LA EVIDENCIA DIGITAL EN EL PROCESO PENAL Y LA PRESERVACIÓN DE LOS DERECHOS FUNDAMENTALES

A EVIDENCIA DIGITAL NO PROCESSO PENAL E A PRESERVAÇÃO DOS DIREITOS FUNDAMENTAIS

LA EVIDENCIA DIGITAL EN EL PROCESO PENAL Y LA PRESERVACIÓN DE LOS DERECHOS FUNDAMENTALES[1]

A EVIDENCIA DIGITAL NO PROCESSO PENAL E A PRESERVAÇÃO DOS DIREITOS FUNDAMENTAIS

Fernando M. Rodrigo[2]

RESUMEN

Las nuevas tecnologías de la información y comunicación ("TIC"), han modificado nuestra cotidianidad. El individuo social ha perdido su anonimato comunicacional, para convertirse en fuente comunicacional registrable. De este modo, la constante comunicación del sujeto en la modernidad mediante estas herramientas permite claramente nuevos mecanismos de control estatal. La evidencia digital es la información o los datos que han sido almacenados o transmitidos en un formato digital o a través de un medio informático y que poseen valor probatorio. Consecuentemente, la manipulación y el examen de las pruebas electrónicas es una tarea que requiere particular cuidado en consideración a las características especiales de la evidencia digital, entre otras cosas porque esta clase de evidencia se puede reproducir y alterar fácilmente, en tanto es maleable, haciéndola vulnerable. A lo largo del presente trabajo se podrá identificar las diferencias que posee la evidencia digital con relación a la física y como consecuencia de ello, se analiza la problemática que genera la aplicación de la normativa hoy vigente a la evidencia digital y la incidencia que tiene la evidencia digital en los diferentes delitos y especialmente en los delitos informáticos. No existe duda alguna que los entornos digitales y los nuevos modos de comunicarse con los que se interactúan cada día y en los que se depositan y registran aspectos íntimos y privados de nuestro proyecto de vida, son ámbitos que merecen protección frente a la injerencia estatal.

1 Data de Recebimento: 03/03/2021. Data de Aceite: 07/06/2021.

2 Abogado (Facultad de Derecho de la Universidad Nacional de Rosario -U.N.R.-, República Argentina); exPresidente de la Asociación de Fiscales del Ministerio Público de la Acusación de la Provincia de Santa Fe, República Argentina (años 2014 a 2018); Magister en Derecho Procesal (Facultad de Derecho de la Universidad Nacional de Rosario -U.N.R.-, República Argentina); Candidato a Doctor en Derecho, Facultad de Derecho de la Universidad Nacional de Rosario -U.N.R.-, República Argentina); Mediador Penal (Ministerio de Justicia y Derechos Humanos de la Provincia de Santa Fe); Docente de la Facultad de Derecho de la Universidad Nacional de Rosario, República Argentina (cátedras de Introducción al Derecho y Derecho Penal I –Parte General-); exProfesor del Instituto de Seguridad Pública (I.Se.P.) –ex Escuela de Cadetes de Policías- de la Provincia de Santa Fe, República Argentina; Certificación Internacional en Ética y Compliance AAEC-IFCA; Miembro de la Asociación Internacional de Derecho Penal (AIDP); Miembro de la Asociación Argentina de Ética y Compliance (AAEC); E-mail: fernandorodrigo1@gmail.com

Palabras clave: Investigación. Evidencia digital. Internet. Ciencia y Tecnología. Derecho a la intimidad. Derechos Humanos. Delitos informáticos. Proceso Penal. Recolección de evidencia digital y evidencia física. Cooperación internacional.

1 INTRODUCCIÓN

Las nuevas tecnologías de la información y comunicación (en adelante, "TIC"[3]), han modificado nuestra cotidianidad: se utilizan smartphones para subir información a redes sociales, a la "nube"[4], para pagar las cuentas, etc. Con ello se dejan huellas digitales que quedan alojadas en registros disímiles que pueden ser evidencia digital en un proceso judicial.

El desarrollo de Internet conlleva beneficios indiscutibles, sin embargo, con ellos se produce la pugna de la modernidad tecnológica con el tradicional sistema de garantías constitucionales vigentes en nuestro país.

Así, el panorama se refleja en el creciente quebrantamiento de éstas y en el seguimiento de los individuos a raíz del almacenamiento de las visitas efectuadas en la navegación[5].

