Revista Electrónica de Estudios Penales y de la Seguridad
ISSN: 2531-1565

LA OBTENCIÓN DE EVIDENCIA DIGITAL EN UN MARCO DE COOPERACIÓN INTERNACIONAL

OBTAINING DIGITAL EVIDENCE IN A FRAMEWORK OF INTERNATIONAL COOPERATION

María Julia Solari
Abogada / Secretaria Judicial
Universidad de Palermo (Argentina) / Tribunal Oral en lo Criminal Federal

Fecha de recepción: 3 de mayo de 2018

Fecha de aceptación: 10 de septiembre de 2018

RESUMEN

Internet es un ámbito que desafía las categorías jurídicas tradicionales de soberanía y territorialidad de los Estados y rompe con el paradigma clásico de cooperación internacional entre estos. Se puede observar una mayor afectación a derechos y garantías constitucionales a la hora de recolectar evidencia digital en investigaciones criminales, porque los códigos de procedimiento fueron pensados para la obtención de evidencia física. De esta forma, somos testigos de un fenómeno novedoso: podemos llegar a soluciones jurídicas y procedimentales inadecuadas, por partir de una catálogo de derechos que protegen a los ciudadanos contra las injerencias de los Estados, creados cuando no existía la lógica imperante de hoy en internet, de base privada y libre. En este nuevo contexto, se vuelven también necesarias nuevas definiciones, sobre todo a la hora de investigar ponderando valores como la seguridad nacional frente a la privacidad de los ciudadanos.

ABSTRACT

The world wide web, as an environment, defies the existing legal categories regarding the sovereignty and territoriality of the states, breaking in the process the established paradigms of interstate cooperation. Given that the procedure codes were established only with the aim of obtaining physical evidence, it can be observed that constitutional rights and guarantees are often broken when it comes to gather digital evidence for criminal investigations. Therefore, the world is being witness of a whole new process: the provision of inadequate legal and procedural solutions in the context of a legal code that was established to protect citizens from state's interference long before the advent of the modern form of internet, based on private and free access. This new context demands brand new definitions, especially when investigations are made

in the thin line between confronted values such as national security and the citizenry's right to privacy.

PALABRAS CLAVE

Evidencia digital – cooperación internacional – jurisdicción – soberanía – investigaciones criminales

KEYWORDS

Digital evidence – international cooperation – jurisdiction – sovereignty – criminal investigation

ÍNDICE

SUMMARY

1. INTRODUCCIÓN

El objetivo del presente trabajo es efectuar un análisis sobre los desafíos implicados en la obtención de evidencia digital, que pone en el centro del debate a internet como

fenómeno que rompe con los paradigmas clásicos de cooperación internacional basados en la idea de territorialidad y soberanía nacional.

Realizaré el estudio estructurado en diferentes niveles: en primer lugar analizaré las ideas vinculadas a las categorías tradicionales de soberanía, principio de territorialidad, sujetos y protección de garantías individuales frente a los desafíos que nos trae la red; y cómo todo ello incide en las formas de llevar adelante la recolección de evidencia. En un segundo nivel intentaré evaluar cómo modifican este tipo de investigaciones criminales a las formas de cooperación en materia penal; para finalmente extraer algunas conclusiones de carácter preliminar sobre el tema que nos convoca.

2. LA TENSIÓN ENTRE DOS PARADIGMAS

El ciberespacio es un ámbito que desafía las categorías jurídicas tradicionales de soberanía y principio de territorialidad, así como las vinculadas a la protección de garantías individuales. En supuestos de comisión de delitos informáticos o de investigaciones criminales en las que sea de relevancia el uso de evidencia digital, el problema radica en que las normas de la mayoría de los países fueron creadas pensando en la obtención de evidencia física, lo que no da respuestas adecuadas en la práctica. Lo mismo parece suceder en cuanto a la forma tradicional de cooperación entre Estados en investigaciones de esta clase.

En parte, el problema parece remontarse a algo más profundo que simples normativas de procedimiento o la suscripción de acuerdos entre países: radica en toda una construcción de Estados nacionales con sus respectivos textos constitucionales -que protegen principios fundamentales de los ciudadanos de las injerencias de esos Estados- creados cuando no existía la lógica imperante en internet, de base privada y libre[1].

La gravedad está en que la aplicación por analogía de los principios del espacio real al espacio virtual puede traer aparejada una mayor afectación de derechos, sobre la base de que en la era digital, tanto el control privado como el estatal tienen la misma destacada característica: el control, o el registro, pueden incrementarse en gran medida sin que resulten necesariamente más molestos para quienes los padecen.

Un ejemplo de ello es el uso de fragmentos de códigos informáticos que se sueltan en la red para que se introduzcan en ordenadores vulnerables –también llamados "gusanos"-. Su uso sería análogo a un allanamiento de morada, aunque no requiere de sospechas para motivarlo. El programador accede a la información sin interferir en el funcionamiento de la computadora, con lo cual la persona investigada no es perturbada.

En ese caso se ve claramente que la eficacia de esta clase de medios de vigilancia, que si bien no generan molestias a los involucrados, pueden afectar la libertad y la

[1] LESSIG, Lawrence, *The code version 2.0*, Cambridge, Basic Books, 2006.

privacidad. Esto da un marco de mucha ambigüedad y por ende dudas en la aplicación de las normas.

En esta lógica, el ciberespacio plantea desafíos y problemas a la hora de ponderar con nuestras constituciones y catálogo de derechos la privacidad, la libertad de expresión, los mecanismos de control, la interacción entre la ley y la tecnología, quién regula internet, qué criterios de jurisdicción se aplican, o cómo conviven las soberanías, entre otros debates[2].

Es que el cambio tecnológico ha tornado ambiguos los compromisos de los Estados en esas temáticas; cuestiones que exceden los fines de este trabajo pero que nos permiten enmarcar el contexto en el que nos encontramos y a partir del cual se nos ofrece la posibilidad de repensar nuestros esquemas judiciales.

En especial nos obligan a pensar nuestras Constituciones, entendidas no solo como un texto legal sino como una arquitectura *"que estructura y constriñe los poderes sociales y legales con el propósito de proteger una serie de principios fundamentales"*[3]. De esta idea se disparan interrogantes vinculados a qué mecanismos de control son posibles en este espacio virtual, cómo se separan los poderes o de qué manera se puede asegurar que el regulador de internet –una suerte de Estado- no acapare todo el poder pero que tampoco le falte.

Antes de analizar más en profundidad la cuestión vinculada a la obtención de evidencia y a la cooperación, creo que es importante tener un marco más amplio de hasta qué punto internet nos pone en una necesidad de repensar nuestras formas de regular conductas. Por ello, a continuación detallaré brevemente cómo se ven afectados en concreto los diferentes supuestos vinculados a la configuración de nuestros Estados nacionales y la protección de derechos individuales, tal como lo concebimos hasta ahora.

