevé también la obligación de que los prestadores de servicios y los responsables o titulares de los sistemas informáticos que son objeto de la medida presten colaboración a las autoridades para su ejecución, facilitando el acceso con información sobre el sistema y las medidas de protección. Aunque el deber de colaborar excluye a los imputados y a quienes están dispensados de declarar testimonialmente por parentesco en razón del

---

64 Artículo 588 septies a. 2.: "La resolución judicial que autorice el registro deberá especificar: a) Los ordenadores, dispositivos electrónicos, sistemas informáticos o parte de los mismos, medios informáticos de almacenamiento de datos o bases de datos, datos u otros contenidos digitales objeto de la medida. b) El alcance de la misma, la forma en la que se procederá al acceso y aprehensión de los datos o archivos informáticos relevantes para la causa y el software mediante el que se ejecutará el control de la información. c) Los agentes autorizados para la ejecución de la medida. d) La autorización, en su caso, para la realización y conservación de copias de los datos informáticos. e) Las medidas precisas para la preservación de la integridad de los datos almacenados, así como para la inaccesibilidad o supresión de dichos datos del sistema informático al que se ha tenido acceso"

secreto profesional, entiendo que esta norma generará importantes discusiones sobre los alcances de las obligaciones de colaboración del sector privado[65].

➢ *Portugal*

Portugal no tiene una norma que regule de manera expresa las técnicas de registro y secuestro de datos de manera remota o la utilización de programas troyanos por parte del Estado para la investigación en causas penales. Sin embargo, una parte de la doctrina y jurisprudencia de aquel país entienden que la base legal que habilita esta posibilidad proviene de uno de los artículos de la ley de delitos informáticos (Ley nº 109/2009)[66] . El artículo 19 ley prevé la posibilidad de acciones encubiertas en la investigación en entornos digitales y en el párrafo 2 establece: "2 - Si es necesario el uso de medios y dispositivos informáticos, se observarán en lo que sea aplicable, las normas para la interceptación de las comunicaciones".

La discusión en Portugal se centra en determinar qué significa en el marco de este artículo de la *Ley medios y dispositivos informáticos*. Concretamente, si este párrafo está habilitando la utilización de programas informáticos para la búsqueda de evidencia digital en los sistemas informáticos en forma encubierta (diferenciándose de la medida de intercepción de comunicaciones prevista en el artículo 18 de la ley a la que hacemos referencia en el párrafo siguiente). Por otra parte, de ser así, parecería que la medida solamente sería aplicable en los casos de acciones encubiertas lo cual restringiría mucho su utilización de acuerdo a las previsiones que habilitan las acciones encubiertas.

---

[65] "Artículo 588 septies b. Deber de colaboración. 1. Los prestadores de servicios y personas señaladas en el artículo 588 ter e y los titulares o responsables del sistema informático o base de datos objeto del registro están obligados a facilitar a los agentes investigadores la colaboración precisa para la práctica de la medida y el acceso al sistema. Asimismo, están obligados a facilitar la asistencia necesaria para que los datos e información recogidos puedan ser objeto de examen y visualización.
2. Las autoridades y los agentes encargados de la investigación podrán ordenar a cualquier persona que conozca el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos contenidos en el mismo que facilite la información que resulte necesaria para el buen fin de la diligencia.
Esta disposición no será aplicable al investigado o encausado, a las personas que están dispensadas de la obligación de declarar por razón de parentesco, y a aquellas que, de conformidad con el artículo 416.2, no pueden declarar en virtud del secreto profesional.
3. Los sujetos requeridos para prestar colaboración tendrán la obligación de guardar secreto acerca de las actividades requeridas por las autoridades…"

[66] Ley sancionada el 15 de septiembre del año 2009, publicada en el Boletín Oficial de Portugal, D.R, nro. 179. "Aprueba la Ley del Cibercrimen, adaptando al ordenamiento jurídico interno la Decisión Marco nº 2005/222/JAI, del Consejo, de 24 de febrero, relativa a los ataques contra los sistemas de información, y la Convención sobre el Cibercrimen del Consejo de Europa". La ley adapta la legislación nacional para dar cumplimiento a los compromisos asumidos al adherir a la convención de Budapest previendo tanto normas de derecho penal de fondo como derecho procesal penal.

Otra postura, especialmente sustentada por las autoridades policiales especializadas en la persecución de delitos informáticos (de manera similar a la experiencia en otros países, sostiene que la admisibilidad de utilización de estas técnicas de investigación proviene de la norma que prevé la intercepción de comunicaciones por aplicación analógica[67] y, adicionalmente, la norma especial prevista expresamente para el registro de datos informáticos en el artículo 15[68] de la Ley o mediante una combinación de los requisitos previstos en ambas normas.

Sin embargo, pareciera que ninguna de estas normas ni ambas combinadas permiten dar sustento legal en el sistema portugués a la posibilidad de utilizar las técnicas de *remote forensic* en todos sus alcances y posibilidades tal como destaca parte de la doctrina de aquel país. Básicamente, la norma que prevé la interceptación de comunicaciones no habilitaría la utilización de *malware* o programas para la obtención de datos que exceden el marco de una comunicación (momento en el que la comunicación se produce entre quien envía datos y quien los recibe en tiempo real), mientras que las previsiones del artículo 15 sobre el registro de sistemas informáticos se refiere claramente a la búsqueda de datos previamente determinados en sistemas informáticos también identificados lo que parece excluir una de las posibilidades de investigación de este tipo de programas que es la obtención de datos en línea

---

[67] Artículo 18: "1 - Será admisible la interceptación de las comunicaciones cuando se investiguen los delitos:
a) previstos en esta ley, o b) aquellos cometidos por medio de un sistema informático o en los que sea necesario reunir pruebas en formato electrónico, cuando estos delitos se encuentren previstos en el artículo 187 del Código de Procedimiento Penal.
2 - La interceptación de transmisiones de datos informáticos sólo será permitida mientras dure la investigación si hay razones para creer que es esencial para establecer la verdad o para la obtención de pruebas que, de lo contrario, serían imposibles o muy difícil de obtener, mediante orden motivada del juez y previa solicitud del Ministerio Público".
3 - La interceptación puede destinarse al registro de datos sobre el contenido de las comunicaciones o apenas a la recopilación y registro de los datos de tráfico, a lo cual deberá hacer referencia la orden correspondiente, de acuerdo con las necesidades específicas de la investigación".

[68] "Artículo 15 - Búsqueda de datos informáticos
1. Cuando en el transcurso de un proceso fuera necesario con el fin de descubrir la verdad, obtener datos informáticos específicos y determinados, almacenados en un determinado sistema informático, la autoridad judicial competente autorizará u ordenará por orden que se proceda a un registro en el sistema informático, debiendo, en la medida de lo posible, presidir la diligencia.
2. La orden prevista en el número anterior tendrá un plazo de validez máximo de30 días, so pena de nulidad.
3. La policía criminal podrá proceder a la pesquisa, sin previa autorización de la autoridad judicial, cuando:
a. La misma fuera voluntariamente consentida por quien tuviera la disponibilidad o control de tales datos, cuando el consentimiento prestado se encuentre, por cualquier medio, documentado.
b. En los casos de terrorismo, criminalidad violenta o altamente organizada, cuando haya indicios fundados de la comisión inminente de un delito que ponga en riesgo grave la vida o la integridad de cualquier persona…"

como pueden ser claves, acceso a páginas de internet, o datos de tráfico de comunicaciones que se generan. Lo cierto es que del texto de la norma parece surgir con claridad que esta pergeñado para la habilitación legal de los registros de sistemas informáticos en lugares físicos como una extensión de las normas de registro y secuestro de elementos físicos a la evidencia digital, previsión de suma importancia, pero que no alcanza a la habilitación legal de las técnicas de acceso remoto.

La única habilitación legal clara que posibilitaría este tipo de medidas en el sistema procesal portugués parece surgir entonces de la norma sobre acciones encubiertas lo cual restringe de manera significativa la posibilidad de su utilización.[69]

II. Acceso transfronterizo en el derecho comparado

El acceso transfronterizo de datos[70], en cualquiera de sus modalidades, aparece como uno de los temas más difíciles de resolver tanto para el derecho procesal penal como para el derecho internacional. Se trata de buscar soluciones jurídicas para nuevos supuestos prácticos surgidos del avance de la tecnología en los que la evidencia digital a la cual es necesario acceder en el marco de una investigación penal está alojada en cualquier tipo de soporte físico de datos[71] o

---

[69] En todo este capítulo, cfr., Salt, Marcos G. su tesis doctoral, p. 57 ss.

[70] Salt, Marcos G. tesis doctoral, p. 163.

[71] La evidencia digital puede ser encontrada en cualquier tipo de sistema informático desde computadoras personales, laptops, tablet, consolas de juegos, discos de almacenamiento, pen drive, etc. y, modernamente, teléfonos celulares con tecnología para producir, almacenar o transmitir datos o la denominada internet de las cosas. Ver especialmente la nota interpretativa 1 adoptada por el Comité de la Convención de Delitos informáticos del consejo de Europa, (Cybercrime Convenition on Commite T-CY) en Diciembre del año 2012. Punto conclusivo nro. 4: "Conclusión. El T-CY conviene en que la definición de sistema informático contenida en el apartado a) del artículo 1 abarca nuevas tecnologías que van más allá de los sistemas de ordenadores centrales y personales, como los teléfonos móviles modernos, smartphones, PDA, tabletas o semejantes."Publicación del texto en idioma español en: Convenio sobre la Ciberdelincuencia. Informe explicativo y notas de orientación, Publicación del Consejo de Europa, pág. 262

en un servidor[72] cuyo alojamiento físico de datos está ubicado en extraña jurisdicción (provincia o país diferentes) a la de la autoridad que lleva adelante la investigación en virtud del poder jurisdiccional que ostenta. Puede suceder que el soporte físico o el servidor en el que está alojada la información que es objeto de búsqueda en el marco de la investigación penal se encuentre ubicado geográficamente en una provincia distinta a la de las autoridades judiciales que ejercen *poder jurisdiccional* en una causa penal, o en un país extranjero o, incluso, puede ocurrir que ni siquiera sea posible determinar *técnicamente* al momento de realizar una medida de prueba en qué lugar geográfico se encuentra el servidor que contiene la evidencia necesaria para una investigación penal.

La posibilidad de que las autoridades encargadas de la persecución penal de un Estado accedan (mediante cualquiera de las formas que las tecnologías informáticas y de las comunicaciones hoy permiten) a evidencia digital[73] alojada en servidores o dispositivos informáticos de cualquier tipo ubicados *físicamente* en extrañas jurisdicciones, genera controversias jurídicas tanto en el ámbito del derecho procesal penal como del derecho internacional (especialmente en lo

---

[72]Cf. http://www.alegsa.com.ar/Dic/servidor%20de%20archivos.php:"En internet, los servidores son los proveedores de todos los servicios, incluyendo las páginas web, el FTP, el correo electrónico, los grupos de noticias, etc. Básicamente, una computadora conectada a internet emplea una dirección (dirección web, dirección IP, dirección FTP, etc.) para poder comunicarse con el servidor al que le corresponde. La computadora envía (utilizando el protocolo adecuado) las distintas solicitudes al servidor, y el servidor responde (empleando el protocolo adecuado) las solicitudes. El servidor también puede solicitar datos de la computadora, y la computadora le responde…". Cf. También, http://es.wikipedia.org/wiki/Servidor: "En informática, un servidor es un nodo que forma parte de una red, provee servicios a otros nodos denominados clientes. También se suele denominar con la palabra servidor a: Una aplicación informática o programa que realiza algunas tareas en beneficio de otras aplicaciones llamadas clientes. Algunos servicios habituales son los servicios de archivos, que permiten a los usuarios almacenar y acceder a los archivos de una computadora y los servicios de aplicaciones, que realizan tareas en beneficio directo del usuario final…."

[73] Me refiero a elementos de prueba en la forma de datos generados o almacenados en un dispositivo informático o un sistema informático de cualquier tipo.

relativo a los mecanismos de cooperación internacional en materia penal[74]) que, hasta hoy, no tiene soluciones uniformes ni en la doctrina ni en la jurisprudencia. Asimismo, el tema tiene ribetes importantes de política internacional ya que muchos de los supuestos en los que un Estado accede a evidencia alojada en extraña jurisdicción pueden ser vislumbradas por algunos países y organismos internacionales como violaciones a la soberanía nacional del Estado en el que los datos informáticos están alojados lo que puede llevar a controversias de geopolítica[75].

Los problemas que presenta el acceso transfronterizo de datos en sus diferentes formas fueron advertidos por los principales organismos internacionales preocupados por la investigación de los delitos informáticos ya desde finales de la década del 80, tendencia que fue creciendo en las últimas décadas hasta convertirse en la actualidad en un problema central a partir las posibilidades

---

[74]Es que como veremos en el desarrollo de este trabajo, el acceso por parte de las autoridades judiciales de un estado a evidencia digital alojada en extraña jurisdicción (ya sea que se realice de manera directa, mediante la entrega de los datos por su titular o mediante la cooperación de empresas proveedoras de servicios), genera problemas jurídicos aún sin solución tanto para el derecho procesal penal como para el derecho internacional cuyas normas de jurisdicción para la obtención de pruebas están basadas en el principio de territorialidad (ver apartado siguiente). El tema ha generado también conflictos sobre la aplicación de las normas de protección de datos vigentes en los diferentes países que están involucrados y en las normas internacionales sobre protección de datos personales. La compatibilización de estos marcos normativos de los derechos internos de los diferentes países y los convenios vigente de cooperación internacional resulta complicada en muchos supuestos. Ver a modo de ejemplos, la disparidad de posturas adoptadas por los organismos más vinculados a la persecución de delitos y órganos relacionados a la protección de datos personales en el seno de las audiencias organizadas por el Consejo de Europa. Cfr. especialmente la carta enviada al Consejo de Europa por el Grupo de Trabajo denominado *Article 29 Data Protection Working Party* mediante la que manifiesta sus preocupaciones por las propuestas elaboradas por el Grupo de Trabajo ad hoc sobre Jurisdicción y Acceso Transfronterizo de datos del Comité (TC-Y) del Convenio de Budapest. El 28 de mayo de 2014 el subgrupo de trabajo antes mencionado se reunió con representantes de los principales organismos de protección de datos personales de Europa para analizar las objeciones a la idea de un protocolo adicional de la Convención que permitía nuevas formas de acceso transfronterizo. Como consecuencia de esta reunión se decidió dejar de lado por el momento la idea de avanzar en el protocolo adicional hasta conseguir mayor claridad y nuevos consensos. Cfr. *Transborder Access to data and jurisdiction: Options for further action by the T-CY*, reporte preparado por el grupo de trabajo sobre acceso transfronterizo de datos del TC-Y, adoptado por el Comité en la reunión plenaria de diciembre de 2014, disponible en https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726e .

[75] La arista de política internacional que tiene este tema no puede dejar de señalarse ya que sin duda tendrá especial influencia en las soluciones jurisprudenciales y en la posterior regulación procesal que se adopte en los diferentes países. La falta de acuerdos sobre la cuestión puede poner en crisis los mecanismos de cooperación regional e internacional en materia penal y las posibles soluciones propuestas significan nuevas formas de cooperación o de aceptación de la intervención judicial de un Estado en otro que, en el mejor de los casos, atenderá a la necesidad de nuevos principios de derecho internacional público que permitan respetar adecuadamente la soberanía nacional de los países. El peor escenario, puede significar que la falta de acuerdos se convierta en una excusa para avalar el intervencionismo de algunos estados sobre otros. Estos debates en el seno de los organismos internacionales tendrá influencia en el mediano y largo plazo en las legislaciones de los derechos internos incluido, obviamente, el caso de la Argentina. Según entiendo, las decisiones de política internacional que se adopten se trasladará tarde o temprano a la legislación procesal penal interna de los diferentes países.

que brindan las tecnologías de la comunicación y el fenómeno de la computación en las nubes.

El tema del acceso directo de un Estado a datos alojados en otro Estado ya sea de manera directa (por la propia actividad de las autoridades de uno de penetrar en un sistema informático ubicado físicamente en el otro) o contando con la participación del titular de los datos ya sea como colaboración o por algún tipo de medida de coerción fue objeto de tratamiento en la Recomendación (R89) y en el reporte final del Comité Europeo de Problemas Criminales de 1990[76]. Aunque no se efectuaron recomendaciones ni se propusieron soluciones, los miembros del Comité advirtieron con total claridad los problemas jurídicos y los desafíos que vendrían lo que evidencia la calidad del trabajo le asigna una gran importancia como antecedente de lo que quedaría plasmado en la Convención de Budapest once años después. Más aún, sus reflexiones mantienen vigencia en las discusiones actuales casi veinticinco años después.

El Comité advertía las situaciones que podían derivarse del hecho de que la tecnología permitía que los datos estuvieran disponibles *en línea* en un Estado, aunque físicamente estuvieran alojados en otro. Conforme a ello se señalaba que circunstancias de urgencia podían hacer necesario acceder a esa evidencia con fines de investigación penal a fin de evitar que fueran de alguna manera alterados, borrados o suprimidos por el imputado evitando su utilización como evidencia. Por otra parte, advertía también los problemas de legitimidad que podía tener el acceso directo de autoridades de un Estado mediante mecanismos tecnológicos a datos ubicados en otro Estado con las posibles afectaciones al principio de soberanía nacional. Implícitamente ya se planteaba el tema, aún en discusión, de si el acceso directo a datos *a distancia* violentaba la soberanía del Estado en el que los datos estaban alojados. También se señalaba el caso de una persona sea compelida por una autoridad judicial o del Ministerio Público a acceder desde un Estado a los datos que tiene alojados en otro Estado.

En lo que respecta a los casos de *penetración directa* distingue los siguientes supuestos: allanamiento en el que la policía encuentra en el espacio físico que es objeto de la medida una terminal de computación en la que la pantalla muestra datos buscados que están alojados en extraña jurisdicción; allanamiento en el que la policía encuentra una computadora y realiza una búsqueda *sin saber* que la información está alojada en extraña jurisdicción; allanamiento en el que la policía encuentra una computadora y realiza tareas de búsqueda conociendo

---

[76]Cfr. *Recomendation R (89)9 on Computer Related Crime and Final Report of the European Committe on Crime Problems (1990) ,* versión en ingles en *Computer Related Crime*, prólogo de August Bequai, Council of Europe, Estrasburgo, 1990, especialmente pág. 86 y ss.http://www.oas.org/juridico/english/89-9&final%20Report.pdf. La claridad de los planteos fácticos y jurídicos le otorga a este "viejo" documento importante actualidad.

que los datos están alojados en extraña jurisdicción; la policía utiliza sus propias terminales para acceder a datos que están alojados en extraña jurisdicción.

El Comité expresa de manera somera y sin profundizar en los problemas jurídicos su opinión sobre estos supuestos por la validez de la prueba en el primer caso, la posible validez en el segundo caso basado en la buena fe del policía, pero advirtiendo que si se considerara que estos supuestos constituyen una violación del derecho internacional no sería clara la posibilidad de utilizar esta evidencia en la Corte[77]. En los supuestos tres y cuatro, el comité opina de manera potencial que deberían utilizarse los canales de cooperación internacional en materia penal.

El documento también analizó las situaciones en las que la emergencia podría dar lugar a que futuras convenciones previeron la posibilidad de accesos directos. El documento cuenta con la gran virtud de haber advertido ya en su época mucho de los temas que serían discutidos en las décadas siguientes y que aún hoy están en el centro de debate académico y de política internacional. Si bien el Comité decidió no darles solución ya que considera que no era el momento oportuno por la importancia de los principios que estaban en juego, básicamente la idea arraigada de la soberanía nacional aplicada a los poderes jurisdiccionales y por considerar que en aquel momento no era una necesidad acuciante, aunque advertía que en el futuro el tema debería ser tratado.

En el año 1995 (cinco años después), la Recomendación R (95) del Comité de Ministros del Consejo de Europa[78] advertía la necesidad tanto de armonizar las normas procesales generando nuevas herramientas para la obtención de evidencia digital como de negociar acuerdos internacionales sobre el tema. En los puntos salientes de los antecedentes se señalaba: teniendo en cuenta que las pruebas de los delitos pueden ser almacenados y transferidos por estos sistemas; tomando nota de que las leyes procesales penales de los Estados miembros a menudo aún no establece competencias necesarias para buscar y recoger pruebas en estos sistemas en el curso de las investigaciones penales; recordando que la falta de adecuados poderes especiales pueden perjudicar a las autoridades investigadoras en el cumplimiento de sus tareas en la cara del desarrollo actual de la tecnología de la información; reconociendo la necesidad de adaptar las herramientas legítimas que las autoridades investigadoras se les concede en virtud de las leyes procesales penales a la naturaleza específica de las investigaciones en los sistemas de información electrónicos; preocupados por el

---

77 Report By The European Committee on Crime Problems, pág. 88.

78Recomendación n º r (95) 13del Comité de Ministros a los Estados Miembros sobre los Problemas de Derecho Procesal Penal Relacionados con la Tecnología de la Información*(*Adoptada por el Comité de Ministros el 11 de septiembre de 1995, en la 543 ª sesión de los Delegados de los Ministros*)*

riesgo potencial de que los Estados miembros no pueden ser capaces de prestar asistencia judicial recíproca en forma adecuada cuando se le solicite para recoger pruebas electrónicas en su territorio a partir de los sistemas de información electrónicos; convencidos de la necesidad de fortalecer la cooperación internacional y lograr una mayor compatibilidad de las leyes procesales penales en este ámbito. En el anexo de Recomendaciones, el punto 17 prevé la necesidad de extender los registros de datos a sistemas ubicados en extrañas jurisdicciones en casos en que la urgencia lo hiciera necesario. Los peligros para la soberanía también eran advertidos y por este motivo se exhortaba a los países a establecer mediante acuerdos internacionales una base legal clara que precisara los casos y las condiciones en que estas extensiones de los registros y secuestros de sistemas informáticos a extrañas jurisdicciones serían permitidos.

a) El tratamiento del tema en el grupo de los ocho (G8).