No debe olvidarse que en el origen el ciberespacio fue utilizado por John Perry Barlow en 1966 como rechazo a la intromisión de los Estados en la red[6]. Pero esta idea lejos quedó, puesto que los Estados comenzaron a ver en el ciberespacio una fuente de riesgos, y no sólo de riesgos, sino de datos, y en tanto éstos hacen al poder de la política estatal, se lo consideró una fuente de pruebas y de investigación de sujetos que no saben que están siendo observados en qué momento o bajo qué circunstancias: ¿panoptismo de la modernidad?

Es necesario dejar en claro que ante la mínima búsqueda o con la utilización de la herramienta más frecuente de comunicación, como es el correo electrónico, la red captura datos, que son atribuidos a ese perfil registrado o en su defecto al IP. Es decir que, aunque no se desee, la captación de los datos es parte de la arquitectura de internet[7] y

3 Las tecnologías de la información y la comunicación (TIC) son el conjunto de tecnologías que permiten el acceso, producción, tratamiento y comunicación de información presentada en diferentes códigos (ya sea como imagen, como sonido, en versión de texto, etc.). Su ejemplo más claro es "internet".

4 En inglés el término es cloud, que es la información que se almacena de manera permanente en servidores de internet que proporcionan dicho servicio (iCloud, Dropbox, OneDrive, Google Drive, entre otros).

5 FILLIA, SUEIRO, MONTELEONE, NAGER, ROSENDE, Análisis a "La reforma en materia de criminalidad informática al Código Penal de la Nación (ley 26.388)", en: Sup. Penal 2008 (agosto), 15, LL 2008-E-938; BADENI, Tratado de Derecho Constitucional, p. 564.

6 BARLOW, A Declaration of Independence of Cyberspace. Disponible en: https://projects.eff.org/~barlow/DeclarationFinal.html (consultada el 24/02/2021). También puede v. CORTÉS, Vigilancia de la red: ¿Qué significa monitorear y detectar contenidos en internet?, pp. 3 y ss., en: https://www.palermo.edu/cele/pdf/El-deseo-de-observar-la-red.pdf

7 Por ello puede entenderse que: 1.- El Principio de extremo a extremo (PEE) refiere a un diseño de redes de extremo, donde los datos se transportan hasta su destino. 2.- La conmutación de paquetes de datos complementa al PEE, agrupan-

ello hoy por hoy es inevitable para el usuario, que se ha convertido en "objeto registrable".

El individuo social ha perdido su anonimato comunicacional, para convertirse en fuente comunicacional registrable. Ya no comunica con palabras o escritura, sino con simples búsquedas.

De este modo, la constante comunicación del sujeto en la modernidad mediante estas herramientas permite claramente nuevos mecanismos de control estatal.

Las nuevas tecnologías constituyen un desafío para los conceptos jurídicos existentes y los procesos de investigación que se llevan adelante en los diferentes países.

2 LA EVIDENCIA EN EL PROCESO PENAL Y HECHOS QUE SE PRUEBAN

El objeto de prueba en el proceso penal está constituido por los hechos, pueden probarse hechos humanos individuales o sociales, estados de ánimo de los particulares, condiciones mentales de los individuos[8] y tantas otras situaciones que sirvan al esclarecimiento de lo sucedido y que es sometido al proceso penal.

El material fáctico es incierto en cuanto a su conocimiento[9], de tal modo, se pretenderán probar hechos externos (físicos) y hechos internos (síquicos), que son los que configuran la acción o conducta, los elementos objetivos y subjetivos del tipo, las causas de justificación, la imputabilidad o inimputabilidad y/o a culpabilidad o las causas de inculpabilidad de quien es sindicado por el hecho considerado encuadrable en un tipo penal.

En el esclarecimiento de los hechos juega un gran papel la labor e investigación intelectual, cuyo fin es el descubrimiento o esclarecimiento de lo sucedido, que puede definirse como la conformidad de las palabras, ideas, y las relaciones con la naturaleza y la realidad de los hechos y las cosas, a partir de lo probado y corroborado mediante pruebas introducidas legalmente en el proceso.