2. 1. La jurisdicción, la idea de territorialidad y las soberanías en la era digital

La jurisdicción se basa principalmente en la división geográfica del mundo en territorios nacionales, siendo que cada Estado tiene el derecho soberano de ejercer jurisdicción sobre su territorio[4]. Sin embargo, tanto en el caso de comisión de delitos informáticos como en investigaciones donde sea relevante la evidencia digital, en general las acciones transnacionales ponen en tela de juicio la soberanía de los Estados.

Si partimos de la idea que el ciberespacio es un lugar, la pregunta necesaria es: ¿dónde estamos cuando estamos allí? Frente a un monitor, en realidad nos encontramos

[2] En ese sentido, sobre problemas de "ambigüedad latente", ver: LESSIG, Lawrence, *The code version 2.0*, Cambridge, Basic Books, 2006.
[3] LESSIG, Lawrence, *The code version 2.0*, Cambridge, Basic Books, 2006, capítulo "El código es la ley", página 35.
[4] KURBALIJA, Jovan y GELBSTEIN, Eduardo, *Gobernanza de internet. Asuntos, actores y brechas*, publicado por DIPLO Foundation, 2005, página 80 y siguientes.

en muchos lugares al mismo tiempo, porque se conectan puntos que muchas veces no tienen que ver con la geografía del mapa. De allí surge otra pregunta necesaria: ¿quién es el soberano en ese contexto?[5]

Aquí entran en colisión los criterios para determinar la jurisdicción en el ciberespacio. A modo de ejemplo, se pueden citar:

1) Modelo del autor: la jurisdicción se asigna conforme el lugar donde esté físicamente el autor (de una difamación, por ejemplo). Este criterio no es útil cuando existen anónimos y también en casos donde se afecte la reputación o la privacidad, porque la víctima puede estar impedida de ejercer sus derechos fundamentales, o deberá concurrir a una jurisdicción extraña a dichos efectos;

2) Modelo de la víctima: la jurisdicción en estos casos se determinará conforme el lugar donde se halla la víctima o donde se producen los efectos de la acción. Como correlato con el principio anterior, aquí la dificultad para hacer valer sus derechos será para el actor;

3) Modelo del servidor: aquí se determina la jurisdicción a partir del lugar donde se encuentran los datos. Este criterio trae aparejada la problemática de no satisfacer ni al actor ni a la víctima y en que en muchos casos no se sabe estrictamente dónde se encuentran los datos;

4) Modelo de ejecución: que sigue los estándares de ejecución de sentencias. Este criterio resuelve lo atinente a la ejecución de la medida; más no así concretamente la determinación de la competencia.

Sobre este punto corresponde remarcar que, en general, en casos civiles se ha entendido que correspondía el criterio de la víctima y en casos penales el del autor, para propiciar la garantía de la defensa en juicio.

Los modelos antes expuestos también podrán verse afectados en función de los principios de aplicación de la ley penal que tengan los países; es decir, los principios de territorialidad, real o de defensa, de personalidad o universal[6].

2. 2. Los sujetos en la era digital

En internet necesariamente se observa una descentralización de los actores. En la comisión de delitos informáticos quien comete el delito puede pertenecer a otra jurisdicción a donde se producen los efectos. El panorama se complejiza aún más si tenemos en cuenta que existen nuevos sujetos que son los intermediarios.

[5] Sobre este punto, ver www.internetjurisdiction.net , donde se relevan los problemas de esta tensión.

[6] El Convenio de Budapest sobre Cibercrimen elaborado en el marco de Consejo de Europa (que es de momento el instrumento más relevante en la materia) afirma criterios de territorialidad, aunque permite que los Estados puedan no aplicar las normas de jurisdicción en algunos supuestos específicos (art. 22).

Estos últimos son en general proveedores de acceso, de tránsito, de alojamiento y de contenidos, que contribuyen a la transmisión del contenido, pero no lo crean. Por su rol central en lo vinculado al acceso, alojamiento y facilitamiento de búsquedas e intercambios de contenidos que circulan por la red, a nivel legal, comenzaron a perfilarse diferentes lineamientos en cuanto a la asignación o no de responsabilidad civil o penal, fundadas en su posibilidad de lesionar bienes jurídicos.

Resulta interesante hacer mención a las aristas de estos actores de internet, por ser particulares de este ámbito y para poder contextualizar la complejidad inherente a la red en cuanto a que nos obliga a encontrar nuevas formas de pensar las cosas.

Así, en lo que respecta al ámbito civil, existen diferentes criterios posibles de determinación de responsabilidad para estos intermediarios[7]. En primer lugar se encuentra el de inmunidad absoluta, que supone que los intermediarios no son responsables. Este es el criterio en los Estados Unidos en lo que respecta a daños a la honra y reputación ocasionados por terceros (regido por la sección 230 del Communicatios Decency Act). Aquí se observa la alta valoración a la libertad de expresión, frente a la privacidad.

Otro criterio es el de responsabilidad objetiva, que obliga al intermediario a reparar el daño que produzca por la cosa riesgosa, por razones independientes a su conocimiento del ilícito. Aquí surgen problemas y riesgos para el intermediario, ante la dificultad para conocer con anterioridad si el contenido que está facilitando en la web es legal o no. Ello, toda vez que esta clase de obligaciones que se le imponen pueden ser difusas, si se considera que el mismo intermediario deberá realizar juicios de valor sobre la legalidad de las acciones del usuario.

También puede citarse el criterio de responsabilidad subjetiva, que trae aparejado un deber de supervisión constante. A este criterio se lo relaciona con el de inmunidad condicionada, mediante el cual se condiciona la responsabilidad al conocimiento efectivo de la irregularidad. Es decir, la inmunidad estará en definitiva condicionada al cumplimiento por parte de los intermediarios de diferentes obligaciones o condiciones. Por ejemplo, el sistema de notificación y bajada o “notice and takedown”.

En este último caso la complejidad radica en que cualquier notificación puede ser suficiente para configurar el conocimiento y promover la bajada inmediata de la

[7] En ese sentido, los Principios de Manila, si bien no son vinculantes sirven de guía, ver: Manila Principles on intermediary liability, en https://www.manilaprinciples.org/; así como el Informe de la UNESCO, *Fostering Freedom online: the role of internet intermediaries*, año 2014, disponible en: http://unesdoc.unesco.org/images/0023/002311/231162e.pdf. Conforme esos principios, se propone: I. Los intermediarios deberían estar protegidos por ley de la responsabilidad por el contenido de terceros; II. No debe requerirse la restricción de contenidos sin una orden emitida por una autoridad judicial; III. Las solicitudes de restricción de contenidos deben ser claras, inequívocas y respetar el debido proceso; IV. Las leyes, órdenes y prácticas de restricción de contenidos deben cumplir con los tests de necesidad y proporcionalidad; V. Las leyes, políticas y prácticas de restricción de contenidos deben respetar el debido proceso; y VI. La transparencia y la rendición de cuentas deben ser incluidas dentro de la normativa, políticas y prácticas sobre restricción de contenido.

información, con la afectación a derechos como la libertad de expresión, frente a la necesidad del intermediario de evitar sufrir responsabilidad. Lo mismo cabe referir con relación al filtrado de contenidos, que puede configurar una estrategia invisible, utilizada por un intermediario para cubrir su eventual responsabilidad.