El G8 se ocupó también de las implicancias del acceso transfronterizo de datos. Ya a mediados de la década del 90 comenzó un trabajo paralelo al de los expertos del Consejo de Europa que se ocupaban de la redacción de la Convención de Budapest. En 1997 el Grupo de los Ocho (G8) estableció un Subcomité especial sobre delitos de alta tecnología, cuyo objetivo fue fijar criterios para la luchar contra los delitos informáticos. Durante la reunión del G8, celebrada en Washington D.C., Estados Unidos, los Ministros de Justicia y del Interior del G8 adoptaron Diez Principios y un Plan de Acción de diez puntos para combatir los delitos informáticos. Entre los principios la necesidad de evitar que existan refugios para aquellos que utilizan de forma abusiva las tecnologías de la información a través de unificar legislaciones procesales y penales sobre la materia; generar protocolos para la rápida cooperación internacional; trabajar con el sector privado. Entre los puntos más destacables del plan de acción a los fines de este trabajo: designación de puntos de contacto 24/7; *desarrollar mecanismos procesales para obtener datos procesales más allá de las fronteras de cada país*.

En 1999 el G8 fijó criterios más específicos para luchar contra el delito de alta tecnología en la Conferencia Ministerial sobre la Lucha contra el Delito Transnacional celebrada en Moscú, Rusia, haciendo especial referencia entre los temas a la posibilidad de rastrear las transacciones y el acceso transfronterizo para almacenar datos. En el comunicado publicado con motivo de la Conferencia se consignan varios principios sobre la lucha contra los delitos informáticos que tuvieron gran influencia a nivel internacional y mantienen vigencia aún hoy en las discusiones internacionales. Así, el punto 6 estableció: "Sin perjuicio de las disposiciones de estos principios, un Estado no requerirá autorización de otro Estado cuando actúe de acuerdo a los principios de su

legislación nacional con el fin de: acceder a datos de disposición pública (*open source*) independientemente del lugar geográfico en que estos datos estén alojados; acceder, registrar, copiar o secuestrar datos almacenados en un sistema informático ubicado en otro Estado, en caso de contar con el consentimiento legal y voluntario de la persona que tiene la autoridad legal para revelar a esos datos. El Estado que efectúa el registro deberá considerar notificar al Estado objeto del registro, si esta notificación es permitida por la legislación nacional y los datos obtenidos revelan una violación de la ley penal o de otra manera pueden ser de interés para el Estado objeto del registro". (Traducción de Salt[79]).

La estructura de este principio es el antecedente directo de la redacción del artículo 32 de la Convención de Budapest. Los redactores de la Convención prácticamente mantienen la misma redacción salvo la notificación al Estado en cuyo territorio están alojados los datos que son objeto de un acceso transfronterizo que es omitida en el texto del artículo 32 de la Convención de Budapest.

b) Unión Internacional de Telecomunicaciones de NU

Este organismo de Naciones Unidas elaboró un documento[80] como modelo de normas para los países que quieran modificar su legislación interna en materia de delitos informáticos, tanto en lo que respecta a la legislación de fondo como de forma[81]. Este conjunto de herramientas contiene en materia de acceso transfronterizo en la sección 30[82] una norma similar a la del artículo 32 de la Convención de Budapest, circunstancia que vuelve a dejar en evidencia la dificultad de alcanzar nuevos consensos a nivel internacional para avanzar más allá de lo previsto en la Convención de Budapest (tengamos en cuenta que la

---

79 Salt, Marcos, tesis doctoral, p. 224.

80 Este documento fue elaborado por un equipo de expertos internacionales de diferentes áreas (abogados, representantes de la industria de las TICs, académicos, informáticos, funcionarios gubernamentales de diferentes países) convocados bajo la dirección de la Asociación Americana de Abogados y el Departamento de Políticas y Estrategias de la ITU.

81 ITU Toolkit for Cybercrime Legislation, versión de febrero del año 2010 disponible en http://www.cyberdialogue.ca/wp-content/uploads/2011/03/ITU-Toolkit-for-Cybercrime-Legislation.pdf

82 La norma en idioma original establece: "Section 30. Trans-Border Access to Stored Computer Data, Content Data, or Traffic Data(a) A competent authority may access publicly available (open source) stored computer data, content data, or traffic data regardless of where the data is located geographically. (b) A competent authority from another country may, without authorization of authorities of this country, have access to and receive, by means of a computer or computer system located on its territory, specified computer data, content data, or traffic data stored in this country if the competent authority from the other country obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to such competent authority through that computer or computer system."

guía emanada del organismo de UN fue elaborada en el año 2009). El documento establece dos supuestos en los que se permite que un Estado acceda a datos informáticos alojados en otro Estado sin pasar por los mecanismos formales de cooperación internacional. El primer supuesto prevé el caso en el que los datos se encuentren disponibles públicamente (fuente abierta) sin importar en qué lugar geográfico estén alojados los datos. Se refiere tanto a datos de tráfico como de contenido. El segundo supuesto habilita a las autoridades de un Estado a tener acceso o recibir datos provenientes de otro Estado mediante computadoras o sistemas informáticos ubicados en su propio territorio, sin el consentimiento de las autoridades del Estado extranjero en el que los datos están alojados, si la autoridad competente obtiene el consentimiento legal y voluntario de la persona que tiene la autoridad legal de revelar los datos a la autoridad competente.

c) La regulación en los códigos procesales penales de algunos países paradigmáticos

➢ *Portugal*:

Portugal tiene una de las legislaciones procesales más completas en términos de medidas procesales para la obtención de evidencia digital[83]. La norma procesal está inspirada en los requerimientos de la Convención de Budapest pero ha agregado algunas medidas de investigación no previstas en el texto de la Convención, de hecho la doctrina ha interpretado que el CPP Portugal habilita el acceso transfronterizo de datos en determinados supuestos.

El artículo 15. 5 de la ley[84] prevé la posibilidad de extender el registro y secuestro de datos desde un dispositivo de origen a un sistema o parte de sistema al que se pueda acceder legalmente: "…Cuando, en el transcurso de la investigación, surgieran razones para creer que los datos procurados se encuentran en otro sistema informático, o en una parte diferente del sistema registrado, si tales datos son legítimamente accesibles a partir del sistema inicial, el registro podrá ser extendido mediante autorización u orden de autoridad competente…". El artículo no establece expresamente que la facultad de extender las medidas de registro y secuestro de datos en sistemas informáticos se limite a sistemas dentro de las fronteras de Portugal lo que ha permitido interpretaciones tanto doctrinarias como jurisprudenciales en el sentido validar bajo esta norma los accesos a un sistema informático conectado

[83] Ley número 109/2009, Cf. Versión en español en texto comparado con las normas de la Convención de Budapest, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680304317

[84] La norma fue incorporada para cumplimentar en el derecho interno de Portugal los requisitos exigidos por el artículo 19 de la Convención de Budapest.

o incluso a sistemas de correo electrónico *webmail* alojados en extraña jurisdicción.

Incluso más, el artículo 25 de la Ley que prevé expresamente la posibilidad de que un Estado extranjero pueda acceder a datos alojados en servidores o dispositivos ubicados físicamente en Portugal en los casos de datos abiertos o con consentimiento de la persona autorizada a revelarlos (regulación que adopta los criterios del artículo 32 de la Convención de Budapest): "Las autoridades extranjeras competentes, sin previa petición a las autoridades portuguesas, de conformidad con las normas sobre transmisión de los datos personales contenidos en la Ley nº 67/98 de 26 de octubre, podrán: a) acceder a datos informáticos almacenados en un sistema informático ubicado en Portugal, cuando éstos estén a disposición del público; b) recibir o acceder, por medio de un sistema informático ubicado en su territorio, a datos informáticos almacenados en Portugal, con el consentimiento legal y voluntario de la persona legalmente autorizada a revelarlos".

➢ *Bélgica*

El ejemplo del CPP de Bélgica resulta también interesante como modelo normativo[85]. El tema está específicamente regulado en el art. 88 ter del Código Procesal Penal de Bélgica. La norma autoriza al juez de investigación cuando ordena un registro de un sistema informático a disponer que se extienda el registro a otro sistema informático o a parte de él, sin importar el lugar que esté, bajo determinadas condiciones: la necesidad de la medida para descubrir la verdad, su proporcionalidad y el peligro de desaparición de la prueba. Asimismo, la norma restringe la medida a la parte del sistema desde la que la usuraria inicial allanada tiene acceso. Una nota original del artículo es que prevé expresamente la situación de que se advierta que se está realizando un acceso transfronterizo. En este supuesto, la norma restringe el alcance de la media a la posibilidad de copiar los datos, pero no a removerlos. El legislador belga parece haber tomado el criterio de que la copia no afecta el principio de territorialidad por su menor nivel de afectación en el Estado al que se accede. Esto es, diferenciar la mera copia del secuestro de los datos. Por otra parte, la jurisprudencia de este país ha interpretado que el artículo 46 bis del CPP habilita a los fiscales a solicitar de manera compulsiva a las empresas proveedoras de servicio extranjeras que brinden servicios en el país datos necesarios para una investigación penal aunque estén alojados en un servidor en extraña jurisdicción.

---

[85] La modificación al CPP Belga fue introducida en el año 2000, antes de la aprobación de la Convención de Budapest pero, evidentemente, siguiendo sus discusiones y documentos preparatorios.

➢ *España*

El caso español previo a la nueva ley que regula todo lo atinente a las medidas de investigación tecnológica[86] (o sea sobre una base normativa del viejo ordenamiento procesal que no contenía norma alguna en relación a la evidencia digital), presenta similitudes a lo sucedido en nuestro país con este tipo de accesos transfronterizo de datos, con la diferencia de que el tema recibió mayor discusión tanto en ámbitos académicos como jurisprudenciales. En la práctica de los tribunales se produjeron situaciones de acceso a datos alojados en extraña jurisdicción aún sin una norma que así lo habilitara de manera expresa (especialmente el acceso al contenido de cuentas de correo electrónico alojadas en servidores extranjeros *webmail* o datos alojados en extraña jurisdicción, pero accesibles desde una terminal en España a la que se accedía en el marco de una medida procesal de allanamiento o requisa).

La Ley 13/2015, introdujo un extenso catálogo de normas para regular de manera expresa las diferentes formas de obtener evidencia digital evitando los problemas que traía la aplicación analógica del viejo Código procesal. Sin perjuicio de que no contiene una regulación expresa para los supuestos que estamos analizando, esto es la posibilidad extender el acceso a datos de manera transfronteriza, la norma que habilita a extender la búsqueda de datos a sistemas informáticos conectados no prevé tampoco un límite expreso que excluya la posibilidad de acceder a datos fuera de las fronteras de España. De manera tal que es posible que la norma sea utilizada en el sentido de habilitar los accesos transfronterizos a sistemas conectados desde terminales a los que se accedió legítimamente en el marco de un allanamiento o una requisa.

Así, el artículo 588 sexies c, en lo pertinente establece: "…1. La resolución del juez de instrucción mediante la que se autorice el acceso a la información contenida en los dispositivos a que se refiere la presente sección, fijará los términos y el alcance del registro y podrá autorizar la realización de copias de los datos informáticos. Fijará también las condiciones necesarias para asegurar la integridad de los datos y las garantías de su preservación para hacer posible, en su caso, la práctica de un dictamen pericial". Y específicamente en el numeral 3: "Cuando quienes lleven a cabo el registro o tengan acceso al sistema de información o a una parte del mismo conforme a lo dispuesto en este capítulo, tengan razones fundadas para considerar que los datos buscados están almacenados en otro sistema informático o en una parte de él, *podrán ampliar el registro, siempre que los datos sean lícitamente accesibles por medio del sistema inicial o estén disponibles para este*. Esta ampliación del registro

[86] Ley Orgánica 13/2015, Modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, publicada en el Boletín Oficial del Estado nro. 239 del 6 de octubre de 2015.

deberá ser autorizada por el juez, salvo que ya lo hubiera sido en la autorización inicial. La norma constituye una aplicación de lo dispuesto en el artículo 19 de la Convención de Budapest pero sin los límites expresos respecto a la jurisdicción, situación similar a la verificada en la legislación de Portugal.

d) El tratamiento del tema en resoluciones judiciales paradigmáticas del derecho comparado

Algunos casos jurisprudenciales del derecho comparado merecen ser analizados, ya sea por su influencia en la discusión de política internacional sobre el tema como por sus análisis teóricos de las cuestiones jurídicas involucradas.

➢ *El Caso Gorshkov- Ivanov.*

Este caso es quizá el primer precedente de registro y secuestro transfronterizo de datos (una de las formas de acceso transfronterizo) realizado de manera directa por autoridades de un Estado en otro que despertó el interés de la doctrina internacional y significó el inicio de importantes discusiones en el plano internacional, que aún continúan y se intensifican a medida que se acrecienta el problema con el avance de la computación en la nube[87]. Las autoridades de un Estado accedieron de manera directa a datos almacenados en un servidor en país extranjero y, posteriormente, la evidencia obtenida fue la base de una sentencia judicial. La conjugación de estos dos elementos hizo que el caso inspirara la atención académica y política sobre el caso.

En el mes de noviembre del año 1999 dos ciudadanos rusos produjeron múltiples accesos ilegítimos utilizando internet en diferentes sistemas informáticos alojados en territorio de los EEUU. El hecho afectó a por lo menos veinte compañías comerciales americanas incluyendo bancos, empresas de

[87] Conforme lo explica Salt, Marcos G. en su tesis doctoral en la cita 386, p. 236: La controversia generada por esta causa tramitada en los tribunales de EEUU puede ser la génesis del alejamiento de Rusia de la política común adoptada por EEUU y los países miembros del Consejo de Europa en materia de persecución de los delitos informáticos que se plasmaron finalmente en la Convención de Budapest. Tal como hemos visto en el punto referido a la evolución histórica, Rusia había participado activamente de las reuniones del G8 y aprobado los principios adoptados en relación a este tema en la reunión de Moscú. La controversia generada por el caso derivó en que Rusia iniciara proceso penal para los agentes de EEUU que realizaron la investigación, mientras que EEUU respondió premiando a los agentes por la operación. Actualmente Rusia presenta en ámbitos internacionales la postura antagónica a la de EEUU y los países europeos en relación a la promoción de la aprobación de la Convención de Budapest por la mayor cantidad de países posibles y propone, en cambio, convocar a una nueva convención internacional en el marco de las Naciones Unidas (postura seguida en el ámbito regional por Brasil). Si bien Rusia participa de las reuniones de seguimiento de la Convención Europea que se realizan anualmente en Estrasburgo, presenta posturas críticas tanto sobre el texto de la convención como sobre las diferentes propuestas en relación a su actualización como por ejemplo en el tema de este capítulo en el que hoy se trabaja en la preparación de un protocolo adicional.

tarjetas de crédito y proveedores de servicios de Internet (ISPs) – Yahoo, Ebay, CD Universe, OIB, entre otras-. De esta manera, los autores del ilícito lograron acceso a datos personales y comerciales que utilizaron para cometer fraudes. En los comienzos del año 2000 una de las empresas afectadas (OIB) recibió un mail *coactivo* mediante el cual, personas hasta ese momento desconocidas, le informaban que tenían el *password* que permitía acceder a todos los datos de la empresa y que podían borrar los datos de todas las computadoras del sistema salvo que la empresa los contratara como consultores en seguridad. La investigación del caso quedó a cargo del FBI que detectó que el mail provenía de un proveedor con servidor en Washington que también había sido accedido ilegalmente y era utilizado para encubrir el origen de la comunicación. La investigación permitió determinar que en la maniobra se habían utilizado dos computadoras ubicadas en territorio ruso. Con esta información el FBI inició una operación para traer bajo engaño a territorio norteamericano a los ciudadanos rusos que eran autores de las maniobras y posteriormente detenerlos. Así creó una empresa de seguridad informática ficticia que llamó, *invitó* y ofreció trabajo a través de ella a los sospechosos invitándolos a concurrir a EEUU para demostrar sus habilidades. Una vez en territorio norteamericano (ciudad de Seattle), agentes del FBI haciéndose pasar por empleados de la firma, les pidieron que ingresen ilegítimamente a la página *web* de una empresa que había sido creado sólo con la finalidad de engañar a los sospechosos. Toda la actividad fue grabada y además se utilizó un programa espía que permitía grabar toda la actividad de los usuarios. Usando esta computadora, los sospechosos ingresaron a su sistema informático en Rusia para acceder a los programas necesarios para realizar la demostración que les era solicitada. De esta manera, el FBI obtuvo la clave de acceso a sus servidores en Rusia y detuvo a los ciudadanos rusos Ivanov y Gorshkov. Con las claves obtenidas y por temor a que la evidencia que era necesaria para la acusación fuera borrada, los agentes del FBI ingresaron a los servidores de los sospechosos y obtuvieron las pruebas que serían utilizadas posteriormente para su condena (se secuestraron 250 gigabytes de información como por ejemplo datos de 56.000 tarjetas de crédito). En definitiva, ingresaron de manera directa (caso de penetración directa) sin utilizar ninguno de los mecanismos de cooperación internacional existentes ni notificar de manera alguna a las autoridades de Rusia.

Ambos casos judiciales que tramitaron en jurisdicciones estaduales diferentes de EEUU no fueron discutidos desde la perspectiva del principio de territorialidad y sus implicancias tanto para el derecho internacional público como para el derecho procesal penal. Antes bien, la defensa no realizó este planteo y, de hecho, en la decisión del tribunal, la circunstancia de que las computadoras estuvieran en territorio ruso jugó llamativamente en contra de los acusados. En efecto, fue utilizado sagazmente para justificar que las

garantías del texto constitucional norteamericano no eran aplicables al caso. En efecto, el tribunal sostuvo que las garantías sólo eran aplicables en territorio de EEUU y al estar el servidor en Rusia no podían ser invocadas.

La defensa de Ivanov planteó el tema del principio de territorialidad sólo desde un punto de vista del derecho penal de fondo. Básicamente que los tribunales de EEUU no tenían competencia ya que al haber sido cometidos los delitos en Rusia (desde Rusia), lugar en el que él cometió la acción, la ley penal de EEUU no era aplicable. El tribunal rechazo el planteo fundamentando su postura en que el efecto de la acción de Ivanov se produjo en EEUU y que la legislación de EUUU prevé aplicación extraterritorial para los delitos que fueron objeto de la acusación[88]. El fiscal se había opuesto al planteo con el mismo fundamento: "Los tribunales americanos pueden juzgar a Ivanov por la misma razón que podrían juzgar a un hombre que parado en el lado canadiense de la frontera disparara contra alguien en Washington".

En la causa seguida contra Gorshkov, el tribunal estableció que las garantías previstas por la Cuarta Enmienda del texto constitucional norteamericano no se aplicaban al registro y secuestro en cuestión ya que las computadoras a las que accedieron los investigadores del FBI sin la debida autorización judicial no estaban en territorio americano.

➢ *Bélgica contra Yahoo*

El caso fue objeto de análisis en diferentes foros internacionales preocupados por la persecución de los delitos informáticos, especialmente en el ámbito europeo, en donde fue mostrado como un ejemplo de reafirmación de las facultades de persecución penal territorial de un país europeo frente a la negativa en el acceso a datos informáticos necesarios como evidencia por parte de una empresa proveedora de servicios con sede en los EEUU.

En el año 2007, en el marco de una investigación penal por maniobras de fraude cometidas en perjuicio de ciudadanos belgas (compra de productos electrónicos con datos falsos), un fiscal de aquel país solicitó a la sede de la empresa Yahoo en Bélgica información de determinadas cuentas de correo electrónico que habrían sido utilizadas en la maniobra que era objeto de investigación. El fiscal basaba su pedido en una norma del CPP de Bélgica (art. 46 bis) que lo habilita expresamente a solicitar la asistencia de las empresas de comunicaciones para identificar a los usuarios de un servicio cuando le sea requerido en el marco de una investigación penal.

---

[88] Cf. United States v. Ivanov

La empresa Yahoo, basó su negativa en la aplicación para el caso de la Ley de EEUU (*Electronic Communications Privacy Act* –ECPA-). En la base de su negativa a responder favorablemente el pedido del fiscal belga, hay un argumento vinculado a la idea de *territorialidad* y de que los datos almacenados en EEUU no pueden ser alcanzados por una orden emitida por un fiscal de otro país, aunque la empresa preste allí algún servicio. Así, la empresa entiende que la información está en los EEUU, que la empresa no está vinculada *territorialmente* con Bélgica (en el sentido de estar alcanzada por sus poderes procesales de investigación) y por lo tanto no se le aplican las normas del Código Procesal Penal belga. Yahoo alegó que la pretensión de las autoridades belgas significaba una intención de extender sus poderes procesales de manera extraterritorial. De esta manera, Yahoo entendió que la única forma de entregar los datos que le solicitan es a través de un pedido de cooperación internacional en el marco de un tratado de asistencia legal mutua.

Por el contrario, el fiscal argumentó que sin perjuicio de que Yahoo Inc. es una empresa radicada legalmente en los EEUU, tiene presencia en territorio belga ya sea por razones comerciales (tiene clientes, ganancias comerciales, etc.) como por los servicios de comunicaciones que brinda valiéndose de internet.

La justicia belga impuso a la empresa Yahoo una multa por su negativa a cumplir con la obligación impuesta por la norma procesal. Esta resolución fue revisada en diversas instancias hasta que la Cámara de Apelaciones de Amberes reconoció el carácter de empresa obligada a cumplir con los requerimientos de información de las autoridades de cumplimiento de la ley de Bélgica conforme lo establezca la legislación interna de este país. El fallo establece que la empresa tiene presencia territorial en Bélgica independientemente del lugar de alojamiento central de la información y que debe ser considerado un proveedor de servicios de comunicación alcanzado por las previsiones del art. 46 bis antes citado. El tribunal argumentó que Yahoo voluntariamente aceptó la jurisdicción de Bélgica al ejercer actividades económicas, utilizar en su página el idioma local, usar el dominio yahoo.be, vender publicidad, etc. La Corte Suprema confirmó esta resolución, importa el 1 de diciembre del año 2015. Previamente la Corte Suprema (*Cour de cassation/ Hof van cassatie*), ya había determinado en fallo del 18 de enero del 2011 que los servicios que brindaba Yahoo en territorio belga reunían las características para ser considerada como una empresa proveedora de comunicaciones obligada por la norma procesal del art. 46[89].