Tras lo expresado podría llegarse a la conclusión, un tanto precipitada, de que el proceso penal no es un medio adecuado para encontrar la verdad, y que de lo que en realidad se trata es del cumplimiento de ciertos ritos y fórmulas más que la búsqueda de la verdad misma. Como advierte Habermas, la búsqueda de la verdad en el discurso institucional tiene sus particularidades que la distinguen de la búsqueda de la verdad en el discurso libre de dominio, en el que precisamente por serlo, todas las partes están en

do los datos que se transmiten en la red, formada por un encabezado y una carga útil que permite el ensamble del dato. 3.- El modelo de interconexión de Sistemas abiertos: aquí el modelo de red está dividido en capas (MISA), estandariza la función, asignando funciones separadas.

8 FLORIÁN, De las pruebas penales, tomo I, p. 101.

9 JAUCHEN, Tratado de la prueba en materia penal, p. 21.

un plano de igualdad y tienen el mismo interés de encontrar la verdad[10].

En el proceso penal, la búsqueda de la verdad está limitada, entonces, por el respeto a las garantías que tienen incluso el carácter de derechos humanos reconocidos como tales en todos los textos constitucionales y leyes procesales de todos los países de nuestra cultura. Principios como el de proporcionalidad, dignidad[11] o el derecho a intimidad, entre otros.

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).

El avance tecnológico exige el acompañamiento del derecho penal y de las garantías, mediante una revisión integral de tales conceptos, los cuales deben ser amoldados a este nuevo paradigma social, para dar tutela efectiva y una respuesta satisfactoria.

3 QUÉ ES LA EVIDENCIA DIGITAL Y DÓNDE SE ENCUENTRA

Cuando se habla de delitos informáticos o aquellos cometidos utilizando directa o indirectamente un medio tecnológico, se pregunta inmediatamente por el tipo de prueba o evidencia que se puede utilizar para probarlos.

En informática forense, la evidencia digital es uno de los términos más destacados. El término evidencia digital de acuerdo con la ISO/IEC 27037:2012[12], se conoce como

10 *Cfr*. HABERMAS, *Teoría de la acción comunicativa: complementos y estudios previos*, pp. 113 y ss. Una exposición resumida de esta teoría puede verse en: HASSEMER, *Fundamentos del derecho penal*, pp. 163/8.

11 El principio de dignidad de la persona humana implica reconocer la personalidad jurídica de todos los seres humanos y el carácter de sujetos de derechos, con derechos y obligaciones. Ello tiene grandes consecuencias dentro del proceso penal, ya que significa reconocerle al imputado el carácter de sujeto de derecho, lo que exige que debe garantizarse su derecho de defensa y dentro de este el derecho de audiencia, de modo que pueda influir sobre el resultado final del proceso. Por otro lado, como consecuencia del principio de dignidad de la persona humana se debe garantizar el derecho de abstención de declarar, de modo que no puede ser compelido a aportar prueba en su contra. Ello lleva también a la proscripción de toda forma de tortura y malos tratos, careciendo de todo valor la declaración recibida en esta forma, lo mismo que la prueba que sea obtenida como consecuencia de dicha declaración. La tortura y los malos tratos constituyen violaciones extremas del principio de dignidad de la persona humana. El principio de dignidad de la persona humana lleva también al necesario respeto del principio de proporcionalidad en la actuación estatal.

12 Es una norma perteneciente a la familia de estándares ISO/IEC 27000 (estas normas son estándares de seguridad publicados por la Organización Internacional para la Estandarización -ISO- y la Comisión Electrotécnica Internacional -IEC-), la misma establece las "Directrices para identificación, recolección, adquisición y preservación de evidencia digital

"información o datos, almacenados o transmitidos de forma binaria que pueden ser tomados en cuenta como evidencia o prueba". La evidencia digital es la información o los datos que han sido almacenados o transmitidos en un formato digital o a través de un medio informático y que poseen valor probatorio[13]. Este último elemento -valor probatorio- estará dado por la normativa procesal de cada país que posibilita la utilización de la evidencia recolectada en un proceso judicial, siempre y cuando respete las pautas y principios establecidos.

La evidencia digital no es ni más ni menos que todo dato que esté almacenado o sea transmitido mediante la utilización de computadoras (en sentido amplio) que soporta o bien rechaza una teoría acerca de cómo ocurrió un delito o bien aborda los elementos críticos de este, como ser la intención (dolo) o su coartada. Pareciera, entonces, que la evidencia digital se asimila en gran medida a cualquier elemento de prueba susceptible de ser secuestrado en un procedimiento judicial.