En Argentina, por ejemplo, la jurisprudencia ha sentado la postura de la responsabilidad civil de los motores de búsqueda, en la medida de su conocimiento. Ello implica que un buscador puede llegar a responder por un contenido que le es ajeno si tomó efectivo conocimiento de la ilicitud, y si tal conocimiento no fue seguido de un actuar diligente[8].

En lo atinente al ámbito penal, los criterios difieren a la hora de asignar responsabilidad penal a personas jurídicas[9]. Sobre este punto es interesante remarcar que en su art. 12 la Convención de Budapest sobre Cibercrimen promueve que los Estados adopten medidas legislativas y las que resulten necesarias para que pueda exigirse responsabilidad a las personas jurídicas, invitando –en su art. 13. 2- a la imposición de sanciones efectivas, proporcionadas y disuasorias, incluidas sanciones pecuniarias.

En este sentido, el modelo anglosajón prevé la posibilidad de imputar a las corporaciones por los hechos de sus representantes, mientras que la tradición románico-germánica no, por partir de la culpa del sujeto individual[10].

Sobre este apartado me parece interesante apuntar otro elemento a tener en consideración con relación a la actuación de los intermediarios en internet: racionalmente es un actor que va a priorizar su propio beneficio, con lo cual, ante una normativa que le imponga la revisión exhaustiva de contenidos, es lógico que no tenga en cuenta el valor expresivo del usuario, lo cual puede atentar, en resumidas cuentas, contra la libertad de expresión.

De esta forma se produce una tensión entre la reglamentación vinculada a estos actores en un contexto de derechos de autor, pornografía infantil, ataques a la honra, intimidad o dignidad –cada una de estas temáticas con un valor de expresión distinto y con intereses colectivos e individuales diferentes- frente al potencial impacto de esas reglas sobre la libertad de expresión.

Aquí lo particular de estos supuestos es que las soluciones que tienden a buscar una respuesta universal para todos los casos no suelen ser adecuadas, ya que es necesario observar las particularidades de cada contexto expresivo.

---

[9] Conforme doctrina sentada por la Corte Suprema en: CSJN, R. 522.XLIX, rta. 28/10/14 –"Rodríguez, María Belén c/Google Inc. s/daños y perjuicios" y otros.

[10] Concretamente en Argentina, pese a la sanción de la ley 26.388 no se ha contemplado la sanción penal expresa a estos proveedores. En ese sentido, ver CHERÑAVSKY, Nora, *Responsabilidad penal de los proveedores de servicios de internet*, publicado en Sistema Argentino de Información Jurídica (SAIJ) en agosto de 2014.

Después de lo expuesto puede observarse la complejidad inherente a estos nuevos actores de internet, para observar hasta qué punto se necesita una nueva normativa y criterios para pensar las investigaciones criminales y la determinación de responsabilidad en cada caso. Ello, toda vez que, como se puede observar, los intermediarios no solo hacen posible nuestra actividad en la web, sino que la moldean según sus propias necesidades.

2. 3. La interpretación de principios constitucionales en la era digital

En cuanto a la protección de derechos individuales existe una tensión entre la protección a la privacidad e intimidad y la necesidad de proveer a la seguridad nacional, siendo estos dos los valores que principalmente han de ponderarse en el contexto de las redes.

Lo nuevo en este esquema es qué definición se le dará de aquí en más al término "privacidad", que originalmente siempre fue entendida como un límite sustantivo a la intromisión del poder estatal en la esfera íntima. Ello por cuanto en el ciberespacio son las empresas privadas las que en general tienen más información sobre las personas -más que los Estados-. Cuando navegamos por internet cada paso que damos acumula información, datos que brindamos en forma "voluntaria", siendo que de esa forma los proveedores de servicios registran nuestras búsquedas y utilizan los datos para evaluar nuestras pautas de consumo.

Ello no tendría por qué ser un problema *a priori*, pero podrían surgir inconvenientes si aparecen otras necesidades que impliquen darle otro uso a esa información, como podría ser la justificación de la vigilancia digital en la protección de bienes jurídicos como la seguridad nacional.

Aquí también estamos frente a definiciones con bordes poco claros, siendo necesario redefinir qué es privacidad, si aplica también a la protección de la dignidad o a limitar cualquier tipo de intrusión[11].

En este contexto resulta necesario promover la aplicación de pautas claras en los procedimientos judiciales. Como ejemplo de ello se pueden citar los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones[12]:

1) Legalidad, es decir, que ese medio de vigilancia digital esté prescripto por ley;

2) Objetivo legítimo de la ley (que no sea discriminatoria, por ejemplo);

[11] En ese sentido, ver el capítulo once del libro de LESSIG, Lawrence, *The code version 2.0*, Cambridge, Basic Books, 2006. Allí el autor habla sobre la privacidad y la ambigüedad latente de ese término.

[12] Sobre la afectación a la privacidad, ver los 13 Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, que pueden servir de guía, disponibles en: https://necessaryandproportionate.org/principles.

3) Necesidad de ese objetivo legítimo, verificando por ejemplo si existen otros medios menos intrusivos;

4) Idoneidad;

5) Proporcionalidad: debe ser evaluada la intervención de comunicaciones en casos graves. En estos supuestos el daño que se provoque eventualmente a la privacidad debería ser menor al beneficio que se obtiene. Por ejemplo, si se interfiere en el ámbito privado de una persona debe ser a partir de una ponderación vinculada a un interés público;

6) Autoridad judicial competente: que sea un juez o un organismo designado el que determine la intervención, así se asegura el cumplimiento de las garantías. En estos casos las autoridades deben ser independientes del poder político;

7) Debido proceso: dar la posibilidad de que la persona afectada pueda defenderse frente a una eventual violación de una garantía;

8) Notificación del usuario: en este caso habrá de evaluarse la pertinencia de la notificación, sobre todo en caso de investigaciones delicadas;

9) Transparencia: mediante la promoción de informes de transparencia;

10) Supervisión pública: un principio estrechamente vinculado a la transparencia, dando posibilidad a la ciudadanía de controlar los actos de gobierno y de las empresas privadas;

11) Integridad, seguridad y privacidad de sistemas de comunicación: este principio propone que los Estados no puedan solicitar a los proveedores la retención de datos *a priori*, o la identificación de usuarios, entre otros supuestos.

12) Garantías para la cooperación internacional: se trata concretamente de mecanismos de acuerdo de asistencia jurídica recíproca en caso de investigaciones transfronterizas. Dado que los datos pueden ser borrados de manera rápida, son necesarios canales de comunicación veloces.

13) Garantías contra el acceso ilegítimo: este principio prevé que la información sea utilizada para el fin determinado y luego eliminada o devuelta a su procedencia, para evitar otros usos, entre otras cuestiones.

3. CÓMO INCIDE LA CUESTIÓN DE LA TECNOLOGÍA EN LOS PROCESOS PENALES

Ahora sí después de analizar la situación general de la incidencia de internet en nuestra concepción tradicional, corresponde observar qué sucede en el marco de procesos criminales, ya sea por la comisión de los denominados delitos informáticos o en supuestos de obtención de evidencia de tipo digital.