➢ *Micrososoft vs United States*

---

[89]Cf. Steven De Schrijver y Thomas Daenens, *The Yahoo! Case: The End of International Legal Assistance In Criminal Matters*, publicado en "Telecommunications Media & Technology", septiembre del 2013.

El estudio de este caso resulta de especial interés no solamente por las cuestiones jurídicas involucradas sino también por su trascendencia política y su potencial influencia en las futuras normas de cooperación internacional sobre la materia (especialmente en lo atinente a la relación entre los EEUU y los países de la Unión Europea). El conflicto involucra a una de las empresas multinacionales de origen norteamericano más importantes del sector enfrentada en la disputa con el gobierno de su propio país. Asimismo, el tema involucra a Irlanda (ubicación geográfica de los servidores donde están alojados los datos a los que el Departamento de Justicia pretendía acceder) y despierta el interés de los organismos de protección de datos personales de la Unión Europea[90]. El caso presenta características distintivas en relación a los supuestos de *cooperación asimétrica* (sector público- sector privado) que habían sido debatidos en ámbitos internacionales hasta ahora. Lo cierto es que la discusión había estado centrada en los problemas que genera para la eficiencia de las investigaciones penales la falta de colaboración de los grandes proveedores de servicios multinacionales con sede en EEUU con relación a los pedidos de autoridades de la justicia penal de países extranjeros. Los ejemplos expuestos reflejaban siempre las dificultades que encontraban los países (especialmente en el ámbito de nuestra región) para obtener datos de los denominados *grandes de internet* (Microsoft, Google, Facebook, etc.). Este precedente implica un cambio de escenario en el que el Estado afectado por la reticencia a entregas determinados datos en el marco de una causa penal es EEUU en relación a una empresa de su propio país. Concretamente está en discusión el rechazo de Microsoft (empresa multinacional con sede central en EEUU) a cumplimentar un pedido de datos de contenido solicitados por la fiscalía en el marco de una investigación penal argumentando que los datos solicitados están alojados en extraña jurisdicción (en este caso Irlanda) y que las autoridades de EEUU deben utilizar los convenios internacionales de cooperación internacional aunque se trate de una empresa cuya sede central está en territorio norteamericano. Por otra parte, se trata de un supuesto en el que los órganos de persecución penal le piden a la empresa privada que obtenga, utilizando los mecanismos tecnológicos de los que dispone, los datos alojados en extraña jurisdicción. Se discute la posible utilización de una

---

[90] La relación entre EEUU y la Unión Europea en lo referente a la transferencia de datos (tanto en el caso de empresas privadas como en supuestos de pedidos estatales) ha sido muy cambiante e influenciada por las preocupaciones y críticas de la Unión Europea a las medidas de vigilancia de sistemas informáticos por parte de autoridades gubernamentales de EEUU. De hecho, muchas de las preocupaciones europeas se refieren al aumento de los poderes de investigación otorgados al Estado en desmedro de la protección de los datos de los ciudadanos y una percepción de que los EEUU pueden extender sus poderes extraterritorialmente ignorando los valores europeos sobre la materia. Recientemente, el bloque europeo llego a un nuevo acuerdo sobre el tema que puede resultar un antecedente interesante en materia normativa de cooperación, *The Privacy Shield* (aprobado en julio de 2016), cf. texto en ingles en http:// ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf

empresa del sector privado para realizar una medida de investigación penal por parte del Estado. La disputa se centra también sobre el significado de esta orden. La empresa afirma que la orden implicaría acceder al contenido de los *mails* almacenados en extraña jurisdicción (Irlanda) para posteriormente entregárselo a las autoridades federales. El gobierno entiende que no se trata de un registro y secuestro de datos sino simplemente de una orden de entrega de información.

Los hechos del caso pueden resumirse así. Haciendo lugar a un pedido del fiscal en el marco de una investigación de tráfico de estupefacientes, un juez de Nueva York solicitó a la empresa Microsoft los datos de tráfico, de abonado y contenido de una cuenta de mail de un cliente. Microsoft aceptó revelar los datos que no implicaran *contenido de comunicaciones*–aceptó la orden en cuanto a los datos de abonado y tráfico- pero rehusó revelar y poner a disposición de las autoridades los datos de contenido. El argumento principal de la empresa es que los datos de contenido correspondientes a la cuenta están alojados en servidores que la empresa tiene en Irlanda. Conforme a ello, Microsoft argumentó que la empresa está obligada a cumplir con la legislación de datos personales de aquel país y de protección de datos personales europea. Conforme a ello, Microsoft impugnó la orden de registro y secuestro de datos sosteniendo que su cumplimiento implicaría un caso de acceso transfronterizo a datos almacenados en Irlanda por más que puedan ser accedidos desde los EEUU. Objetó la idea de que el registro se pudiera hacer desde el lugar en que los datos están disponibles (*power of dispossal*) o la posibilidad de actuar como controlador de los datos por el hecho de que la sede central de la empresa está en EEUU. Conforme a la postura de la empresa, ello significaría una violación a la cuarta enmienda y daría lugar a una intromisión en la soberanía de otro Estado violando convenciones internacionales. Siempre según la postura adoptada por Microsoft, cumplir con la pretensión del gobierno implicaría realizar un registro de datos de manera extraterritorial a través de la cooperación de Microsoft (utilización de) cuando lo correcto sería utilizar los canales de cooperación internacional existentes con Irlanda.

El gobierno de EEUU, en contraposición a la postura de la empresa, sostuvo el argumento de que el *lugar de alojamiento de la información* no era lo importante para determinar el alcance y obligatoriedad de la orden de entrega de datos, sino el poder de control real sobre los datos que, en el caso concreto, Microsoft tiene desde territorio de EEUU independientemente del lugar físico en el que los datos están alojados. El juez en primera instancia rechazó el pedido

Microsoft y la empresa presentó un recurso de apelación[91]. El trámite del recurso atrajo la atención tanto del sector gubernamental, académico, de las empresas del sector, miembros del Parlamento Europeo y de las organizaciones de la sociedad civil tanto de EEUU como de Europa que ponen de manifiesto la trascendencia de la resolución. En la apelación se han presentado importantes argumentos tanto de empresas importantes del sector como de organizaciones preocupadas por la protección de los derechos civiles en internet[92] (*amicus curiae*).

Finalmente, la cámara de apelaciones en este importante precedente, otorgó la razón a la empresa y dejó de lado la orden del Departamento de Justicia[93]. El tribunal de apelaciones sentó el precedente de que la ley americana que da sustento a este tipo de ordenes (*Stored Communications Act*, 18 US 2701), no tiene aplicación extraterritorial. Concretamente establece que esta ley no autoriza a los jueces norteamericanos a emitir órdenes contra proveedores de servicios de EEUU que los obliguen a entregar datos de contenidos de sus clientes que estén alojados en servidores ubicados en extraña jurisdicción.

En cuanto a los alcances extraterritoriales de la orden, la resolución afirma que si los datos están alojados y serían secuestrados de un *data center* ubicado en Dublín, Irlanda, el contenido de la orden se cumpliría en aquel país sin perjuicio del domicilio del cliente o de la ubicación en territorio de EEUU de la sede central de la empresa.

La resolución critica los argumentos del juez de primera instancia que fundamentaba que no se trataba de un ejercicio de poder extraterritorial basado en que no criminalizaba conductas en el estado extranjero ni implicaba la actividad de agentes estatales en el extranjero ni requiere la presencia de empleados de la empresa en el extranjero. La resolución de la Cámara de Apelaciones entiende que: "los esfuerzos narrativos no pesan adecuadamente los hechos de que el data center está ubicado en Dublín y que Microsoft necesariamente debería interactuar con estos centros de datos para poder

---

[91] Para un análisis de los detalles del caso y los argumentos jurídicos en discusión recomiendo la lectura de la apelación presentada por los abogados de la empresa Microsoft, disponible en http://digitalconstitution.com/wp-content/uploads/2014/12/Microsoft-Opening-Brief-120820141.pdf .

[92] Cf. el texto de las distintas presentaciones en su idioma original disponible en https://www.eff.org/es/cases/re-warrant-microsoft-email-stored-dublin-ireland

[93] Cf. *Microsoft Corporation v United States of America*, resuelto el 16 de Julio de 2016, United States Court of Appeals for the Second Circuit, Docket No 14-2985. Microsoft apela concretamente el rechazo al planteo de nulidad que había realizado para que se deje sin efecto la orden de que entregue el contenido de una cuenta de correo electrónico almacenado en un servidor ubicado físicamente fuera de Estados Unidos y que imponía sanciones a la empresa por no cumplir con dicha orden.

acceder y secuestrar los datos en beneficio del gobierno y que estos datos están bajo la jurisdicción de una soberanía extranjera" (Traducción de Salt[94], pág. 40 de la resolución).

Sin perjuicio de la importancia de la resolución, el tema en disputa está todavía abierto y es de esperar cambios tanto en la jurisprudencia como en la legislación interna de EEUU[95].

4. Proveedores de internet

Una particularidad de la evidencia digital en el mundo es la importancia que adquieren en las discusiones jurídicas las empresas importantes del sector informático (Microsoft, Google, Facebook, Apple, AT&T, Amazon, Accenture, Ebay, Cisco, Hewlett Packard, etc.). Estas empresas alojan los datos que finalmente serán solicitados por los Estados.

En virtud de que el problema de la evidencia digital no es sólo un problema entre Estados, sino también entre el sector estatal/privado, las empresas proveedoras intervienen en la discusión con un poder casi de un Estado (poder por el alojamiento de datos). A ello se le suma la dificultad que ni siquiera tienen la misma postura, por ejemplo, en la definición de los criterios de atribución de jurisdicción para acceder a datos en la nube. Antes bien, es posible diferenciar las posturas atendiendo a la arquitectura y características de sus servicios. Mientras algunas empresas defienden la idea de que los Estados tendrán acceso a los datos siempre que estén alojados en su territorio (ubicación de los datos), otras defienden la postura de que los Estados sólo tendrán poder para compeler a la entrega de datos si el controlador de los datos –*data controler*- tiene domicilio en su territorio, lo que puede ir variando todo el tiempo.

Empero, además, se encuentra el problema de la información recibida de manera directa de parte de empresas proveedoras de servicios de internet del sector privado de una jurisdicción diferente sin utilizar los canales de cooperación formales, ya sea que provenga de la respuesta a un requerimiento o sea enviada por iniciativa de la empresa. Se trata de una comunicación directa entre los órganos de persecución penal del Estado y una empresa privada de extraña jurisdicción sin participación alguna del Estado en el que la empresa que brinda los datos está ubicada. De hecho, las empresas incluso cuentan con un protocolo interno, casos donde proceden, reglas formas de acceso, normas que los tribunales siguen para obtener la información por fuera de canales de

---

94 Salt, Marcos G. tesis doctoral, p. 247.

95 Cfr. En todo este capítulo, Salt, tesis doctoral, p. 217 y ss.

cooperación internacional. Por ende, son las propias empresas que imponen reglas que deben seguir las autoridades estatales para obtener información.

En la práctica de los tribunales argentinos se advierte ya un importante crecimiento en el uso de estos elementos de prueba y seguramente será mucho mayor en el futuro. En general, se trata de datos de abonados y de tráfico de comunicaciones que ingresan al sistema por canales informales (en el sentido de que la información es entregada o enviada por fuera de los canales de cooperación en materia penal previstos en las normas – ya sea los tratados internacionales de asistencia legal mutua o los acuerdos interprovinciales-). La información puede provenir de una respuesta a un pedido enviado por un juez o fiscal argentino en el marco de una investigación penal concreta ya existente (de manera similar a un pedido de informes que se realizara en el marco de nuestro territorio). Incluso puede llegar por iniciativa de la empresa, por ejemplo, cuando advierte un delito que se comete desde un dispositivo que se conecta a través de dirección IP de la Argentina.

Un caso especial lo constituye la información que recibe nuestro país sobre delitos que afectan la integridad sexual de menores cometidos utilizando la tecnología de internet. La Argentina recibe información directa a través de una red VPN administrada por una ONG de EEUU de casos de explotación sexual de menores, *grooming* y pornografía infantil que se vinculan con direcciones IP de la Argentina. La información se recibe en el marco de un Convenio entre el Centro Nacional para Niños Desaparecidos y Explotados (NCMEC) y el Ministerio Público Fiscal de la Ciudad de Buenos Aires a través del Cuerpo de Investigadores Judiciales (CIJ). NCMEC es una organización sin fines de lucro con sede en los Estados Unidos de América que recibe el apoyo del Congreso de dicho país, con el fin de construir una respuesta internacional coordinada e intercambiar información respecto de la problemática de los niños desaparecidos y explotados sexualmente. Esta organización, debido a la proliferación de hechos delictuosos contra menores de edad existentes en internet, estableció un mecanismo centralizado donde los proveedores de servicios de internet (por ejemplo, Google, Facebook, Microsoft) reportan actividades sospechosas relacionadas a la explotación sexual de los niños. Dicho mecanismo se denomina *CyberTipline* y recibe reportes efectuados por los proveedores de los diversos servicios de internet que están obligados a informar cuando tienen conocimiento de estos hechos. La organización envía un reporte al FBI con los datos necesarios para que se dé inicio a una investigación (fecha y hora del hecho, identificación del usuario sospechado y determinación geográfica de la IP utilizada para cometer el hecho). El ministerio Público de la CABA firmó un convenio que le permite tener acceso virtual directo al servidor donde funciona la CyberTipline a fin de acceder a la información de los hechos cometidos contra menores de edad por parte de usuarios de Argentina. A su vez

el Ministerio Publico de la CABA firmó un convenio con la Red de Procuradores Fiscales de todo el país para distribuir los casos de acuerdo a la jurisdicción de su comisión. Esta información ha determinado un aumento importante en los casos ingresados al sistema y en la eficiencia de su persecución. Puesto que las normas procesales vigentes no prevén de manera alguna la forma de incorporar estos elementos de prueba, ni los habilita ni los prohíbe de manera expresa, su utilización debería ser limitada, ya sea como noticia del delito (cuando el dato es el disparador o inicio de una investigación) o como un indicio más que debe ser corroborado con otros medios de prueba para servir como elemento de convicción fundante de resoluciones importantes del proceso, teniendo en consideración que no reúne las condiciones de confiabilidad propias de una información recibida de acuerdo a los estándares previstos en tratados de asistencia legal mutua[96].

[96] Cfr. Salt, su tesis doctoral, p. 258.

5. Los problemas jurídicos de la evidencia digital en Argentina

En Argentina, pocos problemas jurídicos han sido tan complejos en el proceso penal desde sus inicios, como lo es el de la *evidencia digital*. Si se le presta la atención que exige el tema, ello puede llegar a modificar toda la forma en que en nuestros sistemas han regulado los medios de prueba, principalmente, medios de coerción probatorios o medios de investigación. Uno de los aspectos más complejos a resolver es que el asunto —si es posible— debe ser zanjada a futuro. Es que —si es abordada de manera seria— las decisiones que se tomen a principios del siglo XXI nos regirán por los próximos 50 o 100 años.

En este contexto, regular medios tecnológicos ya conocidos, ajustar normativa a lo que ya establecido, en todo caso, parece carecer de demasiado sentido. En todo caso, la normativa interna en todo momento va a estar *corriendo de atrás* a la tecnología. Ello nos llevará que una secuencia sin fin, nunca solucionaremos el problema: ¿es legítimo aplicar nuevos medios de prueba, coercitivos o de investigación no previstos aplicando analógicamente medios tradicionales? Si lo es, ¿de qué modo? ¿debemos modificar e ir regulando nuevos medios a medida que van surgiendo? ¿ello implica una única decisión para el sistema? Incluso si debemos regular medios novedosos, el real desafío es establecer estándares (normativos, jurisprudenciales, ello debe ser estudiado detenidamente) que permitan que el proceso penal se ajuste de manera automática (a excepción de cuestiones muy puntuales) a los avances tecnológicos.

Lo cierto es que nuestro sistema no suele examinar estas cuestiones, ni presta atención al modo de hacerlo, meramente *simplifica* soluciones que luego intenta legitimar.

A.En *Argentina*, la Convención de Budapest fue propiciada para regular la cooperación internacional en materia de persecución de delitos informáticos y la asistencia internacional para la obtención de evidencia digital para la investigación de cualquier delito.

En el año 2008 el Poder Ejecutivo Nacional conformó a una comisión integrada por representantes del Ministerio de Relaciones Exteriores, Comercio Internacional y Culto, del Ministerio de Justicia, Seguridad y Derechos Humanos, de la Oficina Nacional de Tecnologías de Información dependiente de la Subsecretaría de Tecnologías de Gestión de la Secretaría de Gestión Pública de la Jefatura de Gabinete de Ministros, del Ministerio Público Fiscal de la Nación, expertos del sector académico y de las empresas privadas a fin de analizarla y determinar si sus principios y normativa se adecúan a los principios constitucionales de nuestro sistema penal. La comisión, salvo algunas objeciones y recomendaciones de reservas respecto a algunos artículos, destacó

la conveniencia del Convenio para nuestro país como herramienta de cooperación en materia de delitos informáticos. En el marco de la Conferencia sobre Cooperación contra el Cibercrimen (*Octopus Interface Conference: Cooperation against Cybercrime*), organizada por el Consejo de Europa y desarrollada entre los días 23 y 25 de marzo de 2010 en Estrasburgo, Francia, la delegación argentina hizo entrega a las autoridades del mencionado organismo regional de la solicitud del Jefe de Gabinete de Ministros para que el país fuese invitado a acceder a la Convención de Budapest. El 20 de septiembre del año 2010, el Consejo de Europa, luego de un proceso de consulta con todos los países miembros de la Convención, remitió la invitación formal a la República Argentina para acceder a la Convención de Budapest[97]. La ley 27.411[98] aprobó la Convención de Budapest, de la cual, Argentina ya es miembro.

Algunos autores especialistas en el tema entendieron que concretar el objetivo de acceder a la Convención de Delitos Informáticos del Consejo de Europa (Convención de Budapest) constituiría un paso importante para la Argentina en el proceso de modernización de su sistema penal, que ello le permitiría mejorar el marco normativo necesario para hacer frente a los desafíos que genera al sistema penal los delitos informáticos y, asimismo, contar con herramientas procesales y de cooperación internacional modernas que permitan obtener, de manera eficiente y respetuosa de las garantías individuales, evidencias en entornos digitales necesarias para la investigación de cualquier delito. Y que, puesto que se trata de una convención *viva*, en el sentido de que no es solamente un texto normativo rígido, sino que los países miembros han implementado un sistema de trabajo que está en constante movimiento generando nuevos instrumentos de interpretación, capacitación y

---

[97]Cf. http://www.coe.int/en/web/portal/octopus-conference-cybercrime-2012.

[98] Con reservas previstas en el ARTÍCULO 2°.- Al depositarse el instrumento de adhesión deberán efectuarse las siguientes reservas:a) La REPÚBLICA ARGENTINA hace reserva del artículo 6.1.b. del CONVENIO SOBRE CIBERDELITO y manifiesta que no regirá en su jurisdicción por entender que prevé un supuesto de anticipación de la pena mediante la tipificación de actos preparatorios, ajeno a su tradición legislativa en materia jurídico penal. b) La REPÚBLICA ARGENTINA hace reserva de los artículos 9.1.d., 9.2.b. y 9.2.c. del CONVENIO SOBRE CIBERDELITO y manifiesta que estos no regirán en su jurisdicción por entender que son supuestos que resultan incompatibles con el CÓDIGO PENAL vigente, conforme a la reforma introducida por la ley 26.388. c) La REPÚBLICA ARGENTINA hace reserva parcial del artículo 9.1.e. del CONVENIO SOBRE CIBERDELITO y manifiesta que no regirá en su jurisdicción por entender que el mismo sólo es aplicable de acuerdo a legislación penal vigente hasta la fecha, cuando la posesión allí referida fuera cometida con inequívocos fines de distribución o comercialización (artículo 128, segundo párrafo, del CÓDIGO PENAL). d) La REPÚBLICA ARGENTINA hace reserva del artículo 22.1.d. del CONVENIO SOBRE CIBERDELITO y manifiesta que no regirá en su jurisdicción por entender que su contenido difiere de las reglas que rigen la definición de la competencia penal nacional. e) La REPÚBLICA ARGENTINA hace reserva del artículo 29.4 del CONVENIO SOBRE CIBERDELITO y manifiesta que no regirá en su jurisdicción por entender que el requisito de la doble incriminación es una de las bases fundamentales de la LEY DE COOPERACIÓN INTERNACIONAL EN MATERIA PENAL N° 24.767 para el tipo de medidas de cooperación previstas en artículo y numeral citados.

modificaciones normativas que atienden a las necesidades que plantea la tecnología informática y de esta manera poder acceder a participar en este proceso de toma de decisiones de influencia global, disminuyendo, aunque sea mínimamente, la relación de desventaja en la que se encuentra frente a los países centrales en la definición de estas políticas de trascendental importancia en el mundo actual[99].