Hoy en día, cualquier operador o investigador judicial o de las fuerzas de seguridad realiza investigaciones en fuentes abiertas (OSINT, por sus siglas en inglés, *open-source intelligence*), con el objetivo de obtener aquella información que está disponible en internet respecto de todos los seres humanos y la cual no requiere de ningún otro acto más que el colocar nombre y apellido de determinado sujeto en un buscador *online*. Ahora bien, la clave está en tratar de identificar cuándo es posible validar aquellos datos obtenidos a través de las TIC en una investigación penal preparatoria, para así incorporarlos y usarlos, por ejemplo, para probar la intención de un imputado o bien su inocencia[14].

En este sentido, evidencia digital no solo es una fotografía digital recopilada en un teléfono, sino que también lo son los resúmenes bancarios almacenados en un CD, archivos y documentos guardados en el disco rígido de una computadora (piénsese, verbigracia, un archivo de *Word*, una planilla *Excel*, una presentación en *Power Point*,

(*Guidelines for identification, collection, acquisition and preservation of digital evidence*)", por lo que proporciona guías para actividades específicas en el manejo de evidencia digital, dichas actividades hacen referencia a la identificación, recolección, preservación de evidencia digital potencial. Provee guías para: medios de almacenamiento usados en computadores estándares, dispositivos móviles, sistemas móviles de navegación, computadores estándares y conexiones de red, redes basadas en los protocolos TCP/IP y otros.

Además de dicha norma ISO, existen otras aplicables a la materia de evidencia digital, así se encuentra la ISO/IEC 27042 (2015), "Directrices para el análisis e interpretación de la evidencia digital", que provee guías en el análisis y la interpretación de la evidencia digital, de forma que se logre garantizar o abordar cuestiones de continuidad, validez, reproductibilidad y repetitividad. Contiene, además, buenas prácticas para la selección, diseño e implementación de un proceso analítico y recoger suficiente información que permita que dichos procesos puedan ser sometidos a escrutinios independientes cuando sea necesario. En resumen, este estándar provee un marco común, para lidiar con incidentes en sistemas de seguridad analizando e interpretando los elementos propios del incidente. El cual puede ser empleado para asistir a la implementación de nuevos métodos.

13 Definición del FBI: "*Digital Evidence: Information of probative value stored or transmitted in digital Form*", en: https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm (consultada el 24/02/2021)

14 ABDELCADER, *La evidencia digital en el proceso penal. A propósito del fallo mediante el que se condenó a Ricardo Russo, pediatra del Hospital Garrahan*.

audios, entre otros), o en un *pendrive*, o bien, datos registrados en un *Smart TV* (el historial de búsquedas en internet, listas de reproducción de *Youtube*, películas y series vistas en *Netflix*, entre otros)[15].

La ciencia que adquiere, preserva, recupera y presenta la evidencia digital se denomina informática forense[16].

Lo cierto es que día a día cada uno de los individuos genera más información[17] lo que puede convertirse en evidencia digital, fenómeno que se retroalimenta con las nuevas ofertas de dispositivos cada vez más compactos y cuyo almacenamiento es cada vez mayor (hoy en día es fácil acceder a un disco rígido externo de un Terabyte que cabe en la palma de la mano, capacidad que duplica, y muchas veces cuadriplica la contenida en un disco rígido de una Notebook). Estas conductas han originado lo que se conoce como *Big Data* que posibilita el *Data Mining*[18].

Lo anterior resulta muy importante si se considera que la manipulación y el examen de pruebas electrónicas es una tarea que requiere particular cuidado en consideración a las características especiales de la evidencia digital, entre otras cosas porque esta clase de evidencia se puede reproducir y alterar fácilmente, en tanto es maleable, haciéndola vulnerable, como también, en muchas ocasiones establecer la verdadera procedencia de los datos no firmados digitalmente es muy difícil para alguien sin el debido entrenamiento.

4 DIFERENCIAS ENTRE LA EVIDENCIA FÍSICA Y LA EVIDENCIA DIGITAL

La evidencia digital no tiene las mismas características que la evidencia física, presentando diferencias.

En primer término, la evidencia física es tangible, mientras que la digital no lo es (sí podrá serlo el soporte que la almacena pero no el dato en sí). Esta última es volátil, ya que es fácil modificarla, suprimirla, alterarla (ya sea para cambiar su formato, extensión o tamaño, por ejemplo). Por otro lado, el volumen también es distinto -lo que dificulta muchas veces la pertinente investigación-, anteriormente se señaló que el almacena-

15 PICCIRILLI, *Ausencia de regulación procesal penal aplicable a la evidencia digital y su correlación con los delitos informáticos. Legislación vigente, anteproyectos y convenio de Budapest*.