Preliminarmente, corresponde mencionar que el dictado de **normas penales de fondo** que prevean específicamente los "delitos informáticos" es de relevancia por diversos motivos.

En primer lugar, ello sirve para garantizar el debido proceso, si partimos de la base que no existe delito sin ley previa (art. 18 de la Constitución Nacional) y que no es posible

la aplicación de la ley penal por analogía. A su vez, ante la velocidad de innovación en las redes, normas legales claras permiten que las conductas no queden impunes ante la falta de una normativa específica; además de asegurar la reciprocidad necesaria a la hora de requerirse colaboración de otras jurisdicciones.

Ahora sí, respecto al punto que es motivo de este trabajo, en el caso de **normas de procedimiento,** existe la tendencia a aplicar, en parte, en forma analógica, institutos que ya conocemos.

Por ejemplo, se plantean interrogantes: la intervención de una comunicación electrónica puede ser llevada a cabo invocando normativa que permite la intervención de comunicaciones telefónicas o "cualquier otro medio de comunicación del imputado" para impedirlas o conocerlas; o si es correcto asimilar el conocimiento del contenido de correos electrónicos a la interceptación e correspondencia; o si pueden ser aplicadas a la obtención de evidencia digital las disposiciones procesales atinentes a la regulación de allanamientos, secuestros y requisas[13].

En general, puede presumirse que la aplicación de estas normativas por vía analógica puede llevar muchas veces a soluciones que no son apropiadas. En ese sentido, al no existir reglas claras pueden darse tanto supuestos de enormes invasiones a derechos individuales y en otros se puede decidir cerrar investigaciones legítimas en sustento a una idea de privacidad cuya definición quedó desactualizada.

Bajo el principio de la libertad probatoria y la falta de regulación se puede ver el peligro de avasallar garantías individuales, sobre todo vinculadas a la intimidad y privacidad. Por todo ello se vuelve necesaria una regulación procesal específica para la obtención de evidencia digital, en función de las nuevas prácticas en ese ámbito y sobre todo teniendo en consideración los respectivos estándares de sospecha requeridos para cada medida.

3. 1. Un caso como ejemplo

Me pareció interesante traer un ejemplo para ver más claramente lo antes expuesto[14]. En el caso de un robo a un banco –en la forma "normal" en la que nos lo figuramos-, una persona ingresa al edificio burlando los dispositivos de seguridad, ingresa a la bóveda y retira el dinero. Una variante posible sería robar en la caja previo a amenazar al cajero. En esos casos, la investigación a cargo de la policía va a consistir primeramente

[13] Otra vez cito como ejemplo las disposiciones del Código Procesal Penal de la Nación, de Argentina, específicamente sus arts. 236 (sobre intervención de comunicaciones); art. 234 (interceptación de correspondencia); y art. 224 a 231 (regulación de allanamientos, secuestros y requisas). Este código de procedimiento no prevé una actualización acorde a la era digital, lo cual supone problemas en lo que respecta a la aplicación analógica de normas en la obtención de evidencia digital.

[14] El caso fue obtenido del texto de KERR, Orin*, Digital Evidence And The New Criminal Procedure*, The George Washington University Law School, 105 Columbia Law Review 279 (2005), GWU Law School Public Law Research Paper n° 108: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=594101

en la búsqueda de testigos que den cuenta del hecho tal como lo vieron a través de sus sentidos. También pueden concurrir al lugar del hecho para obtener elementos de prueba que sirvan para reconstruir lo ocurrido. Finalmente la evidencia recabada será producida en juicio.

Ahora, si cambiamos el caso a una versión "digital" veremos diferencias sustanciales. En vez de ir a robar, la maniobra delictiva se podría perfeccionar a través de una computadora o de cualquier dispositivo digital. El delincuente ingresará a la web desde el lugar que decida, pudiendo hacer maniobras para acceder a otras computadoras con pocos dispositivos de seguridad, para usar sus servidores. Supongamos que da con las claves necesarias e ingresa al sistema del banco, generando su propia cuenta bancaria, asignándole un monto y re-direccionándolo a una cuenta off-shore.

Siguiendo con el ejemplo podría suponerse que un empleado del banco advierte lo ocurrido y hace la denuncia a la policía. Lo cierto es que aquí la forma de obtener la evidencia es sustancialmente diferente: no hay testigos, no hay evidencia tangible. Los técnicos en informática pueden reconstruir lo ocurrido, por medio de la dirección IP podrían rastrear los datos y movimientos hasta dar eventualmente con el sospechoso.

A la hora de recabar la información, se podría pedir a cada uno de los servidores que informen los respectivos pasos de esta persona en la web. Sin embargo, es muy posible que se corte la cadena de información en algún momento, porque los servidores pudieron no haber guardado los datos. Otra opción posible es que el banco esté atento a nuevos ataques: si intentan ingresar de vuelta al sistema podrían verificar si fue esa persona, para lo cual pueden instalar un sistema de monitoreo.

De cualquier forma que se pueda llegar a la persona, para vincular a ese sujeto con el hecho deben ingresar a su computadora personal, lo que implica llevar el aparato a un perito informático. Ello conlleva a su vez concretas particularidades, tratándose de medidas que llevan su tiempo y en virtud de que se puede encontrar muchísima más evidencia que la inicialmente buscada, y que puede incriminarlo.

También podría sustituirse el registro y el secuestro por la utilización de un software "a distancia" o "de acceso remoto a datos"[15] para acceder a la computadora del sospechoso, que permita interceptar en tiempo real y grabar datos transmitidos o recibidos a través de diferentes medios, así como obtener datos de archivos almacenados en la memoria de los equipos investigados.

[15] Ver: DUPUY, Daniela, *Desafíos procesales en la investigación de delitos informáticos*, publicado en SAIJ en agosto de 2014.

3. 2. Las fallas en la aplicación de las reglas de procedimiento existentes

En los términos expuestos, ¿se podría decir que el procedimiento descripto en el punto anterior puede afectar al debido proceso y a la garantía de no autoincriminación? ¿Podríamos hablar de supuestos de abuso al principio de libertad probatoria?

En primer lugar tanto el hecho de pedir información a los servidores como instalar dispositivos para captar nuevas posibles maniobras, puede implicar una afectación a la privacidad, porque al obtener esos datos se puede tener mucha más información de la persona que lo que "normalmente" se detalla de forma estricta en una orden de allanamiento o registro.

A su vez, se observa la particularidad de que interviene un tercero: el proveedor de servicios de internet. Ello difiere de los casos donde está involucrada evidencia física, ya que rara vez un imputado le entrega evidencia clave a un tercero.

En general las órdenes de registro y allanamiento que conocemos se sustentan en la división de lo que presumiblemente se entiende como la esfera de lo público o lo privado. El punto es que ello, en este nuevo contexto, parecería que se desdibuja: por un lado, si se permite acceder a la información sin mayores restricciones se afecta a la intimidad, pero –por otro- si se prohíbe, se corre el riesgo de que "caigan" las investigaciones.