Sin embargo, estas parecen expectativas demasiado optimistas. Ingresar en la Convención es necesario para la Argentina, pero en nada soluciona los problemas jurídicos referidos al proceso penal, pues el camino para un examen serio de la cuestión, no es posible simplificarlo con la incorporación de normas a las leyes de forma. Diferente es el caso de las penales pues implican el avance en la tipificación de determinadas conductas. En algunos casos no será necesario pues es posible la aplicación analógica en nuestro sistema, y lo que debe solucionarse aún es de qué modo esta aplicación debe realizarse. La tarea jurídica por delante es este desafío, que no se enmienda con la incorporación de Argentina a la Convención. Las discusiones jurídicas más profundas de los reales problemas del moderno derecho procesal penal en modo alguno se agotan, ni finalizan con la Convención ni la adaptación a su normativa, que incluso a esta altura puede ya no resultar novedosa. En este sentido, la normativa procesal penal en Argentina será realmente novedosa y moderna en tanto prevea la evolución tecnológica que resulta mucho más veloz que las reformas normativas.

El otro desafío que enfrenta Argentina en su incorporación es el congeniar la agenda propia del Consejo de Europa (que igual lo hace en todos los países hayan o no ratificado la Convención) que no tiene como fin último específicamente el resguardo de derechos civiles para los ciudadanos de países periféricos como Argentina sino unificar normas, incorporar las redes 24/7, flexibilizar normas de cooperación internacional, etc. con el objeto de lograr eficacia y celeridad en la investigación de estos delitos. Para ello, propicia la incorporación de países a la Convención, promueve la formación de operadores del sistema, envía expertos, etc., a los diferentes países donde se producen modificaciones legislativas, de manera tal que, con diferencias menores, las normas suelen contener las previsiones de la Convención.

La Cooperación Internacional aunque no lo declama expresamente sabe que la cuestión no se circunscribe a la Convención de Budapest, ni a la denominada *ciberdelincuencia*, sino que la forma en que se administran los medios tecnológicos que ponen en jaque la misma soberanía de las naciones y por ello trabajan (en todos los continentes y países con diferentes expertos para influir el

[99] Salt, Marcos G., tesis doctoral, p. 20

modo en que estas cuestiones son discutidas, y solucionadas) en la forma de regular la interacción en el mundo que nos regirá en todo este siglo (del mismo modo que sucedió con los tratados internacionales, bilaterales y la forma de relacionarse entre Estados, o el mar, el espacio, etc.)

Las medidas que proponen son presentadas como atractivas, y supuestamente eficaces, y en muchos aspectos beneficiosas para el país, sin embargo, deben ser minuciosamente estudiadas para encontrar un adecuado equilibrio con la protección de los derechos de sus ciudadanos y el respecto la soberanía.

B. En *Argentina* existe una escasa regulación de nuevos medios tecnológicos. Del mismo que ha sucedido en el resto de la región, los diferentes estados provinciales han ido reformando sus leyes procesales en los últimos 20 años. Sin embargo, esta extensa actividad reformista no ha llegado a la incorporación de normativa que solucione en forma alguna el problema de la evidencia digital, ni ha tenido una incorporación de medios tecnológicos novedosos. En este sentido, y a modo ejemplo, el devenir del CPPN, en ese aspecto, es el que han tenido los códigos provinciales.

Los diferentes códigos procesales penales en Argentina han seguido el mismo esquema (con pequeñas diferencias) en las medidas de coerción probatorias: regulan el allanamiento, la requisa, la intercepción de la correspondencia, la intervención de las comunicaciones. Adviértase que correspondencia y comunicaciones suelen tener regulaciones diferenciadas, ello seguramente tendrá motivos más históricos que jurídicos, en el sentido, que la correspondencia era la única manera de comunicarse hasta principios del siglo XX, en donde la comunicación telefónica amplió el espectro. El legislador ha tomado la decisión de regular las formas de comunicarse de modo diferenciado. A principios ya del siglo XXI, las maneras de comunicarse se vuelven tan diversas, lo que nos debe incitar a la reflexión si la regulación de las formas de intromisión de las comunicaciones no debería unificarse para evitar discusiones en el futuro sobre las nuevas maneras tecnológicas de comunicarse.

Con relación a las intervenciones telefónicas el CPPN, el art. 236, no sólo prevé la orden judicial para intervención del contenido de la comunicación sino también de los datos de tráfico, de manera tal que le ha dado carácter de dato protegido por el derecho a la intimidad.

En cuanto a la correspondencia, la jurisprudencia ha equiparado la correspondencia electrónica a la epistolar, no obstante, el legislador nacional al dictar la ley 26.388 de delitos informáticos ha equiparado en la tipificación la protección de la correspondencia epistolar a la electrónica (CP, 153), de manera que, al menos en el ámbito federal se ha eliminado cualquier objeción referida a

su intercepción, pues ya una ley establece la equiparación. Más discutible podría ser para los estados provinciales en tanto la regulación de los códigos de forma no han sido delegados al Congreso Nacional[100].

El Código Procesal Penal de la Provincia de *Neuquén*[101] prevé una norma para habilitar el registro y secuestro de datos en equipos informáticos encontrados en el marco de un allanamiento y agrega, sin mayores condiciones ni requisitos especiales, la posibilidad de los registros remotos: Artículo 153º Información digital. Cuando se hallaren dispositivos de almacenamiento de datos informáticos que por las circunstancias del caso hicieran presumir que contienen información útil a la investigación, se procederá a su secuestro, y de no ser posible, se obtendrá una copia. O podrá ordenarse la conservación de los datos contenidos en los mismos, por un plazo que no podrá superar los noventa (90) días. Quien deba cumplir esta orden deberá adoptar las medidas necesarias para mantenerla en secreto. También podrá disponerse el registro del dispositivo por medios técnicos y en forma remota…."[102]

La 27.063 [103], el nuevo CPPN (no vigente), avanzó en la regulación de nuevas medidas: "Artículo 143.- *Interceptación*. Siempre que resulte útil para la comprobación del delito, el juez podrá ordenar, a petición de parte, la interceptación y secuestro de correspondencia postal, telegráfica, electrónica o cualquier otra forma de comunicación o de todo otro efecto remitido por el imputado o destinado a éste, aunque sea bajo nombre supuesto.
Se procederá de modo análogo al allanamiento.
La intervención de comunicaciones tendrá carácter excepcional y sólo podrá efectuarse por un plazo máximo de treinta (30) días, pudiendo ser renovada, expresando los motivos que justifican la extensión del plazo conforme la naturaleza y circunstancias del hecho investigado.

---

[100] En un sentido diferente, cfr. Salt, tesis doctoral.

[101] Ley 2784 del año 2011.

[102] Criticado por Salt, tesis doctoral, p. 98: "Según entiendo, esta norma ya vigente en la provincia de Neuquén, no prevé un sistema de garantías adecuado para regular este mecanismo intrusivo. Del texto de la norma parece surgir que asimila los requisitos a los previstos para el allanamiento. Si bien habilita la medida legalmente bajo autorización judicial, la falta de claridad sobre los supuestos en los que puede ser aplicada y la posibilidad de afectación al principio de proporcionalidad ponen en duda su legitimidad constitucional".

[103] Sancionada el 4/12/2014, ley procesal que reforma el CPPN, es ley vigente sin embargo, no ha entrado en vigencia efectiva (*vacatio legis*) a la espera de una ley de implementación que aún no pareciera estar regulándose, y continuamente se prevén proyecto de reformulación de esta ley, cfr. Salt, tesis doctoral, p. 98.

La solicitud deberá indicar el plazo de duración que estime necesario según las circunstancias del caso. El juez controlará la legalidad y razonabilidad del requerimiento y resolverá fundadamente.
Rige para los funcionarios encargados de efectuar la intervención el deber de confidencialidad y secreto respecto de la información obtenida por estos medios, excepto respecto de la autoridad que la haya requerido. Quienes incumplan este deber incurrirán en responsabilidad penal.
Las empresas que brinden el servicio de comunicación deberán posibilitar el cumplimiento inmediato de la diligencia, bajo apercibimiento de incurrir en responsabilidad penal.
Si los elementos de convicción tenidos en consideración para ordenar la medida desaparecieren, hubiere transcurrido su plazo de duración o ésta hubiere alcanzado su objeto, deberá ser interrumpida inmediatamente.
Artículo 144.- *Incautación de datos.* El juez podrá ordenar a requerimiento de parte y por auto fundado, el registro de un sistema informático o de una parte de éste, o de un medio de almacenamiento de datos informáticos o electrónicos, con el objeto de secuestrar los componentes del sistema, obtener copia o preservar datos o elementos de interés para la investigación, bajo las condiciones establecidas en el artículo 129.
Regirán las mismas limitaciones dispuestas para el secuestro de documentos.
El examen de los objetos, documentos o el resultado de la interceptación de comunicaciones, se hará bajo la responsabilidad de la parte que lo solicitó.
Una vez secuestrados los componentes del sistema, u obtenida la copia de los datos, se aplicarán las reglas de apertura y examen de correspondencia.
Se dispondrá la devolución de los componentes que no tuvieran relación con el proceso y se procederá a la destrucción de las copias de los datos. El interesado podrá recurrir al juez para obtener la devolución de los componentes o la destrucción de los datos".

Por fuera de estas disposiciones las leyes procesal penales no prevén normas novedosas, sin embargo, ello no ha impedido al sistema recolectar *evidencia digital*.

C. La aplicación del principio de la libertad probatoria y la *nulla coactio sine lege*. La falta de normas procesales específicas que regulen los diferentes supuestos de evidencia digital u obtenida en entornos digitales, ha sido suplida, con la aplicación del *principio de libertad probatoria*. El problema es que, en general, ello sucede sin realizar un examen adecuado de la limitación constitucional, ni en la forma en dicha aplicación debe realizarse.

I. A diferencia de lo que sucede en el derecho privado, en el ámbito del derecho procesal penal rige el principio de libertad probatoria. En el proceso penal todo objeto de prueba puede ser probado y por cualquier medio. Es por ello que, en

principio, es posible la aplicación analógica de medios probatorios regulados[104]. Ello ha permitido en la práctica de los tribunales el uso en el marco de los procesos penales de estos novedosos medios de investigación y prueba y la incorporación de los elementos de prueba digital así obtenidos.

Sin embargo, existen excepciones a este principio, entre las que a este informe importan[105], la excepción más importante se refiere a las limitaciones probatorias de origen constitucional, esto es, cuya fuente reside en la protección que se otorga a las personas en un Estado de Derecho, por razón de su dignidad (derechos humanos)[106]. De manera tal que el principio de libertad probatoria no es absoluto y no podría avalar las pruebas obtenidas en violación a garantías constitucionales o prohibidas por la ley (ya sea que la limitación recaiga sobre el objeto de la prueba —límite absoluto— o respecto a los órganos, medios o procedimientos probatorios –limitaciones relativas—).

De este modo, el principio de libertad probatoria no puede ser interpretado como una autorización abierta para que el Estado haga cualquier cosa en la búsqueda de la verdad, aun cuando actúe bajo la justificación de que el hecho ilícito investigado sea de especial gravedad (en el ámbito informático, por

---

[104]Ello significa la admisión implícita de que en materia procesal penal es posible aplicar por analogía las normas que regulan los medios de prueba reglados a medios no previstos expresamente, aun cuando ello pueda ser una aplicación analógica que perjudique a la persona imputada (cuestión vedada en materia de interpretación de las normas penales de fondo en virtud del principio de legalidad penal -CN, art. 18-). Conforme a ello, el principio de legalidad penal previsto en el texto constitucional (CN, art. 18) que tiene como una de sus derivaciones la imposibilidad de interpretar analógicamente las normas en perjuicio del imputado sólo tendría aplicación en materia penal sustantiva y solamente de manera limitada en materia procesal penal. Sostiene una postura diferente Pérez Barberá: "…el principio de legalidad penal tiene también aplicación en el derecho procesal penal, por mandato constitucional, independientemente de la existencia o no de disposiciones procesales específicas que ordenen una interpretación restrictiva para ciertos casos, o que expresamente establezcan que todo puede ser probado con cualquier medio de prueba…" "…conforme a la tesis que aquí se defiende, la posibilidad de comprobación de un hecho que consolide la hipótesis acusatoria a través de un medio de prueba no reglado expresamente por la ley procesal vigente es un acto irregular, y más precisamente inconstitucional, por ser violatorio del principio de legalidad penal…" (el resaltado me pertenece). Posteriormente en el mismo trabajo postula la inconstitucionalidad del principio de libertad probatoria: "…la única solución para este problema, acorde con un Estado de derecho, es respetar en toda su amplitud el principio de legalidad penal también en el derecho procesal penal, y rechazar por tanto el principio de libertad probatoria, por inconstitucional. El autor entiende que esta afirmación sólo podría ser dejada de lado si se interpretara que el principio de libertad probatoria solamente implica que puede probarse cualquier hecho jurídico penalmente relevante a través de cualquier medio de prueba expresamente reglado". Ver Pérez Barberá, Gabriel, *Nuevas Tecnologías y libertad probatoria en el proceso penal*, ponencia presentada en el VI Encuentro Nacional de Profesores de Derecho Procesal Penal realizado en la ciudad de Salta, mayo de 2009.

[105] Este principio admite como límite, la prueba de hechos que de acuerdo a una ley material no pueden ser acreditados o deben ser probados de una manera especial prevista específicamente en la ley.

[106]Maier, Julio, B.J; *Derecho procesal penal argentino*, Tomo I, Editores del Puerto, 1996, p. 697.

ejemplo, la pornografía infantil). Antes bien, el Estado no puede utilizar todos los medios de prueba disponibles desde un punto vista fáctico sino solamente aquellos que, además, pueden ser obtenidos e incorporados al proceso conforme a derecho.

II. Es el principio *nulla coactio sine lege* que determina que todos aquellos mecanismos de investigación, procedimientos probatorios o medios de prueba que impliquen algún grado de injerencia[107] (o la utilización de coerción) en el ámbito de derechos fundamentales reconocidos por la Constitución Nacional o los Pactos internacionales de Derechos Humanos de jerarquía constitucional (CN, art. 75. Inc. 22) deben estar previstos en leyes que, por otra parte, deben cumplimentar los requisitos propios de la reglamentación constitucional que exige que el legislador no altere, sustituya o modifique el principio constitucional que reglamenta (CN, arts. 14, 19 –segunda parte- y 28 y, de manera expresa, en el art. 30[108] de la Convención Americana de Derechos Humanos). Según este principio, vinculado también al principio de legalidad o de reserva[109] (diferente al principio que con la misma nomenclatura guía la actividad penal –*nullum crimen sine lege*-) 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 tienen como condición de validez una autorización legal previa[110].

En nuestro medio jurídico, Gustavo Bruzzone advirtió con total acierto la necesidad de diferenciar los *medios de prueba en general* de las *medidas de*

---

[107] La injerencia de carácter general modernamente se refiere a todo acto u omisión estatal que de cualquier manera afecta a un derecho fundamental, sea a través de un acto jurídico o una actuación u omisión meramente fáctica; a través de un acto jurídico imperativo o meramente declarativo; con o sin la finalidad de afectar el derecho de que se trate; a través de una afectación directa, mediata o inmediata, cfr. Pérez Barberá, Gabriel, *Reserva de ley, principio de legalidad y proceso penal*, publicado en http://www.pensamientopenal.com.ar/system/files/2015/12/doctrina42610.pdf.

[108] "Las restricciones permitidas, de acuerdo con esta Convención, al goce y ejercicio de los derechos y libertades reconocidas en la misma, no pueden ser aplicadas sino conforme a leyes que se dictaren por razones de interés general y con el propósito para el cual han sido establecidas".

[109] Gabriel Perez Barberá prefiere usar el concepto "principio general de reserva de ley" precisamente para diferenciarlo del principio de legalidad penal. Ver, *El Principio General de Reserva de Ley (o principio general de legalidad en la doctrina alemana)*, ob. Cit., pág. 331.

[110] La Corte Interamericana de Derechos Humanos (CIDH) tuvo oportunidad de aclarar qué debe entenderse por "ley" a los fines de la interpretación del Art. 30 de la convención en una opinión consultiva emitida a pedido del Gobierno de Uruguay: "...que la palabra leyes en el artículo 30 de la Convención significa norma jurídica de carácter general, ceñida al bien común, emanada de los órganos legislativos constitucionalmente previstos y democráticamente elegidos, y elaborada según el procedimiento establecido", OC 6/86 del 9 de mayo de 1986. Texto completo disponible en http://www.corteidh.or.cr/docs/opiniones/seriea_06_esp.pdf

coerción probatoria[111]. Y ha establecido sobre la evidencia digital: "Es decir que hay amplitud en materia probatoria. Si los adelantos técnicos descubren o desarrollan nuevos elementos probatorios o de acreditación de circunstancias relevantes para el proceso, y se encuentran en consonancia con el respecto a la dignidad humana, las pruebas que de ellos se deriven podrán ser incorporadas fácilmente porque el sistema, en principio, salvo excepciones como las antes señaladas, es abierto"[112]. Cualquier necesidad que tenga el Estado de ejercer coerción o cualquier actividad que implique una injerencia en ámbito de garantías fundamentales para obtener datos, ellos sólo podrán usarse válidamente si están expresamente previstos en el texto legal, resultando prohibidos cualquier aplicación analógica de normas habilitantes[113].

D. El derecho a la intimidad[114].

I.*a)* La Constitución Nacional y los tratados internacionales de Derechos humanos de jerarquía constitucional (CN, art. 75, inc. 22) prevén un marco de protección fuerte de la privacidad e intimidad en sus diferentes formas y manifestaciones.

En este caso, el avance de la tecnología nos obliga a analizar jurídicamente un ámbito de intimidad de características especiales. Se trata de un ámbito de intimidad personal construido y derivado de la particular vinculación entre las personas y los sistemas informáticos con los que se relacionan. De la mano de los avances tecnológicos y del mayor acceso por parte de la población a las herramientas informáticas y de telecomunicaciones se torna más evidente un vínculo diferente a lo conocido hasta ahora entre el hombre y las herramientas tecnológicas con las que interactúa.

---

[111] Ver Gustavo Bruzzone, *La nulla coactio sine lege como pauta de trabajo en materia de medidas de coerción en el proceso penal*, publicado en AAVV, *Estudios sobre Justicia Pena*l. *Homenaje al Profesor Julio B.J. Maier*, Editores del Puerto, Buenos Aires, 2005, pág. 245, en un sentido similar, Perez Barberá, Gabriel, *El Principio General de Reserva de Ley (o principio general de legalidad en la doctrina alemana)*,y también la tesis de Salt, Marcos, p. 26.

[112] Gustavo Bruzzone, ob. cit. pág. 247

[113] Pérez Barberá lo denomina como "Prohibición de analogía Contraindividual": "…cuando se trata de actuaciones estatales que pueden importar una afectación (una injerencia) en derechos individuales de carácter fundamental corresponde inferir del principio general de reserva de ley una prohibición de analogía para proteger eficazmente a esos derechos, es decir, una prohibición de analogía in *malampartem* o contraindividual", pág. 365.

[114] Salt, tesis, p. 106

Algunas constituciones han modificado sus normas atendiendo a las implicancias de nuevas tecnologías[115], abarcando un ámbito de intimidad y privacidad *novedoso*. Las constituciones provinciales han regulado de manera más amplia el contenido de los derechos y garantías previstos en la CN y leyes tanto de fondo como de procedimiento que reglamentan y delimitan el contenido de las garantías. Así, la Constitución de Córdoba significa un avance en términos de profundizar la claridad sobre el alcance de los límites al Estado, al regular de manera más precisa las condiciones que habilitan el allanamiento del domicilio y la intercepción de papeles privados, correspondencia y comunicaciones, dejando un ámbito menor a la interpretación del legislador al momento de reglamentar legalmente el contenido de la garantía. Así, regulando la protección del domicilio, el Artículo 45 de la constitución provincial establece: "Inviolabilidad del domicilio – Allanamiento. El domicilio es inviolable y sólo puede ser allanado con orden motivada, escrita y determinada del juez competente, la que no se suple por ningún otro medio. Cuando se trate de moradas particulares, el registro no puede realizarse de noche, salvo casos sumamente graves y urgentes". A su vez, el Artículo 46 regula la protección de los papeles privados y comunicaciones: "El secreto de los papeles privados, la correspondencia epistolar y cualquier otra forma de comunicación personal por el medio que sea, es inviolable. La ley determina los casos en que se puede proceder al examen o interceptación mediante orden judicial motivada". Especial interés reviste el artículo 50 que prevé de manera específica garantías en relación al procesamiento de datos informáticos: "Artículo 50: Privacidad. Toda persona tiene derecho a conocer lo que de él conste en forma de registro, la finalidad a que se destina esa información, y a exigir su rectificación y actualización. Dichos datos no pueden registrarse con propósitos discriminatorios de ninguna clase ni ser proporcionados a terceros, excepto cuando tenga un interés legítimo. La ley reglamenta el uso de la informática para que no se vulneren el honor, la intimidad personal y familiar y el pleno ejercicio de los derechos".

De hecho, algunos autores consideran que se trata de una novedad no prevista por la CN (por ejemplo, Salt[116]), que sólo ha previsto la protección del *habeas data* introducida con la reforma de la CN de 1994, limitada a un aspecto del derecho de los ciudadanos frente al desafío del procesamiento de los datos, y que la analogía no permite un adecuado resguardo de la garantía constitucional. Por ende, concluye que la lógica indica que esta mayor potencialidad de

---

[115] Así a modo de ejemplo, la Constitución de España en el art. 18 inc. 4 establece que "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"; la Constitución alemana en el art. 13 relativo a la inviolabilidad de domicilio prevé un inciso para regular la posibilidad de utilizar medios técnicos para para la vigilancia acústica de un domicilio (reforma del 26/3/1998.