16 Definición del FBI: "*Computer forensic science is the science of acquiring, preserving, retrieving, and presenting data that has been processed electronically and stored on computer media*".

17 Sobre todo, si se compara, por ejemplo, la cantidad de fotografías físicas que guardamos en contraposición a las digitales, o los documentos físicos que almacena una oficina con relación a los archivos digitales que resguardan una PC o un disco rígido externo.

18 Mientras que *big data* es la acumulación de muchísimos datos, *data mining* es el fenómeno por el cual se utilizan herramientas que analizan grandes bases de datos con el objetivo de crear perfiles, patrones o tendencias. En este sentido ver: https://www.techopedia.com/7/29678/technology-trends/what-is-the-difference-between-big-data-and-data-mining

miento y producción de datos digitales crece exponencialmente en virtud de la existencia de dispositivos de mayor capacidad y generación de muchísima información, que antes era inconcebible (fotos digitales, perfiles en redes sociales, numerosos archivos almacenados en una PC, en la "nube", entre otros).

Asimismo, y como se expresó anteriormente, la evidencia digital puede ser alterada, por lo cual es necesario contar con herramientas de recolección más sofisticadas y personal experto -a diferencia de la evidencia física que puede tomarse simplemente-. En este sentido, cabe explicar que cuando un usuario elimina un archivo en una computadora, existe la posibilidad de recuperarlo[19], por lo que existen archivos que, aunque a primera vista estén "borrados" (y un simple usuario no pueda verlos), pueden ser recolectados mediante el empleo de técnicas forenses, lo que involucra una mayor complejidad.

En este mismo sentido, archivos que han sido alterados (por ejemplo, en su formato) o han sido ocultados, también pueden ser obtenidos mediante la utilización de herramientas forenses[20].

Por otro lado, las técnicas forenses permiten realizar una copia *bit a bit* o copia forense, que implica la creación de un duplicado íntegro de la información que se recolecta. Es decir que, en esa copia, mediante el empleo de herramientas que más adelante se explicarán, es posible obtener exactamente lo que hay, a guisa de ejemplo, en una computadora, incluyendo archivos que cualquier usuario puede ver, como así también los "borrados" que no están a simple vista.

A diferencia de la evidencia digital, con la evidencia física no es posible obtener este tipo de copias exactas, o "clonación"[21].

Como corolario de lo expuesto, cabe resaltar que la evidencia digital requiere del conocimiento de un experto con formación técnica especial, justamente por sus características de volatilidad, como también para recolectar archivos que a primera vista no se visualizan y sobre todo para comprender la información que se quiere recolectar ya que

19 Siempre y cuando el lugar en el cual se alojaba no se haya sobrescrito, es decir que con la utilización de herramientas forenses es posible recuperar archivos que se han borrado a simple vista, mientras que ese "lugar" no haya sido utilizado para alojar un nuevo archivo.

20 A modo de ejemplo el software EaseUS Data Recovery disponible en Internet para su descarga cuenta "(c)on una poderosa capacidad de recuperación de datos, este software profesional puede tratar con todos los casos de pérdida de datos, como recuperar archivos cifrados y comprimidos, formateados, recuperar datos infeccionados por virus, y soporta recuperar datos desde varios tipos de dispositivos de almacenamiento, todo este hace que sea el mejor para la recuperación de datos forense", (consultado el 24/02/2021 en el sitio web https://es.easeus.com/data-recovery-solution/best-forensic--data-recovery-software.html. Por otro lado, Disk Drill "es una herramienta de recuperación de datos probada que ha sido utilizada con éxito por innumerables usuarios en todo el mundo para recuperar documentos, imágenes, archivos de vídeo y otros tipos de datos de una variedad de dispositivos de almacenamiento diferentes" (consultado en fecha 24/02/2020), en https://hardzone.es/2017/08/22/recuperar-archivos-disco-duro-disk-drill/ y https://www.cleverfiles.com/howto/es/computer-forensic.html#:~:text=Disk%20Drill%20es%20una%20herramienta,de%20dispositivos%20de%20almacenamiento%20diferentes.