En el caso de peritajes también nos encontramos frente a problemas similares. El ingreso a una computadora implica tener una orden de registro; sin embargo, puede ser difícil determinar cómo se limita lo que la policía puede hacer, porque el análisis de los archivos implica quizás revisar algunos que son inocuos. La afectación también está dada desde que los peritos intervinientes podrían copiar los archivos y continuar con la investigación sin un lapso temporal definido.

3. 3. Otras posibilidades en la normativa procedimental

En este punto me parece interesante citar la Convención de Budapest sobre Cibercrimen, en lo que respecta a la recolección de evidencia digital, en virtud de establecer estándares legislativos en ese sentido. Así, en su artículo 14, la Convención prevé que los Estados firmantes adopten las medidas pertinentes para instaurar procedimientos que la misma convención prevé a los efectos de investigaciones penales, y que tienen diferentes tipos de injerencia: la conservación de los datos informáticos (quick freeze)[16], la divulgación y comunicación de datos informáticos y personales, el registro y decomiso de datos almacenados y la recogida en tiempo real e interceptación de datos (ver arts. 16 a 21).

De esta forma, a partir del caso descripto como ejemplo, y de lo indicado en el párrafo precedente, quizás podrían pensarse los procedimientos desde otro foco. Es que,

[16] No regulado en el ordenamiento procesal argentino, por ejemplo, sin perjuicio de que a través de maneras informales de cooperación se puede pedir la conservación de información, a través de canales como la Red 24/7 o los protocolos de empresas.

siguiendo las disposiciones de la mentada Convención de Budapest, no puede soslayarse que su art. 15 prevé un contenido garantista, remitiendo a pactos internacionales de derechos humanos como límite a la actividad del Estado.

Con esto me refiero a la utilización de la tecnología en lo que respecta a la investigación criminal aunque sin avasallar garantías constitucionales. Solo para mencionar un ejemplo, es una delgada línea la que justifica intromisiones en lo referente a cuestiones de seguridad o terrorismo, esgrimidos como excusa para violaciones masivas a la intimidad de un gran número de personas ante un eventual ataque de una soberanía estatal.

Concretamente en lo que respecta a la obtención de evidencia, por ejemplo, la requisa de dispositivos informáticos podría extenderse hasta donde se hubiere determinado la orden de registro, la cual deberá prever en forma específica qué elementos se obtendrán en función de lo que motiva esa búsqueda y los que deberán ser establecidos en forma previa.

Así, cabe referir que existen diferencias sustanciales entre la evidencia física y la digital en este punto. Ésta última, dada su naturaleza no corpórea, no es observable por los sentidos, sino mediante la utilización de medios técnicos. En ese contexto ningún hallazgo será casual, ni producto de la aplicación simple de los sentidos y solo puede tener lugar al requisar la totalidad de los datos de un dispositivo[17]. Ello necesariamente nos lleva a indagar más a fondo una de las maneras en que se inician investigaciones, a través de la denominada doctrina del hallazgo casual o la "Plain View Doctrine".

Concretamente en estos casos, las diferencias son claras: si se efectúa un registro en un ámbito físico, una vez revisado todo el espacio uno va a terminar encontrando sólo lo que se halla efectivamente en ese lugar y en ese momento. En cambio, si se realiza un registro sobre un dispositivo electrónico se tendrá acceso a toda la información que se encuentra guardada digitalmente en ese momento y también años atrás, lo que descargó otro usuario, lo que se intentó eliminar y se guardó en la papelera de reciclaje; solo para citar ejemplos.

De esta forma se observa claramente que los datos obtenidos como consecuencia de un registro digital no pueden ser regulados de la misma forma que los de un registro físico; debiéndose ponderar en el caso la protección de garantías, por un lado, y la eficiencia de las investigaciones, por otro.

La normal distinción de la expectativa de privacidad quizás pueda reconfigurarse en algunos supuestos, ya que el carácter público o privado no serviría para justificar mayores o menores injerencias, según cada caso. Ante el indudable caudal de información que se puede obtener de una persona solo a partir del acceso a un dispositivo electrónico, podría pensarse en seleccionar categorías diversas que habiliten procedimientos diferentes para la obtención de información.

[17] PETRONE, Daniel, *La prueba informática*, Ediciones Didot, Buenos Aires, 2014, págs. 64 y sgtes.

Por ejemplo, si consideramos que los correos electrónicos tienen material más privado que las búsquedas de internet de usuarios que quedan registradas en los motores de búsqueda, habrá diferentes lineamientos en la obtención y manejo de uno u otro grupo de evidencia digital. Los límites se pueden sustentar también en otras categorías: en métodos tales como la intención del investigador, el uso de herramientas de búsqueda digital, por el tipo de crimen, límites basados en el acusado, o criterios de proporcionalidad sobre la base de las escalas penales requeridas para los delitos[18].

En esta línea, también los peritajes informáticos necesitan ser sometidos a una nueva reglamentación, sobre todo tendiente a limitar búsquedas a tiempos más reducidos de realización. Quizás sería interesante proponer que se establezca en primer término de qué manera y qué método se utilizará para definir el análisis de datos, siendo quizás necesario que el juez interviniente pre-apruebe el método para ver si se ajusta a la normativa constitucional. Para ello podría promoverse la confección de protocolos de actuación, para seguridad de la cadena de custodia de los dispositivos y preservación de la evidencia digital.

4. INSTRUMENTOS DE COOPERACIÓN

Sobre la base de lo que se expuso previamente, es indudable la necesidad de redefinir y afianzar la cooperación a nivel internacional en lo que respecta a la investigación de delitos que involucren la necesidad de obtención de evidencias digitales en jurisdicciones diferentes a las de la autoridad que asume la investigación, que no involucra solamente a autoridades estatales, sino también a empresas multinacionales del sector de telecomunicaciones e informática.

En este contexto es interesante remarcar que las normas necesarias para una cooperación internacional eficiente van a ser un "espejo" de las normas procesales[19].

A **nivel regional**, con relación a los Estados parte y asociados del Mercosur, cabe mencionar que al momento coexisten en la región y en materia de asistencia penal diferentes documentos que vinculan recíprocamente a los Estados, con aplicación de procedimientos de asistencia judicial mutua[20]. No existe una legislación armónica sobre

[18] PETRONE, Daniel *La prueba informática*, Ediciones Didot, Buenos Aires, 2014, págs. 69-70.

[19] SALT, Marcos. *La relación entre la persecución de delitos informáticos y el Derecho Penal Internacional*, publicado en SAIJ en agosto de 2014.