[116] Cfr. Su tesis doctoral, p. 106.

intromisión que habilitan las herramientas informáticas requiere un tratamiento diferente, aún desde la óptica de la misma garantía.

b) El texto constitucional de 1853 prevé las garantías de privacidad e intimidad en dos artículos separados (CN, arts. 18 y 19). La doctrina constitucional más calificada ha destacado la diferencia entre ambos conceptos, la privacidad como un concepto más amplio que abarca la protección de todas las acciones que no afecten a terceros y la intimidad como una esfera de protección de la persona que queda exenta del conocimiento de terceros[117]. Sin perjuicio de ello, no se trataría de una superposición de normas constitucionales, sino que, por el contrario, se complementan. En lo que se refiere a la intimidad de comunicaciones el art. 19 de la CN protege de manera general las comunicaciones privadas que no afecten a terceros, protección absoluta que no admite límites. El hecho de que no afecten a terceros las hace inviolables de forma absoluta y en el caso de que fueran conocidas por el Estado tornaría obligatorio devolverlas al estado anterior de intimidad, por ejemplo, destruyendo los registros. En el caso de que exista una afectación a terceros pierden la inmunidad total frente a injerencias del Estado pero no su carácter de íntimas, que las protege frente a ingresos arbitrarios del Estado o no respetuosos de las garantías impuestas[118].

El derecho a la privacidad en su acepción más amplia ha sido establecido en el artículo 19 de la CN de 1853 establece: "Las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un

---

[117]En nuestra doctrina constitucional, Carlos Nino ha expuesto con claridad la diferencia entre los que denomina bienes de la privacidad e intimidad regulados de manera diferente en el texto constitucional: "…privacidad entendida no como equivalente a intimidad sino en lo que se refiere a las acciones voluntarias de los individuos que no afecten a terceros…". Con ello se refiere Nino a acciones privadas no en el sentido de que no deben ser accesibles al conocimiento público sino de que deben mantenerse incólumes de la injerencia estatal salvo que afecte a terceros. Resume la privacidad como la libertad de realizar cualquier acción que no cause daños a los demás, La intimidad, en cambio se refiere a una esfera de la persona que está exenta del conocimiento generalizado por parte de los demás. Cf. Carlos Nino, *Fundamentos de Derecho constitucional*, pág. 304 y ss. En el mismo sentido la tesis doctoral de Gustavo Garibaldi, con el interés que reviste para esta investigación al estar dirigida a analizar la incidencia de las modernas tecnologías de control del delito en el Derecho Penal y en los principios constitucionales. Señala el autor: "Llamaré privacidad al derecho irrestricto de realizar, en todo tiempo y lugar, acciones que el Estado no puede prohibir porque carecen de aptitud para provocar daño a terceros. A su vez me referiré a la intimidad, como la esfera de la personalidad que cada uno puede mantener fuera del conocimiento generalizado", ob. cit. Pág. 91. Otro sector de la doctrina se inclina por extraer el derecho a la intimidad del art. 19. De todas formas, coincido con Julio Maier en el carácter meramente académico de la discusión o de claridad analítica pero que no incide en la presencia de la garantía independientemente del artículo constitucional en el que encuentre andamiaje ya sea como derivación del art. 19 o como aplicación extensiva del artículo 18. Cf. Maier Julio, "*DPPA"*, tomo III, especialmente nota 416.

[118] Cf. García, Luis, *La intervención de las comunicaciones telefónicas y otras telecomunicaciones en el Código Procesal Penal de la Nación: un cheque en blanco para espiar nuestra vida privada*, publicado en "Cuadernos de Doctrina y Jurisprudencia Penal", nro. 6, 1997, editorial Ad Hoc, Buenos Aires, pág. 407 y ss.

tercero, están sólo reservadas a Dios, y exentas de la autoridad de los magistrados. Ningún habitante de la Nación será obligado a hacer lo que no manda la ley, ni privado de lo que ella no prohíbe". Esta norma protege privacidad en el sentido de mantener incólume un ámbito de protección del individuo que le permita realizar todas las acciones que no afecten a terceros, sea que ellas se realicen de manera privada o pública. Se trata de una inmunidad que protege a los ciudadanos de acciones del Estado que puedan intervenir o coartar la autonomía individual para cualquier idea pensamiento o actividad que no signifique una afectación a terceros (expresado en el texto del artículo constitucional como orden y moral pública). Así, el artículo 19 de la CN refleja una idea más amplia que la de proteger el bien *intimidad*. Protege la privacidad como forma de plasmar los ideales de la concepción liberal en el plano de la autonomía personal garantizando todos aquellos bienes necesarios para asegurar la libre elección de un plan de vida sin interferencias estatales, salvo cuando afecte a terceros. Asimismo, tal como ha sido rescatado por un sector de la doctrina, esta idea de *privacidad* permite también justificar la necesidad de garantizar la protección de la intimidad (en el sentido estricto de no conocimiento de terceros) de determinados datos o cuestiones cuando ellos puedan significar un menoscabo en la autonomía individual, cuestión que puede ser importante a los fines de esta investigación en la medida que resulta necesario analizar el resguardo de los ciudadanos frente a la intromisión del Estado en sus sistemas informáticos.

La protección de la *intimidad* está prevista en el art. 18 de la CN que reúne todas las garantías constitucionales frente al poder penal del Estado y que, en el párrafo pertinente, establece: "…El domicilio es inviolable, como también la correspondencia epistolar y los papeles privados; y una ley determinará en qué casos y con qué justificativos podrá procederse a su allanamiento y ocupación…". Así, el art. 18 garantiza la intimidad entendida como la posibilidad de excluir a terceros (incluido el Estado) del conocimiento de determinados hechos, circunstancias, comunicaciones o datos registrados en diferentes soportes. La norma se refiere de manera expresa a lo que sucede en un domicilio, lo que se registró en papeles privados o lo que se comunicó en una carta –correspondencia epistolar-, ello también es abarcado, por ejemplo, por el secreto bancario o fiscal y otros aspectos de la vida de un individuo, las comunicaciones telefónicas y otro tipo de comunicación mantenida por medios electrónicos como el correo electrónico o la comunicación a través de voz ip[119]. Lo contrario implicaría dejar sin protección constitucional aspectos trascendentales para la intimidad de los ciudadanos como pueden ser sus

[119] Cf. Alejandro Carrió, *Garantías constitucionales en el Proceso Penal,* 5 edición actualizada y ampliada, Editorial Hammurabi, Buenos Aires, 2008, pág. 353 y ss. El autor analiza el tema y la jurisprudencia respecto a situaciones especiales como la vigencia de la protección respecto a otros espacios físicos como automóviles o los armarios en el ámbito laboral o a otro tipo de comunicaciones como las telefónicas o los correos electrónicos.

conversaciones telefónicas y, más modernamente, las comunicaciones electrónicas y los documentos contenidos en soportes digitales. Correctamente, en la interpretación dinámica de la CN, Alejandro Carrió sostiene una tesis amplia que parece adecuarse más a una interpretación teleológica del texto constitucional que tiene en cuenta no sólo la letra de la norma sino sus antecedentes y la ideología liberal que lo inspira y que tiene como fundamento la idea de que, aun con matices, los ámbitos de privacidad e intimidad de las personas deben ser protegidos para garantizar el libre desarrollo de la personalidad[120]. El autor fundamenta una interpretación más amplia de la protección como derivación de la defensa en juicio de las personas y de los derechos (CN, art. 18) y del reconocimiento del texto constitucional de extender los derechos explícitos a los derechos no enumerados (CN, art. 33). De allí extrae que la esfera de intimidad protegida constitucionalmente se extienda a ámbitos donde las personas manifiestan una especial expectativa que por otra parte aparezca como razonable para los intereses estatales[121].

La garantía de intimidad prevista en el art. 18 de la CN, a diferencia de la privacidad prevista en el art. 19, no es absoluta. Antes bien, la misma norma constitucional prevé supuestos admitidos de injerencia estatal y delega la regulación de los casos y las condiciones en que estas injerencias se pueden producir a la legislación[122]. Esta materia es propia del desarrollo de las garantías constitucionales en los códigos procesales penales.

Las normas constitucionales referidas a la privacidad e intimidad, se han visto reforzadas en el bloque de constitucionalidad con la incorporación de los Pactos internacionales de Derechos Humanos. En ellos, la diferenciación entre privacidad e intimidad no aparece tan clara como en nuestro texto

---

[120]Ibid, pág. 437: "A través de fórmulas tales como la que protege la inviolabilidad del domicilio (art. 18), o la que señala que las acciones privadas de los hombres… están exentas de las autoridad de los magistrados (art. 19), nuestra constitución ha consagrado ámbitos de privacidad que con distintos matices, quedan protegidos de una indiscriminada invasión estatal…"

[121] En el mismo sentido, sobre la extensión de la garantía a otros ámbitos pero fundamentado en una interpretación conjunta con el derecho de reserva previsto en la CN, art. 19 y como una necesidad de garantizar ámbitos ligados a la autonomía de la voluntad protegida en dicho artículo.., cf. Luis García, ob. Cit.

[122] Julio Maier destaca el carácter no absoluto de la protección comparándolo con lo previsto en relación a la incoercibilidad del imputado como medio de prueba y la supresión de tormentos. Destaca que aun cuando los derechos y garantías no son absolutos (CN,28), en el caso de la intimidad se trata de una de las garantías respecto de la cual el mismo texto constitucional concibe con limitaciones: "…Al menos como principio no se concibe que lícitamente una persona sea torturada o sea coaccionada para que declare contra ella misma, pero está permitido entrometerse en la vida privada de una persona, allanando su domicilio, secuestrando su correspondencia epistolar o sus papeles privados, o interceptando sus comunicaciones, siempre que se respete las condiciones y exigencias que para ello prevé la ley común…", *Derecho Procesal Penal*. Tomo I, pág. 681.

constitucional. Así la Convención Americana sobre Derechos Humanos lo prevé como una derivación de la protección a la honra y la dignidad humana en el artículo 11: "1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad. 2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación".

c) Es claro que la relación de las personas con los sistemas informáticos ha generado situaciones fácticas de potencial afectación a la intimidad antes impensada. Así, a modo de ejemplo, resulta evidente que el ingreso (con fines de registro y secuestro de datos) por parte del Estado al conocimiento de todo lo contenido en una computadora personal o en un teléfono inteligente de una persona sospechada de haber cometido un delito, podría llegar a exceder las posibilidades de injerencia en la intimidad que ese mismo acceso significa en un domicilio personal o la apertura de un maletín a los fines de su requisa y posterior secuestro de "papeles privados" útiles para la investigación. Por este motivo, pudiera parecer en algunos casos errado que la analogía entre ambas situaciones fácticas (registro en un domicilio/registro en una computadora) sea una vía que permita proteger adecuadamente la garantía constitucional.

El acceso al contenido de una computadora por parte del Estado permite un conocimiento de ámbitos de intimidad de las personas protegidos constitucionalmente mucho más comprensivo y profundo que el que permite el acceso y registro a un domicilio. A modo de ejemplo, el registro de una computadora o la memoria de un teléfono inteligente podría permitir el conocimiento no solamente de los documentos, fotos, videos, etc. que existen en el momento en que se realiza la medida, sino que puede alcanzar a la obtención de datos del pasado o incluso de terceras personas[123] que hubieran tenido

[123] A modo de ejemplo, si registramos el contenido de un teléfono inteligente que antes de pertenecer a la persona que es objeto de investigación, perteneció a un familiar o un amigo, puede ser que encontremos datos de comunicaciones, fotos, mensajes, etc. de esta tercer persona, incluso algunos de estos datos podrían constituir elementos de prueba de un delito diferente que cae en conocimiento del Estado.

contacto con el dispositivo en el pasado[124]. Asimismo, permite acceder a elementos que posibilitan trazar perfiles personales y conocer gustos tendencias etc. (acceso a documentos electrónicos existentes e, incluso los borrados por el usuario aunque hubiera transcurrido un tiempo considerable; correos electrónicos, incluso aquellos que la persona hubiera decidido eliminar; tendencias y gustos personales y datos sensibles como tendencias religiosas, políticas, orientación sexual; páginas *web* visitadas; fotos y videos; manejo de cuentas bancarias; personas con las que se comunicó; películas vistas; interacción con otras personas en redes sociales, viajes realizados y planeados, etc.).

II. Ello nos lleva a reflexionar sobre si ello implica un derecho novedoso[125], o en realidad lo novedoso es la *amplitud* de la injerencia. La capacidad de intromisión puede ser potencialmente tan expansiva que obliga a un examen más minucioso. La protección de la CN pareciera más clara aplicando correctamente la interpretación dinámica de los derechos que obliga la interpretación constitucional. Lo que no resulta tan claro es la manera de protegerla.

En definitiva, el derecho a la intimidad en todos sus aspectos (domicilio, comunicaciones, correspondencia, papeles privados, etc.) se trata de un derecho no absoluto, pues la CN admite que una ley pueda establecer en qué presupuestos, condiciones y requisitos es posible para el Estado ingresar dentro de ese ámbito protegido. En este sentido, lo rige el principio de legalidad (pues la CN, establece que es una ley la que habilita la intrusión), funciona a la inversa que el principio de reserva que rige en el derecho material. De este modo, en el derecho material todo lo que no se encuentra prohibido está permitido y la prohibición la establece una ley. Sin embargo, en materia de medidas de coerción, funciona a la inversa: el ámbito de intimidad se encuentra protegido de ataques del Estado, sólo una *ley* puede establecer cuándo es posible una intrusión, dentro de determinado marco, condiciones y requisitos.

---

[124] Un ejemplo sencillo ayuda a comprender las sustanciales diferencias entre el allanamiento de un espacio físico y el "allanamiento" de un espacio digital. Supongamos que un agente estatal se presenta en nuestro domicilio con una orden de allanamiento para buscar documentos vinculados a una causa de evasión tributaria. El agente estatal podrá registrar nuestro domicilio y sus hallazgos estarán limitados a los elementos físicos que existen en el momento en que realiza la búsqueda. Si por ejemplo, el día anterior yo traslade los documentos a otro lugar, el resultado de la medida será negativo (por más que busque y busque, solo encontrará lo que existe en el espacio físico en el momento en que ejecuta le medida). No sucede lo mismo en el ámbito digital, el registro de soportes digitales utilizando software especiales de investigación permite encontrar no solamente lo que el usuario tiene accesible en el presente sino también lo borrado o intentado de eliminar por el usuario, incluso podría encontrar lo que un usuario anterior hubiera hecho, por ejemplo en el caso de una computadora comprada de segunda mano, el investigador podrá encontrar documentos de un tercero que nada tiene que ver con la persona que es objeto de la investigación.

[125] En sentido contrario, cfr. Salt, su tesis doctoral.

Ahora bien, no resulta tan claro que por el mero hecho de que se acceda a determinados ámbitos protegidos por medios tecnológicos, informáticos, electrónicos, ello no se encuentre previsto. Si el medio tecnológico permite acceder a las comunicaciones, resulta irrelevante el medio en que se accede, lo que regula la ley son los requisitos jurídicos para a la comunicación privada y no el medio por el que se accede. De manera tal que es posible sostener —no sin discusión— que el legislador ha admitido esas intrusiones, la dificultad es cómo hacerla.

El problema se agrava pues el sistema no siempre percibe la intrusión masiva a la intimidad que significa el ingreso a un sistema informático. Literalmente, el acceso permite que el Estado acceda a todos los aspectos de una persona (física o ideal), a aspectos personales, a todas las comunicaciones (también correspondencia) que hayan quedado en el dispositivo, a imágenes y videos sobre su vida personal, datos personales sensibles, médicos, como económicos (secreto fiscal y bancarios); incluso el acceso a un sistema informático, puede acceder a información borrada y del pasado. Es más, de acuerdo a diferentes medios informáticos puede ser accedida la información en tiempo real y remoto.

Si bien en la vida cotidiana se podría tener la impresión que las nuevas tecnologías flexibilizan el derecho a la privacidad; en realidad, en el ámbito jurídico, y más aún en el examen de las facultades con las que cuenta el Estado para acceder a los ámbitos de intimidad*, el resguardo debe ser más estricto*: cuanto mayor peligro en la violación a la intimidad, mayor cuidado y estrictez debe tener el Estado en su manipulación[126]. De modo que no siempre el problema yace en la previsión constitucional o legal, sino en la manera de interpretarla.

Es por ello que acceder a un sistema informático resulta una medida de coerción probatoria, debe ser ordenada por un juez (CN, 116) y dentro de las exigencias formales establecidas por el legislador para acceder a determinados ámbitos de intimidad (CN, 18), que aporte una motivación suficiente que permita establecer el motivo por el cual es necesario ese grado de intrusión, criterios de proporcionalidad en la disposición de la medida, y el menor gravamen posible para lograr una eficacia de la medida sin violentar o restringir el derecho a la intimidad u otros más allá de lo necesario. Ahora bien, esta medida debe tener en cuenta —*para adquirir legitimidad*— el grado de intrusión en la intimidad para determinar cuáles son los requisitos que la medida debe abarcar, y tener cuenta la extensión y gravedad de dicha intrusión.

---

[126] Debe merecer un examen exhaustivo determinar si le asisten razón a la Corte Suprema Alemana que —como vimos en capítulos anteriores— se refiere a un nuevo derecho constitucional de *confidencialidad e integridad de información de sistema informáticos.*

De manera tal que la decisión de si se encuentra abarcada la medida por el legislador, establecer de qué modo es posible realizar una aplicación analógica, y en su caso, a qué medida se refiere, no resulta una tarea sencilla, y el sistema suele fallar en este aspecto poniendo en riesgo la validez de la medida. No parece posible sostener con seriedad jurídica que toda medida sobre un sistema informático se encuentra prohibida por no estar regulada, ello carece de rigor, pues el medio no es lo relevante, sino antes bien, el grado de compromiso en la restricción del derecho. Lo que va a determinar su legitimidad son las circunstancias del caso concreto (caso/capacidad de la medida) y el grado de intromisión que significa.

Ello obliga al operador judicial a realizar un examen laborioso de advertir posibles accesos qué ámbitos de intimidad, objeto de búsqueda, posibles hallazgos[127], períodos temporales, si va a ser necesario quebrar contraseñas[128], etc. tanto al momento de ordenar la medida como en la evaluación de su resultado. En este sentido, puede implicar cumplir con los requisitos de una orden de allanamiento, la intercepción de la correspondencia y la intervención de comunicaciones[129] (todas al mismo tiempo), no sólo en la orden sino también en su ejecución, incluso puede significar delimitar temporalmente la medida. Si la medida fuera realizada por un particular e implicara delito, si es admisible para el Estado, siempre debe ser ordenada judicialmente —se encuentre o no previsto normativamente—.

III. El sistema ha intentado solucionar el problema que plantean las nuevas tecnologías realizando una aplicación analógica de los medios de prueba tradicionales no siempre de manera correcta y en general de un modo

---

[127] Son muy habituales los hallazgos sorpresivos, en el examen de examen informático. Estos hallazgos pueden referirse a la comisión de otro delito (al que se le aplicarían las reglas de la *plain view*), o vulneraciones a la privacidad que no tienen vinculación con hecho ilícito alguno, por ejemplo, en casos en donde se buscan imágenes sobre tapas de libros (para verificar una infracción a la ley de protección de la propiedad intelectual) ordenada como pericia y fueron incorporadas al informe pericial, imágenes de la relación personales íntima que las imputadas mantenían entre si.

[128] La contraseña significa per se un ámbito indiscutido de intimidad que, por ende, debe tener orden judicial.

[129] Ahora bien, lo que debe considerarse es que justamente deben abarcarse todas estas opciones para que sean legítimas y no una sola. Por ejemplo el acceso a la correspondencia epistolar cuando con exigencias formales diferentes a la intervención de las comunicaciones (por ej., prohibición de fuerzas de acceso a fuerzas de seguridad, CPPN, 185, y similares ver CPPCABA, y otros) ,
La ley de delitos informáticos ha equiparado la correspondencia epistolar a la electrónica mediante el CP 153, Sin embargo, cuando las fuerzas de seguridad acceden en el marco de peritación técnica a los correos electrónicos (muchas veces existe una orden judicial que lo habilita) sin embargo, no es el juez quien verifica eta correspondencia que se aplican en definitiva la misma solución que para las intervenciones telefónicas (las fuerzas acceden al contenido de la comunicación).

deficiente, esto es, sin abarcar las posibilidades que plantea el caso concreto. Ello trae diversos inconvenientes que el sistema no suele advertir y que legitima en virtud de que la extensión de esta aplicación.

Por una parte, no siempre es posible realizar una aplicación analógica, pues como veremos más adelante, existen medidas probatorias informáticas que por sus características no es posible aplicarlas sin una previsión expresa del legislador. La otra cuestión se refiere al modo en que, si es admisible y permitida, debe realizarse una aplicación analógica. La elección de la medida no agota la discusión sobre los requisitos que la legitiman. Por más que llamemos pericia técnica (que sólo se plantea si es irreproducible y definitiva) a una intrusión a un correo electrónico, no lo exime de aplicar las reglas de la medida de coerción, por ejemplo, orden judicial[130], muchas veces, incluso para validar medidas dudosas se aplica analógicamente medidas de prueba menos estrictas en sus requisitos.

Es también común, cuando se accede a un sistema/disco, informático secuestrado, que se aplique analógicamente la medida de apertura de documentación, cuyo recaudo es que intervenga la defensa, brinda certeza y resguardo del derecho de defensa, pero no protege *per se* el derecho constitucional a la intimidad.

a) Dos casos nos permiten realizar un relevamiento del modo en que ello sucede en el sistema actual.

➢ *El caso BNP*[131]

En el marco de la investigación por defraudación en contra del INSSJP en el fuero federal, se allanaron[132] oficinas del BNP Paribas con el objeto de verificar si el imputado R poseía dinero en el exterior. En el allanamiento se secuestraron diversos documentos, y computadoras, agendas electrónicas, unidades *zip*, discos compactos y duros violentando reglas básicas aceptadas universalmente

---

[130] Ello es muy común, por ejemplo, en la provincia de Buenos Aires, en donde los fiscales ordenan a las fuerzas de seguridad, o a veces, con la aparatología técnica que lo permiten lo hacen ellos mismos, el acceso a un teléfono inteligente bajando toda la información que allí encuentren, casi sin dudas, correos, comunicaciones de chat, imágenes, videos, incluso información bancaria. Ello se hace al amparo de la disposición de una pericia sin orden judicial. En otras ocasiones, se notifica por nota por considerar que determinadas pericias son reproducibles, por ejemplo, en el caso HSBC.