[20] En el marco interamericano: el Tratado de Derecho Penal Internacional de Montevideo (1889); El Código Bustamante de Derecho Internacional Privado (1928); la Convención Interamericana de Nassau sobre Asistencia Jurídica Mutua en Asuntos Penales; en el ámbito del MERCOSUR y sus Estados Asociados: el Protocolo de San Luis de Asistencia Jurídica Mutua en Asuntos Penales entre los Estados Parte del MERCOSUR (1996); el Acuerdo de Asistencia Jurídica Mutua en Asuntos Penales entre los Estados Parte del MERCOSUR, Bolivia y Chile (2001); los Acuerdos Complementarios al Protocolo de San Luis y al Acuerdo de Asistencia Jurídica Mutua en Asuntos Penales con Bolivia y Chile -formularios de facilitación de la asistencia- (2001); c) instrumentos interministeriales específicos de cooperación en la materia; el Acuerdo RMI N°05/03 de Complementación del Plan General de Seguridad Regional en materia de Piratería entre los Estados Parte del

esta clase de delitos ni criterios unívocos sobre jurisdicción, aunque sí hay foros que operan como guías y manuales de buenas prácticas y redes[21].

En lo que respecta al **ámbito internacional**, resulta interesante hacer mención a las reglas de cooperación internacional de la Convención de Budapest –actualmente el convenio de más relevancia en la materia- que están construidas acertadamente como espejo de las medidas procesales, previendo su necesidad de obtención mediante la cooperación internacional. Con ello me refiero a que, si se necesita asegurar, obtener, secuestrar o registrar datos necesitaré a su vez normas procesales para realizar esas medidas en el ámbito nacional, pero también precisaré una norma de cooperación que prevea esa misma posibilidad con datos alojados en servidores en el extranjero.

El convenio establece una serie de medidas procesales que deben ser adoptadas por los Estados, relativas a pruebas informáticas: por ejemplo, la conservación inmediata de datos informáticos almacenados (art. 16); la conservación y divulgación inmediata de los datos de tráfico (art. 17); el mandato de comunicación (art. 18); el registro y decomiso de datos informáticos almacenados (art. 19); la recogida en tiempo real de datos informáticos (art. 20) y la interceptación de datos relativos al contenido (art. 21).

También propone la puesta en funcionamiento de una red de contacto entre agencias de prevención del delito para mejorar la obtención de estas pruebas –Red 24/7 de asistencia inmediata a investigaciones-. Sobre este punto, el convenio establece en su art. 35 que las partes designarán un punto de contacto localizable las 24 horas al día, y los siete días de la semana, con el fin de asegurar la asistencia inmediata en la investigación de infracciones penales llevada a cabo a través de sistemas y datos informáticos o en la recogida de pruebas electrónicas de una infracción penal. Esta asistencia comprenderá el facilitar la aportación de consejos técnicos, la conservación de datos (arts. 29 y 30) y la recogida de pruebas, aportes de información de carácter jurídico y la localización de sospechosos.

En su tercera parte, se refiere a la cooperación internacional, analizando los principios generales que habrán de aplicarse (art. 23), los principios relativos a la extradición (art. 24) y lo vinculado a la colaboración (arts. 25 a 35). En ese sentido, el objetivo es facilitar y acelerar el proceso de asistencia mutua, para lo cual se promueve una colaboración amplia y veloz, habilitándose, en casos de emergencia, la realización de

MERCOSUR (2003); el Acuerdo Mercosur/RMI/N°06/03 de Complementación del Plan General de Seguridad Regional en Materia de Piratería entre los Estados parte del Mercosur, Bolivia y Chile (2003); el Acuerdo Mercosur/RMI/ Operacional sobre la Implementación de Acciones en la Lucha contra la Piratería (2004); Convenios bilaterales y normativa nacional de cooperación penal: los Convenios o Tratados Bilaterales Sobre Asistencia Mutua en Materia Penal vigentes entre los Estados; la legislación Nacional Interna de Cada País Sobre Procedimientos de Asistencia Judicial Mutua en Materia Penal; ello citado en CERDEIRA, J. J., *Una aproximación a la Cooperación Regional en materia de ciberdelito*, publicado en Sistema Argentino de Información Jurídica (SAIJ), 2011.

[21] Como la Red Iberoamericana de Cooperación Jurídica (Iber Red) que comprende los Ministerios de Justicia, a los Ministerios Públicos y Poderes Judiciales de los estados de la región y el Grupo de Asistencia Jurídica en materia penal de la OEA.

pedidos por medios no formales y expeditivos, sobre todo teniendo en cuenta la volatilidad de los datos informáticos.

De esta forma, se promueve la cooperación en materia de medidas cautelares, como ser la conservación inmediata de datos informáticos almacenados (art. 29); la comunicación inmediata de los datos informáticos conservados (art. 30); la asistencia concerniente al acceso a datos informáticos almacenados (art. 31) y la asistencia para la recogida en tiempo real de datos de tráfico (art. 33).

Sin embargo, más allá de lo expuesto, los tratados multilaterales y bilaterales de asistencia en materia penal no siempre resuelven los problemas que plantea la evidencia digital y hasta en algunos puntos el Convenio de Budapest no da respuestas satisfactorias en lo referente a los problemas prácticos que genera el acceso transfronterizo de datos[22].

4. 1. Qué sucede con los territorios, soberanías y jurisdicciones a la hora de cooperar

Así como en otro apartado del trabajo, me pareció interesante analizar el tema partiendo de supuestos posibles[23]. Volviendo al ejemplo utilizado más arriba -del robo al banco a través de una computadora-, supongamos que las autoridades que llevan a cabo la investigación puedan tener acceso directo a la información, pero resulta que los datos son de acceso restringido y se encuentran alojados en un servidor en extraña jurisdicción[24].

Sobre este ejemplo cabe poner de resalto que no se toman los supuestos de acceso directo (libre) a sitios públicos, previstos en el inciso a) del art. 32 de la Convención de Budapest, que trata el acceso transfronterizo de datos informáticos almacenados. Esa posibilidad no plantea problemas porque esa información no formaría parte de la esfera de la privacidad, por lo que no se necesita autorización judicial para su consulta.

Ahora bien, en el caso mencionado: ¿se podría registrar y secuestrar la información sin recurrir a mecanismos de cooperación que vinculen a los países, en caso de que la información sea accesible desde la terminal que se encuentra en el lugar para el cual el juez ordenó el allanamiento? Para obtener la clave, ¿puedo utilizar técnicas o colocar programas especiales que introducidos en la computadora graben las contraseñas? Si se entiende que no corresponde secuestrar dicha información, ¿puede entenderse válido proceder al copiado de la información sin removerla ni alterarla?

En estos casos de acceso directo, en general, si no se requiere destrabar datos, los operadores intervinientes podrían copiar la información que la orden de allanamiento

[22] Estas cuestiones, por ejemplo, no se encuentran legisladas en el caso argentino.
[23] Para estos casos tuve en cuenta el texto de SALT, Marcos, *Nuevos Desafíos de la evidencia digital. El Acceso trasfronterizo de datos en los países de América Latina*, disponible en la web; también citado por PETRONE, Daniel, *La prueba informática*, Ediciones Didot, Buenos Aires, 2014, págs. 71/2.
[24] En ese sentido, ver PALAZZI, Pablo, *Los delitos informáticos en el Código Penal*, Ed. Abeledo Perrot, 2° Edición, Buenos Aires, 2012.

prevé. Inclusive podría ser posible que para la obtención de ese material se hubiere ingresado en algún servidor extranjero –sobre todo teniendo en cuenta la tendencia de alojar información en la nube (cloud computing)-, situación que podría no ser informada al juez ni de lo cual podría quedar constancia en el acta. Si ello sucediera, diríamos que prevalece aún la idea de que se ingresó a través de un aparato que estaba en el lugar físico alcanzado por la orden de allanamiento, pudiendo ser irrelevante -según ese criterio- si la información en realidad está alojada en un servidor en otro lugar. Diferente sería si el acceso a la información requiere romper claves de acceso. Ahora, en concreto, nos enfrentamos a este panorama: todas estas opciones podrían vulnerar los principios tradicionales de territorialidad o soberanía estatal.

En el marco de situación actual, las fronteras físicas siguen actuando como límite a la determinación de competencia e intervención de las autoridades judiciales[25]. En la legislación penal de la región rige en general el principio de aplicación territorial de la ley penal sustantiva[26], que resulta ineficaz para solucionar los problemas que plantea el acceso transfronterizo de datos y la obtención de prueba en la nube.

Por otro lado, en el caso de la ley procesal penal no se aplica el principio de territorialidad de la misma forma. Podría decirse que los convenios que prevén asistencia jurídica mutua en materia penal, tienden a respetar las soberanías estatales, aunque intentan instaurar sistemas más ágiles de cooperación[27].

A modo de ejemplo, se puede citar la Convención Interamericana sobre Asistencia Mutua en Materia Penal, la Convención de las Naciones Unidas contra la Corrupción y el Acuerdo de Asistencia Jurídica Mutua en Asuntos Penales del Mercosur, los cuales en general sustentan criterios generales de desformalización y mayor agilidad en las solicitudes de asistencia jurídica recíproca en investigaciones penales; aunque sin facultar a un Estado para ejercer funciones jurisdiccionales en el territorio de otro Estado, salvo excepciones.

[25] Una vez más traigo como ejemplo al caso argentino: ello también se aplica a su derecho interno, por su organización de tipo federal, para lo cual se recurre a la cooperación interprovincial para poder actuar fuera de sus respectivos territorios. Por ley 22.172, que establece el convenio de comunicación entre tribunales de la República, en el art. 2° se determina que la ley del lugar del tribunal al que se remite el oficio rige su tramitación; pero se puede aplicar, a pedido del exhortante, la ley procesal de éste último, determinando expresamente la forma de practicar la diligencia. En una excepción de estas características, el juez aplicará una ley extraña que no procede del poder soberano que lo invistió.

[26] En el caso del Código Penal argentino, el artículo 1º establece que la ley argentina se aplica a los delitos cometidos en el territorio argentino y a aquéllos cuyos efectos deban producirse allí. La ley penal, en general, es de aplicación territorial.

[27] Por ejemplo, la Convención Interamericana sobre Asistencia Mutua en Materia Penal, la Convención de las Naciones Unidas contra la Corrupción y el Acuerdo de Asistencia Jurídica Mutua en Asuntos Penales del Mercosur, en general sustentan criterios generales de desformalización y mayor agilidad en las solicitudes de asistencia jurídica recíproca en investigaciones penales, pero no se faculta a un Estado parte ejercer funciones jurisdiccionales en el territorio de otro Estado, salvo excepciones.

Si bien los supuestos pueden variar según el convenio de cooperación que rija entre los países, podrían aplicarse extraterritorialmente las normas procesales para la realización de las medidas de cooperación que se solicitan en otra jurisdicción, ello siempre y cuando vayan a ser materializadas por la autoridad requirente.

Para citar un ejemplo, cabe referir que un juez a quien se le permite tomar un testimonio en el extranjero, se rige por su propia ley procesal; es decir en general aplica la ley correspondiente al poder soberano que lo invistió, cualquiera que sea el territorio donde cumple el acto, salvo la existencia de una excepción especialmente regulada.

De esta forma, en general, si las evidencias deben ser obtenidas en un país extranjero, se deberá requerir colaboración mediante los convenios de asistencia mutua. Sin embargo, si tomamos como base el ejemplo dado más arriba, no resulta tan claro si se trata de evidencia que debe ser obtenida en el extranjero o si es posible interpretar que al no requerir la presencia física de las autoridades de un país en otro, sino sólo de su actuación a través de medios digitales, si ello puede constituir un caso de producción de prueba en extrañas jurisdicciones[28]. Como puede observarse, no es clara cuál es la ley procesal aplicable.

4. 2. La cooperación del sector privado

Otros casos implican la necesidad de obtener la información a través de empresas del sector privado, lo cual modifica también la forma habitual de pensar la cooperación en la investigación y determinación de delitos.

Supongamos, por ejemplo, que en una investigación es necesario acceder a la información contenida en una cuenta de correo electrónico o a documentos contenidos en servicio de alojamiento de datos, respecto de lo cual no se tiene acceso si no se requiere colaboración[29].

En estos supuestos, ¿es necesario realizar el pedido a través de exhorto o es válido pedir la información a la oficina comercial de la empresa en el país que investiga? En esa línea, ¿se puede pedir la información directamente a la sucursal de la empresa donde está la información? ¿Y si no fuera posible conocer en qué país está alojada la información porque cambia de servidor continuamente?

La particularidad de la solicitud de cooperación a privados es que en general son las empresas las que proponen su protocolo de actuación, definido de forma unilateral y que no necesariamente aplican de manera similar en todos los países. Ello puede suponer un riesgo no sólo para la eficiencia en investigaciones sino también para la protección de los

[28] SALT, Marcos, *Nuevos Desafíos de la evidencia digital. El Acceso trasfronterizo de datos en los países de América Latina*.
[29] Estos también son supuestos previstos en el art. 32 "b" de la Convención de Budapest.

datos personales que quedan sujetos a normas poco claras y cambiantes, desconocidas en muchas ocasiones por los usuarios[30].

Por la creciente tendencia de alojar contenidos en la nube, a veces se genera que no se pueda determinar en qué país está alojado el servidor que contiene la información o evidencia digital necesaria para la investigación. Pese a ello se observa que las empresas, a través de sus protocolos, pueden brindar ayuda transnacional independientemente de la ubicación de los servidores. Todo ello modifica necesariamente nuestras ideas básicas de cooperación entre Estados, en pos de la agilidad que se necesita en esta clase de investigaciones.

En todo este contexto, es de suma importancia la existencia de los canales informales tanto para preservar evidencia como para efectuar pedidos de información de contenido. Por ejemplo se puede hace referencias a la ya mencionada Red 24/7 o la Law Enforcement Online Request System de Facebook, solo para mencionar algunos ejemplos, y sin perjuicio de la necesidad de paralelamente efectuar el trámite diplomático vía exhorto o bajo las formalidades que requiera el caso.

Ahora bien, más allá de lo expuesto veamos el supuesto de colaboración previsto en el art. 32 del Convenio de Budapest[31], en cuanto al acceso a datos ubicados fuera del territorio por medios informáticos con el consentimiento de quien tiene la autoridad legal para revelar esa información. Este caso conlleva problemas operativos, si nos preguntamos quién sería el autorizado en cada caso.