[131]Causa nro. 19888/2009, "BNP Paribas y otros s/ Lavado de Dinero", tramite ante el Juzgado de Instrucción 35, secretaria 120. Sala I de la Cámara Criminal y Correccional.

[132] Ello llevó a dos allanamientos de esas oficinas, luego de la declaración testimonial de ejecutivos de dichas oficinas —luego imputados—.

sobre conservación de evidencia digital (no fueron conservados ni lacrados los CPU).

Dicho secuestro excedió la orden emitida por el juez, pues no se trató de un caso de descubrimiento accidental de pruebas en relación a un hecho distinto al investigado no tenía vinculación con el objeto procesal no se realizó la consulta pertinente con el juez, conforme lo prevé expresamente el CPPN, 224, último párrafo[133], tampoco se verificó fuente independiente de investigación.

Ello provocó que se sucedieran otras irregularidades procesales (que aquí no importan), pero donde BNP comenzó a ser investigado, y se lo hizo a través de una pericia informática que tenía por objeto, "…determinar toda circunstancia que pueda resultar de interés a la investigación en punto a información sobre personas y sociedades objeto de pesquisa, como así también información que permita conocer la actividad propia de la oficina allanada…", así se bajó la información de las computadoras y soportes magnéticos por la Dirección de Policía Científica de Gendarmería, impresa y luego analizada por la Unidad de Delitos Económicos. Allí se llegó a información de un listado de clientes del banco que utilizaban dicha oficina. En estos elementos informáticos se podían identificar clientes, los años de las transferencias a través de *correos electrónicos*, entre otras cuestiones, ello fue copiado en 3 DVDs. Sobre la base de esta información y principalmente los listados de clientes y sus datos se derivó una investigación por lavado de dinero en el fuero ordinario en contra de ejecutivos del BNP[134], llevada adelante por el ministerio público, como autor desconocido (CPPN, 196 bis). El fiscal solicitó colaboración en la investigación no sólo a la PGN en su conjunto con diversos funcionarios, sino a distintos organismos del Estado: UTN; UIF; UFITCO; PFA en cuanto al análisis patrimonial; el BCRA, ANSES, AFIP, el Registro Nacional de las Personas, el GCBA, sin control del juez, ni de las defensas. Incluso más, el fiscal ordenó las medidas probatorias estableciendo que "…la información en cuestión se encuentra exceptuada del secreto fiscal, bancario y bursátil…" A pesar de que el ministerio público no tiene facultades para solicitar datos o información, o cualquier tipo de medidas que impliquen la intrusión en la intimidad (CN, 18) o de los datos personales, incluso requirió a la empresa Telecom las llamados entrantes y salientes de los números telefónicos de BNP Paribas, cuando el CPPN prevé expresamente que esta medida de prueba sólo puede ser solicitada

---

[133] "Si en estricto cumplimiento de la orden de allanamiento, se encontrare objetos que evidencien la comisión de un delito distinto al que motivó la orden, se procederá a su secuestro y se le comunicará al juez o fiscal interviniente".

[134] Luego ello derivó en investigaciones por delitos tributarios en contra de los clientes del banco.

por un juez y ya se ha establecido en nuestra jurisprudencia de la CSJN[135] que resulta nula como medio de prueba los datos de tráfico de comunicaciones solicitados directamente por los fiscales a las compañías sin la intervención judicial (CPPN, 236).El SINTYS (Sistema de Identificación Nacional Tributaria y Social) le advirtió al Fiscal sobre que se requeriría una orden judicial (y no del ministerio público) para solicitar datos personales, de conformidad con la ley 25.326 de Protección de Datos Personales, no hubo, sin embargo, orden judicial.

También en el caso existieron irregularidades en la manipulación y recolección de información de los elementos probatorios de cargo. Prácticamente todos los parámetros de actuación aceptados por la informática forense[136] fueron violentados tanto la adquisición de los soportes informáticos, su posterior aseguramiento y traslado a las distintas autoridades, su registro y análisis técnico y su documentación, violentaron de manera flagrante las buenas prácticas sobre la materia, que una vez contaminada es de muy difícil recuperación. En este caso concreto, al no haberse tomado recaudo alguno en el resguardo del elemento de prueba asegurando los originales y manteniendo una adecuada cadena de custodia su recuperación era imposible. Se tornó, entonces, en un acto irreproducible que impedía cualquier tipo de intento de reproducción

---

135 Así fue entendido también por la jurisprudencia, incluso por la Corte Suprema de Justicia de la Nación al analizar la constitucionalidad de la Ley 25.873 de Retención de datos de Tráfico (cf. CSJN h.270. XLIT, Halabi Ernesto c/PEN – Ley 25.873 s/amparo: "Acerca de estas situaciones este Tribunal ha subrayado que solo la ley puede justificar la intromisión en la vida privada de una persona, siempre que medie un interés superior en resguardo de la libertad de los otros, la defensa de la sociedad, las buenas costumbres o la persecución del crimen…" "…Es en este marco constitucional que debe comprenderse, en el orden del proceso penal federal, la utilización del registro de comunicaciones telefónicas a los fines de la investigación penal que requiere ser emitida por un juez competente mediante auto fundado (conf. Art. 236, segunda parte del Código Procesal Penal de la Nación, según el texto establecido por la Ley 25.760), de manera que el común de los habitantes está sometido a restricciones en esta esfera semejantes a las que existen respecto a la intervención sobre el contenido de las comunicaciones escritas o telefónicas".

136 Los nuevos criterios normativos y jurisprudenciales para su utilización válida en el proceso penal y nuevas formas de aplicar los principios que regulan los medios de prueba tradicionales en el proceso penal, pensados y diseñados para la evidencia física, a los desafíos que plantea la evidencia digital, la protección de la garantía de la intimidad y la inviolabilidad de la correspondencia y los papeles privados frente a técnicas que permiten una fuerte intromisión en la intimidad nunca antes imaginada por el legislador. La necesidad de una nueva especialidad, la informática forense, que ha desarrollado criterios para la obtención de evidencia que se traducen en "*buenas prácticas*" del arte hoy aceptados a nivel doctrinario y jurisprudencial en el derecho comparado y también en el medio local (aunque aún sin el mismo desarrollo) y que permiten a los tribunales cotejar su cumplimiento a los fines de analizar la validez de una prueba de estas características, que tiene como finalidad precisamente asegurar que la adquisición y preservación de prueba contenida en soportes digitales se lleve a cabo de manera de asegurar su validez al ser presentado en los tribunales (cf. El Manual elaborado por el profesor alemán Marco Gercke para la International TelecommunicationUnion, *UNDERSTANDING CYBERCRIME: A GUIDE FOR DEVELOPING COUNTRIES*, 2011).

válida[137]. Los 17 CPUs secuestrados no fueron adecuadamente resguardados al momento del secuestro ni en sus posteriores traslados, (si bien otros objetos secuestrados —documentación y efectos— fueron introducidos en sobres, sellados, fajados y firmados por los intervinientes e introducidos en una caja incluso una *notebook* fue precintada), no fueron preservados en forma alguna, ni precintados, ni introducidos en sobres sellados (en sede judicial, por ningunos de los dos juzgados), lo que resultaba la volatilidad de la prueba, su fácil alteración, etc. Asimismo, el hecho de que no se hubieran realizado copias seguras de los originales con *códigos hash* (tal como requieren las buenas prácticas sobre la materia) que aseguren la posibilidad de repetir la medida de análisis, tornaron a esta prueba irreproducible. Se permitió una búsqueda arbitraria en los soportes informáticos violentando la necesidad de que el registro y secuestro de evidencia digitales en un soporte quede acotado por la orden judicial específica y fundamentada conforme a las necesidades basadas en el objeto procesal de la causa, lo que constituyó una peligrosa práctica que permite *pesca de información indiscriminada* en soportes informáticos de enorme potencial de afectación a la intimidad de las personas, soportes que por sus características técnicas concentran gran cantidad de información que se almacena durante años y que puede involucrar a numerosas personas e instituciones indeterminadas que nada tienen que ver con el objeto procesal de la causa y con los fines para los que fue habilitado un allanamiento.

Tampoco hubo una apertura de los efectos secuestrados con la participación de las defensas, otra aplicación de la aplicación analógica. Peor aún, el perito técnico (que intervino inicialmente) fue quien estableció los criterios de búsqueda, sin *orden judicial alguna desbloqueó las contraseñas,* manifestación más evidente en el campo de los soportes informáticos de la voluntad de sus titulares de mantener un ámbito de intimidad. Se volcó la información a tres DVDs que no fueron resguardados en forma alguna, recién luego de ello se ordenaron copias forenses que incluyeron el número *hash* de cada archivo generado para asegurar la indubitabilidad de la imagen y el fiscal que intervino posteriormente ordenó descifrar las claves de los archivos para hacer efectiva la visualización. Recién en dicho momento se utilizó el método —único correcto— con el objeto de brindar seguridad en la clonación, y asegurar que los datos provenientes de estos elementos no hayan sido alterados.

Además, la PGN recuperó archivos NSF, en donde se encontraron archivos categorizados “casilla de mail”. Esto que el Ministerio Público, sin autorización

---

137 Sobre las características especiales que requiere la cadena de custodia en lo que se refiere a datos y documentos contenidos en soportes digitales y la necesidad de medidas distintas a las adoptadas en relación a los documentos en papel; cf. Giuliano Giova, profesor de la Escola Politécnica, Universidade de São Paulo, São Paulo, Brasil*, Improving Chain of Custody in Forensic Investigation of Electronic Digital Systems,* “International Journal of Computer Science and Network Security”, VOL. 11 No. 1, January 2011.

judicial alguna, destrabó claves y accedió a archivos informáticos conteniendo información confidencial y correos electrónicos. El Ministerio Público dejó de lado la profusa jurisprudencia nacional y federal que asimila el correo electrónico a la correspondencia epistolar exigiendo para su incorporación como prueba a un proceso penal las mismas garantías. Ya desde la causa Lanata, Jorge, la Cámara Nacional en lo Criminal y Correccional sostuvo esta postura –resolución de la Sala VI del 4/3/1999-, postura ratificada en numerosos precedentes tales como Causa Abreu 35.369 resuelto por la Sala VII el 9 de octubre del año 2008, más recientemente causa RyR y otros resuelto por la Sala VI el 14 de junio del año 2010. En este último fallo se afirma de manera más que gráfica: "…las Cortes de los países Europeos y Sudamericanos en su jurisprudencia y doctrina casi unánimemente avalan esta afirmación, que parte de tres premisas fundamentales: a) Que costó mucha sangre y cambio de ideología en el mundo comprender que no hay fin que justifique los medios; b) que el e mail, además de su traducción (correo) es la comunicación escrita en computadora, enviada o recibida vía internet; c) documentos privados son los que están en el archivo de una computadora con una clave personal. De ello se desprende que la orden judicial fundada sería indispensable para la intromisión en ese marco de intimidad…". Ni tampoco la ley de delitos informáticos que modificó el CP, 153, incorporando la correspondencia electrónica.

Todo ello fue planteado por las defensas en un incidente de nulidad de la prueba, con fecha 11 de noviembre de 2011, a la cual no se le hizo lugar. Se sostuvo sobre el allanamiento, su resultado positivo y la investigación posterior: "…que desembocó en el secuestro de una gran cantidad de documentación y material informático… pero más importante aún permitió descubrir la realización en ese lugar de una serie de maniobras bancarias que se presumieron sospechosas, y que involucraban tanto a empleados de dicha entidad como a una cantidad de clientes que allí figuraban registrados. Esto a las claras, indica sin hesitación alguna que la investigación primaria, y que involucraba únicamente a R como posible imputado, permitió revelar los hechos antes descriptos y la posterior extracción de testimonios a efectos de que la Justicia en lo Criminal de Instrucción tome intervención respecto de la posible comisión del delito de lavado de activos; lo que indica, a contrario a lo aseverado por el incidentista, que la investigación que aquí es llevada a cabo encuentra un fundamento y un correlato lógico a partir de todas las medidas de prueba que fueron llevando a cabo en el marco de aquella pesquisa, en base a un plexo probatorio que insisto, resulta indiscutible en relación a la presumible extensión ilegítima de la investigación llevado a cabo en el fuero de excepción, entiendo que mucho no queda por decir al respecto, si se tiene en cuenta fundamental que aquel allanamiento tan cuestionado, no sólo habría permitido al magistrado interviniente advertir el presumible desvío de fondos en el que habría incurrido R… , sino también se habrían acreditado la existencia de

cuentas en el exterior pertenecientes al nombrado;... que luego desembocaron en la extracción de testimonios que dieron origen al proceso que aquí tramita....". Sobre la conservación del material: "...en relación a la forma en la cual habrían sido lacradas y mantenidas las CPU y soportes informáticos que fueran oportunamente incautados en la sede de la oficina registrada, entiendo que esa cuestión no sólo no encuentra sustento para ser atacada por medio de esta vía, sino que tampoco existe en el legajo indicio alguno que permita presumir fundadamente que todos los informes que obran en el proceso y respecto de tal documentación, no encuentre correlato con los datos que tales pruebas contienen almacenados...". Sobre el carácter de reproducible de la medida: "...aclarando además que, en caso de presumirse que tales informes no resultan ser veraces, las partes poseen la potestad de solicitar la realización de un nuevo informe en los mismos términos, por cuanto nos hallamos frente a una medida de prueba perfectamente reproducible....sin requerirse en aquella oportunidad, entiendo, la anuncia de personal judicial o de alguna parte a los efectos de practicar un contralar a ese respecto, medida que, repito, puede ser perfectamente reproducible". Sostuvo que los informes periciales iniciales cumplían con las reglas del arte: "... respecto del informe... toda vez que, lejos de haber violado las recomendaciones básicas de las reglas del arte para el análisis de evidencia digital a las que alude, se presume fundadamente que aquellos informes fueron llevados a cabo en el marco de legitimidad habitual en el cual se desenvuelven las fuerzas de seguridad al momento de tomar intervención en un proceso judicial..."

La resolución, por supuesto, no hizo más que dar excusas (y no argumentos) para validar un procedimiento probatorio inválido por diferentes motivos. Excusas que se extienden en el sistema. El hecho de que el allanamiento y las medidas posteriores hubieran dado resultado positivo en modo alguno validó, ni implicó en modo alguno legitimar la medida, ni suprimir sus irregularidades ni acreditar cadena de custodia. Del mismo modo, esta postura obliga a la defensa a indicar los datos errados para acreditar la carencia de certeza, lo que resulta ilegitimo porque ello obliga a prevaricar a la parte. La certeza debe ser una característica inobjetable del elemento probatorio, no la obligación de la parte a verificar su carencia. A pesar de ello la Cámara de Apelaciones no hizo al recurso de apelación, con fecha 9 de abril de 2012, y más tarde los imputados fueron procesados sobre la base de esta prueba.

Esto sucedió en el año 2011/2012, a pesar del desarrollo de estas modalidades y el avance de las conocimiento y formación que ello que provocó en los operadores del sistema, un nuevo caso, muy similar, en modo alguno significó un avance en el examen de la evidencia digital, por lo contrario, el sistema nuevamente volvió a buscar excusas para no imponer límites a la vulneración o

restricción de derechos constitucionales y respecto de la certeza de los elementos probatorios.

➢ *El caso HSBC*[138]

En el caso del Banco HSBC, conforme fue de público conocimiento se inició una investigación penal a contribuyentes en Argentina por evasión tributaria en virtud de información que fue aportada al titular a la AFIP por parte de la administración francesa en formato de evidencia digital, que tuvo como origen reconocido por las propias autoridades, el apoderamiento y tratamiento de datos informáticos de clientes del banco HSBC SUIZA por el ex empleado Hervé Falciani, quien copió información de clientes del banco, en todo el mundo —entre ellos, Argentina— en diferentes bases de datos que se encontraban compartimentadas dentro del propio banco, que él compuso en fichas de clientes con montos de las cuentas, correos electrónicos, etc. Esta información tuvo origen en la comisión de un delito por parte de un empleado infiel del banco HSBC en Suiza, que originó una persecución penal allí por espionaje económico, sustracción de información violación de secreto comercial y violación de secreto bancario, y que posteriormente le fue secuestrada en un allanamiento llevado adelante por autoridades francesas en Niza.

Esta información obtenida ilegalmente por Falciani, y luego secuestrada en Francia en una investigación que le dirigía en su contra, fue examinada excediéndose en el objeto procesal que justificaba la medida original de detención y registro y secuestro, desagregando la información por clientes de cada país y entregada en versión digital a las autoridades fiscales de cada uno para la persecución de las posibles infracciones tributarias, sin resguardo alguno de cadena de custodia. Entre ellos, Argentina.

Esta información luego fue copiada en otro CD que fue motivo de la denuncia penal ante el fuero penal económico, que imprimió las fichas de estos clientes. Estas fichas son el elemento probatorio de cargo principal y casi único de la investigación de cada uno de los contribuyentes. La irregularidad de la obtención de la información[139]; se intentó legitimar por la corte de casación francesa sobre la base de afirmar que fue producto de un allanamiento regular, que España también validó esta información, y por último fue considerara válida por la AFIP por su utilidad. En realidad, ello no la validaba en modo alguno pues se trata del mismo cauce de información viciado.

---

[138] Causa nro. 1652/2014, "HSBC Bank Argentina SA y otros s/ Ley 24.769", en trámite ante el Juzgado Penal Económico 11, Fiscalía Penal Económico 9, Sala B Cámara Penal Económico.

[139]Suministrada por el gobierno francés en virtud del convenio para evitar doble imposición

Las defensas plantearon la nulidad de la prueba de cargo. El planteo dio cuenta de las irregularidades en diferentes aspectos (algunos que no hacen en nada a este informe, por ejemplo, referidos a la cooperación internacional). Básicamente lo que plantearon es que el elemento probatorio principal de cargo se encontraba viciado de nulidad en virtud de su origen ilícito, la conculcación de garantías constitucionales y que dicha nulidad afectó a todos los actos procesales que de allí derivan. Citaron la doctrina de la regla de exclusión y su derivación la doctrina del fruto del árbol envenenado especialmente los antecedentes jurisprudenciales de la CSJN que le da sustento. Entre otros sostuvieron que se afectó el derecho a intimidad (secreto bancario y fiscal), la protección de papeles privados, afectación de datos personales (CN, 18) y explicaron que se encontraban protegidos por La Ley de Entidades Financieras, nº 21.526, art. 39 y la Ley de Protección de Datos Personales, nº 25.326 en virtud de los datos sensibles, art. 7º; y la imposibilidad de la administración de beneficiarse con comportamientos que impliquen violación de un derecho constitucional, Ley 19.549, art. 9, que se deriva no sólo del derecho a intimidad y los papeles privados sino que tiene una protección constitucional específica en CN, 43, tercer párrafo, que protege los datos sensibles recolectados, incluso por entidades privadas y que este resguardo, plantearon, es expreso también a través de la tipificación de la conducta del acceso ilegítimo a datos personales, CP, 153 bis (incorporado por la Ley de Delitos Informáticos, nº 26.388).

Otra violación constitucional en la documentación aportada por la AFIP y es el de la correspondencia CN, 18, pues las planillas impresas reflejaban comunicaciones vía electrónica aparentemente entre agentes del banco y los clientes, en virtud del acceso y su incorporación al proceso es lo que configura una intromisión en la correspondencia que no tuvo ninguna autorización judicial —pues ha sido objeto de un ilícito—[140].

Otro aspecto de la ilegitimidad planteado se refirió a la que surgía en el examen de la información secuestrada en la computadora de Falciani. Es que una vez que la información fue hurtada por Falciani de los registros del banco, y luego de la persecución penal contra el ex empleado, se produce el allanamiento en Niza donde se secuestra la información en su computadora. El objeto de dicho allanamiento era recoger elementos contra el ex empleado en virtud de los delitos imputados, y no recolectar elementos en contra de los supuestos clientes del banco. Una vez registrada, copiada y obtenida la información sobre el hurto

[140]En Argentina no sólo la CSJN (por ejemplo, en el caso Jutton del 20/11/2012) ha asimilado la protección de la correspondencia epistolar a la electrónica, sino que además ello ha sido equiparado por la Ley de Delitos Informáticos, nº 26.388, al modificar el CP, 153. No existe duda que en Argentina la correspondencia electrónica tiene la misma protección que la epistolar (mediante la tipificación de la conducta y constitucionalmente, CN, 18) de modo que no es posible para el Estado valerse de su violación para obtener datos de caso como sucedió en esta secuencia ilícita.

de los datos se agotó la posibilidad de inspección sobre dicho material. De lo contrario, como sucedió en el caso, se estaba realizando un exceso en la inspección que no se encontraba alcanzado por el objeto procesal de la causa llevada adelante en contra de Falciani. Todo el examen y manipulación de la información obtenida para iniciar investigaciones en contra de los clientes del banco violentaban la doctrina de la *plain view*, recogida por nuestra jurisprudencia y en el CPPN, 224 último párrafo. Lo que en términos sencillos implica la *plain view* es que, si la ejecutar una orden de allanamiento la fuerza de seguridad se topa de manera accidental e inadvertida con elementos demostrativos de otro delito diferente del que motivó el allanamiento, se encuentra autorizado a secuestrarlo. Sin embargo, para que rija dicha autorización debe realizarse el examen del domicilio en estricto cumplimiento de la orden y el hallazgo debe ser accidental[141]. Esta misma regla se aplica al examen de dispositivos informáticos, por ejemplo, si el revisar una computadora buscando elementos constitutivos de un fraude se encuentra material de pornografía infantil.

De manera tal que no era posible, con la excusa de secuestrar elementos en contra de Falciani, buscar datos en contra de supuestos clientes del banco, como sucedió en este caso, pues ello no se encuentra autorizado por nuestros estándares probatorios de examen del domicilio y de dispositivos informáticos. Ello violenta la regla del *plain view* en tanto no se trata de un hallazgo accidental sino de la utilización —como excusa— de un allanamiento por violación al secreto bancario para acceder a información de los presuntos clientes perjudicados. Ilegitimidad que también alcanzaba al examen y procesamiento de los datos informáticos hallados, lo que la tornaba ilegítima.

También fue planteada la falta de certeza de los elementos probatorios, esto es, la violación a la cadena de custodia, se sostuvo que no era posible establecer una adecuada cadena de custodia del material no sólo desde que ha ingresado en Argentina por medios que violentaron la certeza que implica las reglas básicas de cooperación internacional, sino que no era posible establecerla con anterioridad al allanamiento en Niza, ni después cuando el material fue manipulado para verificar datos de supuestos clientes y dividirlos por países para iniciar persecuciones penales por evasión tributaria. Más aún, cuando la información secuestrada a Falciani había sido una construcción realizada por él la cual requirió entrecruzamientos de datos. Desde su sustracción hasta que fuera obtenida por las autoridades argentinas evidentemente no se había cumplido con los estándares mínimos de preservación de la evidencia que permite sostener que aquella resultaba información obtenida, efectivamente, del banco. Lo que puso en evidencia que la ilegalidad inicial en modo alguno pudo

[141]Cfr. Carrió, p. 394.

ser purgada por el allanamiento en Francia, pues ello no le brindaba certeza a la información hurtada al banco; ni con posterioridad, pues dichos datos fueron manipulados para las persecuciones en cada Estado a nivel tributario, que ni siquiera siguió los canales diplomáticos establecidos para su incorporación, lo que en el caso se agrava pues los datos se encuentran en soporte informático. Ello también fue recogido por nuestra jurisprudencia en la causa Jaime, Sala I, CNACCF, causa 46.744 Fiscal s/apelación declaración de nulidad de informe pericial, Registro n° 458 del 24/5/2012, donde se nulificó el informe pericial sobre prueba informática pues se había violentado la cadena de custodia.

La juez no hizo lugar a la nulidad, con fecha 7 de marzo de 2017. Sostuvo como meras excusas para no proteger los derechos vulnerados: "Los eventuales delitos que pudiera haber cometido el poseedor de tales documentos -Hervé FALCIANI-, tal como se indica en los diferentes planteos, no constituye una circunstancia que invalide "per se" la obtención de los documentos secuestrados regularmente por las autoridades estatales. … 15°) Que, la regla que invocan los distinguidos defensores en las múltiples presentaciones que dieron lugar a esta incidencia sólo se aplica para restringir las facultades persecutorias de los órganos públicos. A su vez no se ha indicado alguna razón por la que corresponda hacer excepción a ese principio general y tampoco se ha demostrado que la prueba incorporada al proceso vulnere de manera directa y concreta algún derecho fundamental de los imputados. En efecto, la regla fue por primera vez aplicada por la Corte Suprema Federal de los Estados Unidos y ese mismo tribunal ha establecido que no están cubiertas por la regla de exclusión las pruebas obtenidas por particulares y luego utilizadas en un proceso penal…16°) Que, además, del examen de los archivos entregados por las autoridades francesas a la Administración Federal de Ingresos Públicos surge que se refieren a datos relativos a la tenencia de activos depositados en cuentas bancarias, a sus beneficiarios y titulares, el tipo de tenencias, movimientos y saldo al cierre del ejercicio, es decir, información que no integra el ámbito de reserva absoluto de los ciudadanos (artículo 19 de la CN). El secreto bancario no es oponible a la autoridad fiscal de nuestro país, más aún las tenencias de activos depositadas en el circuito bancario local, según la legislación vigente … 17°) Que, por lo demás, debe destacarse que los documentos en cuestión no presentan un contenido confesorio de parte de los aquí imputados obtenido forzadamente que eventualmente permita asimilarlos a la prueba obtenida mediante tormentos tal como se equipara en algunas de las presentaciones en análisis. 18°)… no se verifica alguna violación a las garantías constitucionales de la defensa en juicio e inviolabilidad de los papeles privados, ni los derechos a la intimidad y privacidad de los imputados (artículos 18 y 19 de la Constitución Nacional; artículo 11, inciso 2°, de la Convención Americana sobre Derechos Humanos; y artículo 17, inciso 1°, del Pacto Internacional de Derechos Civiles y Políticos). 19°) Que, se advierte la utilización de supuestas comunicaciones vía

electrónica aparentemente entre agentes del banco y los clientes y que ello implica una intromisión en la correspondencia efectuada sin orden judicial y, como tal, en violación a la protección constitucional establecida en el artículo 18 CN… operaciones que habrían sido efectuadas por personas supuestamente autorizadas para operar en cuentas bancarias. No obra en las fichas en cuestión, ni en las demás constancias del legajo, alguna comunicación interpersonal, que tampoco fue individualizada en la presentación efectuada por la defensa, cuyo resguardo garantiza el artículo 18 de la Constitución Nacional en cuanto a que la protección de datos bancarios no se deriva solo del derecho a la intimidad y los papeles privados sino que tiene una protección constitucional específica en el artículo 43, tercer párrafo, de la CN, cabe aclarar que en dicha disposición de la Constitución Nacional se ha consagrado el derecho de toda persona a interponer una acción expedita y rápida -habeas data- para tomar conocimiento de los datos a ella referidos y de su finalidad, contenidos en registros o bancos de datos públicos y, en caso de falsedad o discriminación, para exigir su supresión, rectificación, actualización y confidencialidad (Fallos: 322:259). No hay duda de que el objeto tutelado por el habeas data no es el dato en sí mismo sino en la medida que afecte la intimidad o privacidad…de la persona y en particular, quedan fuera de la protección del habeas data los datos de interés público, tales como aquéllos que se refieran a la actividad económica, empresarial, etc. 23º) Que, en otro orden de ideas, las objeciones planteadas con relación a la presunta violación de la cadena de custodia y la posible contaminación de la documentación aportada por la República Francesa no resultan cuestiones normativamente vinculadas a la validez de esos documentos sino que, por el contrario, guardan relación con el valor probatorio que jurisdiccionalmente pueda asignárseles. Por ello, la eventual verificación de las inobservancias alegadas por las defensas no comporta per se una causal de nulidad, sino que podrían eventualmente incidir en la fuerza probatoria con la que se valoren esos elementos. En otras palabras, se trata de una cuestión de grado en su función demostrativa y no de su naturaleza como acto jurídico válido."

Con posterioridad a esta resolución, se corroboró que de hecho el CD agregado con la denuncia había obtenido sin observar las reglas forenses (sin código *hash*) que acreditan que sea una copia idéntica a la enviada por las autoridades francesas, que tampoco es posible afirmar que no ha sido alterado.

El recurso de apelación por la resolución del incidente de nulidad fue rechazado el 26/12/2017 por la Sala B de la CNPE con argumentos similares. Mientras se tramitaba el recurso, algunos imputados fueran procesados sobre la base de esta prueba ilegal. Resulta evidente que el sistema validó la evidencia digital sin proteger derechos constitucionales, ni siquiera advirtieron su violación y afectando la cadena de custodia.

➢ *Cuestiones comunes*

Los casos aquí planteados por sus características ponen en evidencia lo que aquí se refleja respecto de la problemática jurídica de base, la incapacidad del sistema para brindar una respuesta adecuada que violenta el derecho a la intimidad:

- Ninguno de estos casos se trata de delitos *informáticos* ni siquiera cometidos a través de medios informáticos, sin embargo, el elemento probatorio de cargo fundamental y original es informático.

- Se trata de casos judiciales con probablemente la mejor defensa técnica del país (se trataba de diversos imputados con defensores técnicos juristas expertos). Ello indica que los problemas jurídicos fueron advertidos correctamente y tratados con rigurosidad ante las autoridades.

- Si bien se trata de hechos de mediana gravedad (lavado de dinero[142] y evasión tributaria, delitos de cuello blanco) tampoco se trataba de supuesto de pornografía infantil (muy común en medios informáticos), ni siquiera los imputados se encontraban detenidos durante el proceso. Esto es, ni siquiera se trataba de casos que el sistema intenta validar (ilegítimamente) a cualquier costo.

- Entre uno y otro pasaron 6 años (2011 y 2017) en donde la evolución de los medios tecnológicos y se supone de la evolución de estándares jurídicos, debería haber tenido alguna influencia. Ello no sucedió.

A pesar de estas características, el resultado fue el mismo, sin importar el tiempo transcurrido entre ambos, el sistema no advirtió de manera correcta el problema jurídico por detrás, el compromiso de determinado ámbitos de intimidad que fueron desprotegidos, por último, la carencia de certeza de elementos probatorios recogidos (de manera ilegítima) y a través de la *analogía* de que se trataba de una pericia, por ende, reproducible y en algunos casos ordenados por un fiscal o accesible a un particular producto de un hecho delictual, o recogidos violentando la regla del *plain view*. Adviértase que el sistema suele confundir la vigencia del derecho constitucional con la certeza del elemento probatorio, que se trata cuestiones diferentes. Es que la característica de certero que debe tener el elemento probatorio no se vincula con el derecho constitucional que puede, o no, estar comprometido, y en ambos casos el elemento puede resultan inválido (por una u otra vía o por ambas). De hecho,

[142] Lavado de dinero proveniente de evasión tributaria, y no de narcotráfico, terrorismo, etc.

ello puede estar regulado normativamente, o no, lo que no resulta desacertado pues cada elemento va a requerir diferentes cuidados técnicos para su conservación y resultar inobjetables, lo que en algunos sistemas se denomina *cadena de custodia*. Ello es particularmente importante en la evidencia digital por su volatibilidad.

Estos problemas son propios de casos con alguna complejidad como los aquí relatados, pero también en casos de los más sencillos del sistema penal. Cualquier tipo de hecho, los denominados informáticos, los de cuello blanco, y cualquier caso tradicional, por más simple que sea. Ello es lo que convierte al problema es *transversal*. No resulta dificultoso imaginar el examen de un teléfono inteligente (smartphone) ello permite acceder a aspectos tan privados del particular, aspectos que incluso pueden ser más íntimos que el domicilio. Allí se puede acceder a todas sus comunicaciones, redes sociales, al menos datos de tráficos en comunicaciones telefónicas, mensajes de texto o de mensajería, correos electrónicos, imágenes y videos, documentos, etc. Ello implica que el acceso a este dispositivo implica acceder a todos los aspectos de la intimidad de un individuo en una sola medida. Ello sucede también con la víctima, quien, por ejemplo, pretende acreditar que ha sido víctima de un delito, decide no denuncia al enterarse que ello puede significar que el Estado acceda a su dispositivo móvil. Consideremos que muchas veces un individuo comparte su domicilio, incluso comparte su habitación y su cuarto baño, incluso su cama, sin embargo, no comparte su teléfono celular, incluso más, puede contar con contraseñas que no conoce su familia, ni sus parejas, ni sus amigos. Esta situación tan cotidiana en el mundo moderno da cuenta de expectativas de intimidad tan elevadas que resulta ilegitimo que el Estado acceda a través de una medida simple de pericia técnica.

b) El sistema trata la problemática jurídica de la *evidencia digital*, unificando las circunstancias, simplificando las soluciones, lo que constituye un error. El sistema recurre en muchos supuestos a la aplicación analógica de la pericia técnica y dicha equiparación es lo que provoca la mayor cantidad de inconvenientes en la interpretación jurídica, la invocación de normas y el análisis posterior. Ello generalmente sucede pues se recurre a expertos informáticos, lo que no determina que la medida sea en concreto pericial propiamente dicha.

La pericia es el *medio probatorio* por el cual se intenta obtener, para el proceso, un dictamen fundado en especiales conocimientos científicos (v.gr., individualización genética -ADN-), técnicos (v.gr., identificación de matrículas identificatorias de armas, vehículos, etc.) o artísticos (v.gr., determinación de autenticidad de cuadros), útil para el descubrimiento o la valoración de un elemento de prueba. No se trata, en consecuencia, de un medio para auxiliar al

funcionario judicial, supliendo su deficiente formación sobre el tema a peritar, pues no se podrá evitar su realización aun cuando aquel tenga los conocimientos especializados necesarios. Variante específica de la pericia es la llamada *prueba científica*, que se caracteriza por nutrirse de comprobados avances de la ciencia. Se impone la intervención en el proceso de una persona que sepa lo que el órgano judicial no sabe: es el perito el sujeto al cual el magistrado debe ineludiblemente recurrir cuando se ha verificado que para *descubrir* o *valorar* un elemento de prueba son necesarios determinados conocimientos, artísticos, científicos o técnicos (art. 253, CPPN; art.231, CPP Córdoba), es decir, conocimientos propios de una *cultura profesional especializada*.

Si bien la ley establece que la autoridad judicial "*podrá ordenar pericias"*, esto no quiere decir que podrá abstenerse de hacerlo cuando "para conocer o apreciar algún hecho o circunstancia pertinente a la causa sean necesarios o convenientes conocimientos especiales en alguna ciencia, arte o técnica" (art 253, CPPN; art. 231, CPP Córdoba), pues en tal caso, o bien renunciara conscientemente a descubrir o valorar correctamente una prueba (lo cual no se concibe frente al principio de verdad real), o bien pretenderá obtenerlo con sus personales *conocimientos especializados*, lo cual no sería legítimo, pues afectaría el derecho de defensa de las partes y la *sociabilidad del convencimiento judicial.* Por tanto no se requerirá la intervención del perito: para la realización de *meras comprobaciones materiales*, que pueden ser llevadas a cabo por cualquier persona (como, por ejemplo, verificar si las llaves secuestradas abren la puerta del lugar del hecho); cuando dentro de la cultura normal, o cultura general, se puede hallar la regla o el criterio para resolver la cuestión; es decir, cuando puedan solucionársela mediante los *conocimientos básicos* de cualquier hombre culto (como, por ejemplo, mediante la aplicación de la ley de gravedad); también se podrá evitar llevarla a cabo, excepcionalmente, en algunos supuestos de *prueba trasladada*, como ocurre cuando la cuestión hubiese sido objeto de una pericia en otro procedimiento, siempre y cuando las partes del proceso penal en que se intenta hacer valer hayan tenido oportunidad de controlar su producción o impugnar su resultado y no se estén tildando de falsas sus conclusiones[143].

Una pericia informática real será aquella en donde se preguntan cuestiones informáticas en concreto. De las medidas a las que se refiere el informe del Ing. Presman muchas de las tareas descriptas no son pericia en el sentido procesal penal, tal vez en algunas necesiten otros medios de prueba asimilables, aun cuando intervenga un experto informático.

---

[143] Cfr. Cafferata Nores, José I y Hairabedián, Maximiliano; con la colaboración de Gorgas, Milagros. *La prueba en el proceso penal, con especial referencia a los Códigos Procesales Penales de la Nación y de la Provincia de Córdoba*, págs. 67, 68, 69.

No son periciales propiamente dichas, aunque intervenga un experto técnico[144]: la recolección de datos, sea en la nube de conexión de tráfico o de contenido, ni tampoco la conservación de datos hasta tanto sean recolectados, la recolección de datos en sí misma no es pericial. La asimilación a medios tradicionales ayuda a comprender la cuestión, por ejemplo, los médicos forenses pueden recolectar elementos que luego serán peritados, pero dicha recolección en sí misma no es pericial. Ello lleva a la aplicación analógica de determinadas normas que en realidad no necesariamente se aplican; la recolección de evidencia mediante dispositivos de intercepción; las búsquedas de contenido por criterio; la identificación de imágenes; el análisis de comunicaciones de correo electrónico y redes sociales.

En cambio, son periciales las siguientes tareas en laboratorio: las líneas de tiempo, esto es establecer qué actividad se realizó en una fecha específica o un intervalo de tiempo determinado en la medida en que significa un examen informático; la recuperación de información eliminada, la comparación binaria de archivos para verificar si son idénticos.

En uno u otro caso, el mero hecho que sea ordenado como pericia, en modo alguno exime al Estado de proteger la intimidad, en cualquiera de sus aspectos, o todos al mismo tiempo, si estuviera comprometido estableciendo reglas limitadoras para el caso concreto que mantenga la injerencia dentro de escalas admitidas. De manera tal que, y luego de haber repasado diferentes situaciones que han realizado una aplicación analógica incorrecta, el sistema no ha logrado jurisprudencialmente a estandarizar estas aplicaciones que por momentos parece una decisión aleatoria de la dependencia judicial que intervenga.

Es por ello por lo que, en casos de medidas informáticas, si bien en muchos casos no resulta obligatorio desde el punto de vista constitucional (pues es admisible una aplicación analógica), sí resulta una buena decisión de política criminal regular el acceso a sistemas informáticos con reglas claras que respeten el derecho a la intimidad si se encontrara comprometido, que unifique la regulación del acceso del Estado a comunicaciones en general y la intercepción de la correspondencia. Asimismo, que regule la cadena de custodia.

Ahora bien, ello nos lleva a otra cuestión. Es que, en el contexto, no parece acertado la regulación específica de cada medios o medida informática posible en el día de hoy, porque el avance de las tecnologías es tan veloz que lo que hoy se regule en modo alguno agotará la discusión; en poco tiempo, será obsoleto. La regulación, y el real desafío del derecho procesal penal, debe ser de carácter general, limitaciones jurídicas y requisitos legitimantes y que aporten certezas a

---

144 Cfr. Problemas planteados por el Ing. Presman en su informe para la ADC.

los elementos probatorios incorporados, que permite al proceso penal adaptarse a nuevos medios posibles.

c) Ahora bien, otras medidas que requieren un examen especial, son la utilización de *software* maliciosos (*remote forensic*) y el acceso transfronterizo de datos. Ambas medidas, por su complejidad jurídica, fueron tratadas por Marcos Salt en su excelente tesis doctoral, aquí son resumidas sus conclusiones en virtud de que le asiste razón.

➢ *Software maliciosos*

Esto son mecanismos de acceso remoto a sistemas informáticos mediante la utilización de programas maliciosos por parte del Estado y las diferentes técnicas de adquisición de evidencia digital utilizando estos mecanismos de búsqueda y obtención de información mediante software especiales instalados subrepticiamente en los dispositivos o sistemas informáticos que son objeto de investigación (denominados por algún sector de la doctrina como formas *hacking legal* o troyanos estatales).

Una primera cuestión surge clara, ni el Código Procesal Penal de la Nación (normas del viejo CPP, L.23.984 y del nuevo CPP, L.27.063 –aún en plazo de *vacatiolegis*-) ni el Código Procesal Penal de Córdoba, ni el Código Procesal Penal de la Ciudad Autónoma de Buenos Aires, contienen una norma expresa que habilite la utilización de estos programas informáticos de investigación. Esto significa que no existe una habilitación legal expresa para que el Estado valiéndose de programas informáticos especiales (variables de programas maliciosos troyanos o espías), ya sea que se instalen a distancia mediante engaño y violando las barreras de seguridad informática del sistema informático *objetivo* (utilizando las vías de comunicación electrónica como por ejemplo un mail), o ya sea que se instale subrepticiamente mediante un acceso físico al sistema que es objeto de investigación[145], obtenga de manera general a distancia todos los elementos de prueba de diferente naturaleza que estos medios tecnológicos permiten acceder.

Son medios de investigación *híbridos* que reúnen al mismo tiempo características propias de diferentes medios de investigación (todos ellos intrusivos del ámbito de intimidad) tales como la intervención de comunicaciones, el allanamiento de un espacio físico, el registro y secuestro de cosas o datos, la observación de espacios físicos mediante uso de tecnología, cámara oculta, etc. Así, el uso de estos programas por parte del Estado con todas

---

145 Por ejemplo, mediante la conexión de un *pen drive* al dispositivo informático del sospechoso que permite descargar el programa espía por parte de un agente estatal o cualquier persona con acceso al sistema.

sus potencialidades permitiría obtener datos de contenido y tráfico de comunicaciones en línea, o sea mientras el proceso de comunicación tiene lugar (situación asimilable a una intercepción de comunicaciones), también grabar toda la actividad que se realiza en el sistema informático en tiempo real (presente), incluidas las claves de acceso o códigos de encriptación de archivos que el usuario utilice, sitios *web* a los que ingresa, *blogs* de los que participa, textos o documentos de cualquier tipo que confeccione, películas y videos que visualiza, etc. Asimismo, permitiría mantener un control *similar* (aunque de alcances hasta ahora impensado) a la interceptación de comunicaciones para grabar y enviar a una autoridad estatal por canales informáticos de manera subrepticia todo lo que el usuario realice con el dispositivo informático en el futuro. Así el programa malicioso instalado en la computadora o sistema informático que es objeto de la medida, enviaría al agente estatal una grabación de cada tecla usada, cada movimiento informático que se produzca en el sistema sin discriminación alguna. El programa malicioso en su función de análisis forense a distancia permitiría también el acceso a archivos almacenados en el pasado (documentos, fotos, videos) y su envío mediante internet al agente estatal encargado de la investigación. Esto es, que permite también realizar tareas de registro y secuestro de datos asimilables a lo que se podría obtener en un registro y secuestro de datos durante un allanamiento o, incluso, la posibilidad de realizar tareas de informática forense más propias de una pericia (como puede ser la búsqueda en línea de archivos borrados o guardados en formatos diferentes a los usuales).

Resulta evidente el grado e intensidad de la injerencia estatal en el ámbito de intimidad de las personas que estos medios de investigación significan no configuran una escala admisible por la regulación legal, ni siquiera en su conjunto. De hecho, este conjunto de potencialidades convierte a la utilización de estos programas en una coerción estatal para la obtención de evidencia de mayor intromisión en la intimidad incluso en el tiempo (pasado, presente, futuro) que las medidas hasta ahora admitidas. Todo ello lleva a la exigencia de su regulación legal expresa como condición ineludible para legitimar su utilización (*nulla coactio sine lege*) y la incorporación legítima al proceso de los elementos de prueba que se obtengan mediante estas técnicas.