Ello además puede traer aparejados conflictos para el derecho de las personas cuyos datos son revelados por una empresa del sector privado sin poder ejercer su defensa conforme a las leyes del Estado del lugar donde el servidor está alojado, ni acceder a la justicia de ese Estado para defender sus datos[32].

Tampoco el artículo citado da una respuesta adecuada a los problemas que en la práctica genera el acceso transfronterizo de datos, en los casos en que la información está alojada en una nube.

---

[30] SALT, Marcos, *Nuevos Desafíos de la evidencia digital. El Acceso trasfronterizo de datos en los países de América Latina*.

[31] El que se transcribe para mayor ilustración a continuación: *"Artículo 32. Acceso transfronterizo de datos almacenados, con consentimiento o cuando sean accesibles al público. Una parte podrá, sin autorización de otra: a. tener acceso a datos informáticos almacenados accesibles al público (fuente abierta), independientemente de la ubicación geográfica de los mismos; o b. tener acceso a datos informáticos almacenados en otro Estado, o recibirlos, a través de un sistema informático situado en su territorio, si dicha Parte obtiene el consentimiento lícito y voluntario de la persona legalmente autorizada a revelárselos por medio de ese sistema informático".*

[32] SALT, Marcos, *Nuevos Desafíos de la evidencia digital. El Acceso trasfronterizo de datos en los países de América Latina*.

5. Consideraciones finales

De lo aquí expuesto, y teniendo en cuenta la tendencia a un mayor uso tecnológico, que inevitablemente generará un avance en la evidencia digital involucrada en casos penales de todo tipo y, por ende, a una mayor cooperación entre Estados, se pueden extraer algunas conclusiones preliminares:

*En lo que respecta a reglas procesales de obtención de evidencia digital pueden darse cambios en la interpretación normativa pero es necesaria una regulación específica a través de acciones concretas de los poderes legislativo y ejecutivo de los Estados.

*Tanto la nueva normativa como las interpretaciones que hagan los jueces, siempre tendientes a ponderar entre los valores de seguridad y privacidad, debería hacerse a la luz de principios constitucionales y del reconocimiento de las garantías individuales.

*Un principio posible que puede tenerse en cuenta, a la hora de disponer órdenes de allanamiento, requisas o intervenciones o al disponer peritajes informáticos es la de tender a promover la determinación previa de qué elementos motivan la orden, en función del delito que se investiga y una mayor restricción en cuanto a tiempos para su análisis, siempre en miras a limitar la posible afectación de derechos.

*En ese sentido, sería bueno establecer estándares de protección de derechos, ver qué límites establecemos a la hora de ingresar en el espacio privado de una persona y acorde a criterios sobre qué prerrogativas están en juego según el tipo de evidencia y el tipo de delito investigado.

*La armonización de las legislaciones nacionales como correlato del establecimiento de normas a nivel regional y global. Esta armonización, vinculada al espacio virtual, debería ser tanto de índole sustantiva y procesal, así como de aplicación de criterios de jurisdicción, y de fortalecimiento de la cooperación jurídica. Ello tiene su fundamento es que la naturaleza global de internet requiere de una regulación de ese mismo tipo.

*En este esquema, resulta necesario gestionar la regulación de la cooperación entre el sector público y sector privado, promoviendo institucionalmente convenios de cooperación con el sector privado a los fines del cumplimiento eficiente de los requerimientos de la justicia; en donde conste en forma clara los alcances de la cooperación, tratando de brindar una mayor seguridad jurídica a los usuarios, por el uso de su información.

*Necesidad de regular en forma clara, a nivel civil y penal la responsabilidad que les cabe a los proveedores de internet. En ese sentido resultaría interesante la fijación de estándares precisos vinculados a la forma en la que los diferentes actores de internet puedan ser responsabilizados por el contenido de la información que circula en la red.

Sobre este punto se han citado a lo largo de este trabajo diferentes supuestos de responsabilidad por criminalidad informática de proveedores de internet, que podría proceder, a modo de ejemplo, en los siguientes casos: por pérdida o manipulación incorrecta de información; por falta de protección de la información de parte de los

proveedores; por alcance del deber de protección de la información; siempre debiéndose observar particularidades de cada responsabilidad según el tipo de proveedor de servicios[33].

*A nivel interno de cada Estado, surge la necesidad de elaborar protocolos de actuación para la labor entre distintas fuerzas de seguridad y las autoridades a cargo de las investigaciones.

BIBLIOGRAFÍA

CERDEIRA, J. J., *Una aproximación a la Cooperación Regional en materia de ciberdelito*, publicado en Sistema Argentino de Información Jurídica (SAIJ), 2011

CHERÑAVSKY, Nora, *Responsabilidad penal de los proveedores de servicios de internet*, publicado en Sistema Argentino de Información Jurídica (SAIJ) en agosto de 2014

DUPUY, Daniela, *Desafíos procesales en la investigación de delitos informáticos*, publicado en SAIJ en agosto de 2014

KERR, Orin, *Digital Evidence And The New Criminal Procedure*, The George Washington University Law School, 105 Columbia Law Review 279 (2005), GWU Law School Public Law Research Paper n° 108: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=594101

KURBALIJA, Jovan y GELBSTEIN, Eduardo, *Gobernanza de internet. Asuntos, actores y brechas*, publicado por DIPLO Foundation, 2005

LESSIG, Lawrence, *The code version 2.0*, Cambridge, Basic Books, 2006.

PALAZZI, Pablo, *Los delitos informáticos en el Código Penal*, Ed. Abeledo Perrot, 2° Edición, Buenos Aires, 2012

PETRONE, Daniel, *La prueba informática*, Ediciones Didot, Buenos Aires, 2014

SALT, Marcos. *La relación entre la persecución de delitos informáticos y el Derecho Penal Internacional*, publicado en SAIJ en agosto de 2014

SALT, Marcos, *Nuevos Desafíos de la evidencia digital. El Acceso trasfronterizo de datos en los países de América Latina,* disponible en la web

UNESCO, *Fostering Freedom online: the role of internet intermediaries*, año 2014, disponible en: http://unesdoc.unesco.org/images/0023/002311/231162e.pdf

CORTÉS CASTILLO, Carlos; investigador de la iniciativa por la Libertad de Expresión en Internet (iLEI), del Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE) de la Facultad de Derecho de la Universidad de Palermo. *Las llaves del ama de llaves:*

[33] En ese sentido, ver CHERÑAVSKY, Nora, *Responsabilidad penal de los proveedores de servicios de internet*, publicado en Sistema Argentino de Información Jurídica (SAIJ) en agosto de 2014.

la estrategia de los intermediarios en Internet y el impacto en el entorno digital, disponible en http://www.palermo.edu/cele/pdf/LasLlavesDelAmaDeLlaves.pdf

MELÉNDEZ JUARBE, H. A. "Intermediarios y Libertad de Expresión: Apuntes para una conversación", en *Hacia una Internet libre de censura. Propuestas para América Latina*, del Centro de Estudios en libertad de Expresión y Acceso a la Información, Universidad de Palermo, Buenos Aires (2012), disponible en http://www.palermo.edu/cele/pdf/internet_libre_de_censura_libro.pdf