No existe posibilidad de aplicar por analogía las normas procesales habilitantes de injerencias en la intimidad ni valerse del principio de libertad probatoria como argumento jurídico para justificar el uso de estos medios de investigación, con las normas procesales vigentes no resultan admisibles como prueba válida en el proceso penal, los archivos o datos informáticos que fueran obtenidos mediante lo que se denomina *allanamiento a distancia*, o sea cuando se accede a ellos mediante un programa informático instalado subrepticiamente que posteriormente envía la información almacenada en el pasado mediante

internet a la computadora de los investigadores. No son asimilables ni aplicables analógicamente a un registro y secuestro de datos realizado a distancia las normas procesales previstas para regular la habilitación legal para el allanamiento de domicilio y el registro y secuestro de elementos físicos.

Las normas habilitantes de la intercepción de comunicaciones no resultan aplicables por analogía a la utilización de programas troyanos utilizados por el Estado para obtener documentos o archivos almacenados en un sistema informático ni para obtener claves o cifrados de encriptación que el usuario utilice fuera del marco de una comunicación alcanzada por la normativa procesal.

De este modo, Salt, propone prever habilitaciones legales diferentes (bajo presupuestos y garantías diferentes) para: a. los casos en los que se persigue el acceso a un dispositivo informático o sistema informático solamente con la finalidad de buscar archivos o datos determinados almacenados en el pasado (lo que se ha conocido en el derecho comparado como registro o allanamiento remoto), b. la obtención de datos de identificación del dispositivo o de la comunicación[146] o claves o contraseñas determinadas que se obtienen en tiempo real como preparación de otra medida y c. para el supuesto más intrusivo que este tipo de programas posibilita y que significa habilitar la medida de manera general como medida de *vigilancia* de un sistema informático determinado por un lapso de tiempo (utilización conjunta de todas o varias de las distintas potencialidades de estos programas de acuerdo a lo resuelto por la autoridad judicial)[147].

➢ *Acceso transfronterizo de datos*

En cuanto al acceso transfronterizo de datos, Salt hace algunas diferencias entre los supuestos de datos obtenidos de manera transfronteriza en redes abiertas (datos de acceso general), entiende que su incorporación al proceso no reviste

[146] Tales como la dirección IP utilizada cuando el imputado está usando algún mecanismo que le permite encubrir la dirección IP desde la que opera haciendo imposible identificar al abonado y por tanto obtener los datos necesarios para poder allanar un domicilio con la finalidad de secuestrar los dispositivos informáticos que se utilizan en la comisión de un delito.

[147] Cfr. Salt, tesis doctoral, p. 136 y ss.

mayor problema vinculado a la legitimidad del medio empleado para su adquisición[148] en relación a la posible afectación del principio de territorialidad.

Entiende que resultará válida la obtención de elementos de prueba en los supuestos en los que la información se obtiene mediante un acceso o recepción de datos ubicados en extraña jurisdicción a través de un dispositivo o terminal informática ubicado en territorio propio al que se accede legítimamente (ya sea mediante una orden de allanamiento o requisa legítima conforme a las normas procesales del país en el que se tramita la causa penal) y que se encuentra conectado sin necesidad de operaciones especiales a los datos buscados. Para evitar posibles nulidades de la evidencia así obtenida, entiende que resulta recomendable limitar los alcances de la medida para evitar cruzar esa *frontera* que convierta a la medida en acto de poder jurisdiccional ejercido en otro Estado. También entiende que se pueden considerar válidamente adquiridos para el proceso los datos obtenidos desde una terminal a la que se accede legítimamente cuando resulta imposible conocer de antemano o durante la ejecución de la medida el lugar físico de alojamiento (se advierte que los datos están alojados externamente pero no resulta posible acreditar en qué jurisdicción están el dispositivo o servidor en el que los datos están alojados). Situación que está en aumento en la medida que se generalizan los diferentes tipos servicios informáticos en la nube. En estos casos, la legitimidad de la medida se justifica por la imposibilidad absoluta de recurrir a los canales de cooperación interjurisdiccional nacional o internacional, precisamente porque no se conoce el lugar de alojamiento de la información a la que se puede acceder de manera directa desde la terminal a la que los órganos de persecución penal accedieron legítimamente.

Utilizando el mismo criterio general diferenciador, esto es, determinar si el medio concreto utilizado para el acceso o los mecanismos utilizados para la ejecución de las medidas de adquisición de la evidencia significaron un uso de poder jurisdiccional en extraña jurisdicción, entiende que no resulta válido con las normas vigentes, la prueba obtenida mediante acceso transfronterizos directos utilizando mecanismos técnicos como destrabar claves, engaños, herramientas de *hackeo*, etc. Para llegar a esta conclusión se basa en que la utilización de fuerza estatal en una jurisdicción extraña *violenta el principio territorial* como base fundente de los poderes procesales de investigación e, incluso puede significar la comisión de un delito realizado por las autoridades

[148]La cantidad de datos existentes en redes abiertas que pueden significar elementos de prueba útiles para una causa penal son innumerables. Sólo a modo ejemplo, datos del imputado obtenidos mediante búsquedas en Google, imágenes que muestren la apariencia física de una persona en un momento determinado, fotos o videos publicadas en redes abiertas, noticias periodísticas en portales alojados en extraña jurisdicción, valores de un producto determinado, clima de un lugar, horarios de medios de transporte, manuales de uso de un producto, características y efectos de una medicación, etc.

del Estado en extrañas jurisdicción[149], esto es, la protección de la soberanía nacional.

E. Otra de las estrategias que el sistema ha llevado adelante para adaptar el sistema es la *especialización* en cuestiones o delitos informáticos[150]. Esta especialización en cuestiones informáticas de fiscalías puede brindar eficiencia en la persecución de determinados delitos, sin embargo, no tiene efecto en el sistema penal en general con relación a modernización de evidencia digital y los problemas dentro del proceso penal que acarrean hacia el futuro.

Si bien la decisión de política criminal institucional de diferentes ministerios públicos de establecer fiscalías especializadas en la investigación de determinados tipos de hechos o delitos, ha resultado adecuada en su momento, lo cierto es que, con el desarrollo de las tecnologías, la cuestión informática no se circunscribe a un tipo de delito, ni siquiera a una forma de comisión. Atraviesa transversalmente todo el sistema, para todos los delitos, en lo que a la evidencia digital se refiere.

Lo que en un principio se refería a delitos denominados *informáticos* o cuya comisión fuera digital, informática, electrónica, se encuentra tan extendida en el sistema de manera que ya no existe especialización, sino que cualquier delito, con relación a cualquier tipo de hecho, abarcará los problemas de la evidencia digital. En este sentido, la *especialización* no ha construido estándares sólidos desde el punto de vista jurídico, ni resultan referentes institucionales para asistir a otros operadores jurídicos del sistema del modo en que sería más útil, justamente por su carácter sesgado de especialización[151]. De manera tal que este tipo de especializaciones ya no tendrán sentido en el futuro.

En este sentido, el ingreso y perfeccionamiento de la tarea de los técnicos informáticos y de los investigadores técnicos, ha tenido mucho más éxito en la

---

[149] Cfr. Salt, tesis doctoral, p. 252 y ss.

[150] Fiscalías especializadas, por ejemplo, *Unidad Fiscal Especializada en Ciberdelincuencia*, unidad fiscal especializada en ciberdelincuencia en el ámbito de la Procuradora General de la Nación que tiene por objeto el cibercrimen, especialmente en la investigación del crimen organizado. En el mismo sentido, aunque su tarea principal parecen ser los delitos en contra la integridad sexual *on line* (*grooming,* pornografía infantil), las fiscalías especializadas en delitos informáticos de la CABA. La Fiscalía de la Ciudad cuenta con tres fiscalías especializadas en delitos informático, cuenta con Red 24/7 que conforman todas las Fiscalías del país en casos de pornografía infantil en Internet a nivel nacional, la Red 24/7 es coordinada por el Cuerpo de Investigaciones Judiciales de la Fiscalía, constituido por un equipo interdisciplinario que asiste a los fiscales en intervenciones de campo y casos complejos.

[151] El único desarrollo que han tenido estas experiencias se vincula mucho más con desarrollos individuales que con un desarrollo institucional relevante.

construcción de estándares y protocolos de actuación que ayudan a brindan certeza a las medidas probatorias.

Mucho más útil para el sistema es la consolidación de estos cuerpos informáticos que pueden llegar al sistema de manera transversal. El desarrollo y la cooperación con los operadores jurídicos del sistema en brindar la información[152] y trabajo en conjunto para poder aprovechar *in extenso* las posibilidades técnicas de la evidencia digital o asesorar en aparatología forense. Ello sí puede producir cambios más relevantes en el sistema.

Esta tarea de consolidación, fortalecimiento de cuerpos técnicos, sin embargo, no se trata de un problema estricto del derecho procesal penal, sino antes bien, de la gestión institucional. El carácter habilitante de los expertos ya sido resuelto en la regulación de los medios probatorios en el sistema con un criterio amplio[153] , de manera que no ofrece problema. La formalización de protocolos de actuación de la actividad forense (en la cuestión informática, como en cualquier otro tema) tampoco requiere de regulación a nivel legal, ni es un problema del derecho procesal penal[154].

[152] Ello muchas veces incluso en la forma de obtener información o dirigirse a las empresas proveedores de internet (Google, Facebook, Microsoft, etc.)

[153] Cfr. CPPN. 254 y normas similares en otros códigos procesales penales.

[154] Cfr. los problemas planteados por el Ing. Presman en su informe para ADC.

6. Conclusiones

A.La *evidencia digital* en el proceso penal, enfrenta al sistema jurídico penal a uno de los desafíos más importantes de la historia. El problema lo afecta de manera transversal pues se vincula con la recolección de elementos probatorios en todo tipo de casos.

En el derecho comparado hace 15 años que se viene trabajando en este tema. La cooperación internacional a través de la Convención de Budapest del Consejo de Europa propicia la incorporación normativa de determinas normas, también procesales, buscando consenso internacional con el objeto de unificar normas, incorporar las redes 24/7, flexibilizar normas de cooperación internacional, etc. Argentina es miembro desde diciembre 2017. Sin embargo, dicha ratificación no implica solucionar los problemas que se plantean a nivel procesal que aún van a persistir. Si bien Argentina tiene la necesidad internacional de ser parte de la Convención, los reales problemas del moderno derecho procesal penal que en modo alguno se agotan, ni finalizan con la Convención ni la adaptación a su normativa, que incluso a esta altura puede no resultar novedosa. Además, tiene la tarea ante países más poderosos de que exista un equilibrio adecuado con los derechos constitucionales de los ciudadanos y la protección de la soberanía nacional.

Otra estrategia que se ha llevado adelante para adaptar el sistema a la problemática es la *especialización* en cuestiones o delitos informáticos, ya no tendrán sentido en el futuro, pues la problemática es transversal del sistema. La *especialización* no ha construido estándares sólidos desde el punto de vista jurídico, ni resultan referentes institucionales para asistir a otros operadores jurídicos del sistema del modo en que sería más útil, justamente por su carácter sesgado de especialización. Debe ser reforzado el perfeccionamiento de la tarea de los técnicos informáticos y de los investigadores técnicos, que sí ha tenido mucho más éxito en la construcción de estándares y protocolos de actuación que ayudan a brindan certeza a las medidas probatorias, lo que antes que un problema procesal resulta de gestión institucional.

Este tipo de discusión tiene una dificultad adicional que se refiere a que la problemática se encuentra atravesada por la intervención de empresas proveedoras de internet en la discusión. Las empresas tienen su propia agenda —por supuesto, en resguardo de sus intereses— y actúan con el poder casi de un Estado, en virtud de que alojan datos, que muchas veces ni siquiera se sabe en qué jurisdicción. Tanto es así que incluso en la investigación de casos en particular, son las propias empresas que imponen reglas que deben seguir las autoridades estatales para obtener información, lo que debería resultar inadmisible.

B.En Argentina, la discusión no se profundizado y no se la ha dado la seriedad que la complejidad requiere, ello afecta la vigencia de garantías de los ciudadanos. El sistema ha intentado solucionar el problema que plantean las nuevas tecnologías de la manera del principio de libertad probatoria, realizando una aplicación analógica de los medios de prueba tradicionales no siempre de manera correcta y en general de un modo deficiente, esto es, sin abarcar las posibilidades que plantea el caso concreto. Ello trae diversos inconvenientes que el sistema no suele advertir y que legitima en virtud de que la extensión de esta aplicación. Así surge del repaso de casos en donde las objeciones fueron planteadas de manera seria, que evidencia la incapacidad del sistema para brindar una respuesta adecuada que violenta el derecho a la intimidad.

A pesar de que este tema se analiza hace años, el sistema no advierte de manera correcta el problema jurídico por detrás, el compromiso de determinados ámbitos de intimidad que fueron desprotegidos, la carencia de certeza de elementos probatorios recogidos (de manera ilegítima) y a través de la aplicación analógica (tal vez autorizada desde el punto de vista constitucional pero realizada de manera errónea). De hecho, el sistema suele confundir la vigencia del derecho constitucional con la certeza del elemento probatorio, que se trata cuestiones diferentes.

Ello tampoco significa que toda aplicación analógica se encuentra prohibida desde el punto de vista constitucional pues no resulta tan claro que por el mero hecho de que se acceda a determinados ámbitos protegidos por medios tecnológicos, informáticos, electrónicos, ello no se encuentre previsto. Si el medio tecnológico permite acceder a las comunicaciones, resulta irrelevante el medio en que se accede, lo que regula la ley son los requisitos jurídicos para dicho acceso y no el medio por el que se accede. De manera tal que es posible sostener —no sin discusión— que el legislador ha admitido esas intrusiones, la dificultad es cómo hacerla.

Es por ello que acceder a un sistema informático resulta una medida de coerción probatoria, debe ser ordenada por un juez (CN, 116) y dentro de las exigencias formales establecidas por el legislador para acceder a determinados ámbitos de intimidad (CN, 18), que aporte una motivación suficiente que permita establecer el motivo por el cual es necesario ese grado de intrusión, criterios de proporcionalidad en la disposición de la medida, y el menor gravamen posible para lograr una eficacia de la medida sin violentar o restringir el derecho a la intimidad u otros más allá de lo necesario. Ahora bien, esta medida debe tener en cuenta —*para adquirir legitimidad*— el grado de intrusión en la intimidad para determinar cuáles son los requisitos que la medida debe abarcar, y tener cuenta la extensión y gravedad de dicha intrusión. De manera tal que la decisión

de si se encuentra abarcada la medida por el legislador, establecer de qué modo es posible realizar una aplicación analógica, y en su caso, a qué medida se refiere, no resulta una tarea sencilla, y el sistema suele fallar en este aspecto poniendo en riesgo la validez de la medida. No parece posible sostener con seriedad jurídica que toda medida sobre un sistema informático se encuentra prohibida por no estar regulada, ello carece de rigor, pues el medio no es lo relevante, sino antes bien, el grado de compromiso en la restricción del derecho. Lo que va a determinar su legitimidad son las circunstancias del caso concreto (caso/capacidad de la medida) y el grado de intromisión que significa. En este sentido, puede implicar cumplir con los requisitos de una orden de allanamiento, la intercepción de la correspondencia y la intervención de comunicaciones (todas al mismo tiempo), no sólo en la orden sino también en su ejecución, incluso puede significar delimitar temporalmente la medida.

Resulta un problema extremadamente complicado que obliga a soluciones complejas para cada caso en particular desgranando posibles afectaciones a la intimidad, junto y especialmente la amplitud de la injerencia, los medios tecnológicos utilizado, la regulación normativa del medio de prueba aplicado. No obstante, el sistema trata la problemática jurídica de la *evidencia digital*, unificando las circunstancias, simplificando las soluciones, lo que constituye un error. Por esta razón, si bien no siempre es necesario desde el punto de vista jurídico constitucional, tal vez resulte una adecuada solución de política criminal la regulación del legislador, aunque no la única, pues también debe trabajarse en la formación de operadores del sistema para la aplicación analógica, y el fortalecimiento de equipos técnicos informáticos.

C. La afectación de la tecnología en la intimidad de los ciudadanos, obliga a una regulación (cuando ello es necesario) muy rigurosa. En este sentido, resulta interesante el concepto de la Corte Federal Constitucional Alemana que reconoce un nuevo derecho fundamental constituido por la garantía a la *confidencialidad e integridad de la información en sistemas informáticos* como una derivación del derecho a la personalidad y la dignidad. Resulta relevante advertir el grado de amplitud (en virtud de algunos medios tecnológicos o en algunos casos en particular) de la injerencia a la intimidad.

Existe obligación constitucional (y por ende, se encuentra prohibida la aplicación analógica) del *software* maliciosos (*remote forensic*) y el acceso transfronterizo de datos. Ello es así en virtud del grado e intensidad de la injerencia estatal en el ámbito de intimidad de las personas que estos medios de investigación significan no configuran una escala admisible por la regulación legal, ni siquiera en su conjunto. En cuanto al acceso transfronterizo de datos, deben ser regulado el acceso directo utilizando mecanismos técnicos como destrabar claves, engaños, herramientas de *hackeo*, etc., en virtud de la

utilización de fuerza estatal en una jurisdicción extraña que *violenta el principio territorial* como base fundante de los poderes procesales de investigación e, incluso puede significar la comisión de un delito realizado por las autoridades del Estado en extrañas jurisdicción.

La regulación normativa en muchos otros casos no resulta obligatoria desde el punto de vista constitucional (pues es admisible una aplicación analógica), pero sí resulta una buena decisión de política criminal regular el acceso a sistemas informáticos con reglas claras que respeten el derecho a la intimidad si se encontrara comprometido, que unifique la regulación del acceso del Estado a comunicaciones en general y los sistemas informáticos, así como regular la cadena de custodia.

Ahora bien, esta regulación implica una *nueva concepción en la manera de regular medios de prueba*, que permita ser sostenida en el tiempo y resistir los embates de los avances tecnológicos. Es que, en el contexto descripto, no parece acertado la regulación específica de cada medios o medida informática posible en el día de hoy, porque el avance de las tecnologías es tan veloz que lo que hoy se regule en modo alguno agotará la discusión; en poco tiempo, será obsoleto. La regulación ─ y el real desafío del derecho procesal penal─, debe ser de carácter general a los sistemas informáticos, estableciendo limitaciones jurídicas, temporales y requisitos legitimantes y que aporten certezas a los elementos probatorios incorporados, que permita al proceso penal adaptarse a nuevos medios posibles.

Bibliografía indispensable sobre el tema

Bruzzone, Gustavo, *La nulla coactio sine lege como pauta de trabajo en materia de medidas de coerción en el proceso penal*, publicado en Estudios sobre Justicia Penal. Homenaje al Profesor Julio B.J. Maier, Editores del Puerto, Buenos Aires, 2005.

Cafferata Nores, José I. y Hairabedian, Maximiliano, *La Prueba en el Proceso Penal. Con especial referencia a los Códigos Procesales Penales de la Nación y de la Provincia de Córdoba*, *Sexta edición*, Lexis Nexis, Argentina, 2008.

Data Protection and Cybercrime Division del Consejo de Europa, *Guía de Prueba Electrónica. Guía básica para Fuerzas y Cuerpos de Seguridad, Jueces y Fiscales*, versión en español, Estrasburgo, Francia, marzo del 2013.

García, Luis, *"La intervención de las comunicaciones telefónicas y otras telecomunicaciones en el Código Procesal Penal de la Nación: un cheque en blanco para espiar nuestra vida privada"*, publicado en Cuadernos de Doctrina y Jurisprudencia Penal, nro. 6, 1997, editorial Ad Hoc, Buenos Aires.

Garibaldi, Gustavo, *Tesis Doctoral Las Modernas Tecnologías de Control y de Investigación del delito. Su incidencia en el derecho penal y los principios constitucionales*, editorial Ah Hoc, 2010.

Gercke, Marco, *Understanding Cybercrime. Phenomena, Challenges and Legal Response*, publicación del Cybercrime Research Institute, segunda edición, agosto del 2011.

International Telecommunication Union, *Manual de Comprensión del Ciberdelito. Fenómenos, Dificultades y Respuestas Jurídicas*, publicación de la versión en Español de Septiembre del año 2012, disponible en http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Legal-Measures.aspx

Kerr, Orin S. *Digital Evidence and the New Criminal Procedure*, Columbia Law Review, Vol. 105:279;
Searches and Seizures in a Digital World, publicado en Harvard Law Review, nro. 119, año 2005, págs. 531-585.

Pérez Barberá, Gabriel, *El Principio General de Reserva de Ley (o principio general de legalidad en la doctrina alemana)*;

Nuevas Tecnologías y libertad probatoria en el proceso penal, ponencia presentada en el VI Encuentro Nacional de Profesores de Derecho Procesal Penal, Salta, mayo de 2009.

Salt, Marcos, *Criminal Procedure Law Provisions on Cybercrime in Latin America Regarding Their Compliance with the Budapest Convention (Argentina, Chile, Colombia, Costa Rica, Mexico, Paraguay and Peru)*, informe preparado para el consejo de Europa, Estrasburgo, 2011;
Identity related crime in Latin American Countries, Estudio realizado para el Grupo de Expertos sobre Identidad Robada de Naciones Unidas (UNODC), diciembre del año 2010;
Nuevos Desafíos de la evidencia digital. El Acceso trasfronterizo de datos en los países de América Latina, publicado en Derecho Penal y Procesal Penal, editorial Abeledo Perrot, Buenos Aires, 2013;
Tecnología informática: ¿un nuevo desafío para el proceso penal?, XXV Congreso Nacional de Derecho Procesal Penal, Rubinzal Editores.
El acceso transfronterizo de datos y las técnicas de acceso remoto a datos informáticos: nuevos desafíos de la prueba digital en el proceso penal, su tesis doctoral presentada en Córdoba en mayo 2017, recientemente editada Ad-Hoc.

Sieber, Ulrich, *The International Handbook on computer Crime*, Ed. John Wiley &sonsUd, 1986, Gran Bretaña.