21 Para un mayor desarrollo sobre el tema puede v. SALT, Nuevos Desafíos de la evidencia digital: Acceso transfronterizo y técnicas de acceso remoto a datos informáticos.

"generalmente 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"[22].

5 LA IMPORTANCIA DE LA EVIDENCIA DIGITAL PARA PROCESO PENAL

Las leyes penales son de suma importancia, por cuanto afectan a la libertad, la honra y a la vida del hombre.

El proceso tiene por finalidad, no el estudio de la ley penal para su fiel interpretación y recta aplicación, sino que debe permitir la averiguación de los hechos, determinándolos con toda precisión y claridad; por donde se deja entrever y comprender hasta dónde llega la importancia de la confirmación procesal. Nunca puede prescindirse de ella.

No hace falta entonces, mayor imaginación para comprender la importancia de la prueba en la vida jurídica, en razón de que la convicción de culpabilidad necesaria para condenar debe derivar de los datos probatorios legalmente recolectados e incorporados al proceso, "son las pruebas, no los jueces, las que condenan, ésta es la garantía"[23]. La prueba, por ser insustituible como fundamento de una condena es la mayor garantía ante la arbitrariedad judicial que busca concretar el *ius puniendi*.

El derecho a la prueba es la posición jurídico-constitucional que posee el presente o futuro justiciable o litigante de exigirle al Estado o al órgano jurisdiccional el aseguramiento, la producción y valoración de los medios de prueba relevantes[24], con el que se busca sintetizar los contenidos de la prueba judicial, posee los siguientes componentes: **1)** es una garantía constitucional; **2)** tiene como destinatario cualquier persona que en el presente o en el futuro tenga el carácter de justiciable; **3)** obliga al Estado, en especial a sus órganos de justicia; **4)** reúne los medios probatorios relevantes o pertinentes; **5)** es suficientemente omnicomprensivo de la actividad probatoria. Se prioriza el enfoque jurídico de la persona, sobre el de la norma, la jurista francesa Aurélie Bergeaud[25] dice que el derecho a la prueba es ante todo un concepto, una manera de representar y de organizar las percepciones y los conocimientos.

22 SALT, Nuevos Desafios de la evidencia digital: Acceso transfronterizo y técnicas de acceso remoto a datos informáticos, p. 32.

23 CAFFERATA NORES, La Prueba en el Proceso Penal, con especial referencia a la Ley 23.984, p. 6.

24 En términos más concisos, Picó i Junoy define este derecho como el "que posee el litigante consistente en la utilización de los medios probatorios necesarios para formar la convicción del órgano jurisdiccional acerca de lo discutido en el proceso", en: PICÓ I JUNOY, El derecho a la prueba en el proceso civil, pp. 18/9. Por su parte, Taruffo define el derecho a la prueba desde su finalidad: "El derecho a la prueba puede ser definido como el derecho de las partes de influir sobre la determinación judicial de los hechos, por medio de todas las prueba relevantes, directas y contrarias de las que se dispone". Por ello, considera el autor que reconocer el derecho de las partes a aducir las pruebas y a que se practiquen se torna ilusoria y meramente ritualista, sino se garantiza el resultado probatorio, esto es la valoración de la prueba como parte del juicio en la sede de las decisiones, cfr. TARUFFO, "Il Diritto allá prova. nel processo civile", en: Rivista di Diritto Processuale XXXIX, p. 106.

25 BERGEAUD, Le droit à la preuve, p. 6.

Para comprender la incidencia que tiene la diferencia que se observa entre la evidencia digital y la física, con relación a las normas procesales vigentes cabe primero recordar el principio de libertad probatoria[26] que prima en el derecho penal y sus límites.

En este sentido, la prueba en el proceso penal puede entenderse como "todo lo que pueda servir para el descubrimiento de la verdad acerca de los hechos que (...) son investigados y respecto de los cuales se pretende actuar la ley sustantiva"[27]. Por otro lado, el medio de prueba refiere a

> las distintas maneras según las cuales quien interviene en el procedimiento penal puede obtener y conducir al procedimiento los conocimientos necesarios, ciertos o probables, acerca de la hipótesis a investigar y conocer (el testimonio, la peritación, los documentos) más las autorizaciones coercitivas que las leyes conceden para poder llevarlos a cabo[28].

La máxima de la libertad probatoria se define expresando que "en materia penal, todo hecho, circunstancia o elemento contenido en el objeto del procedimiento y, por tanto, importante para la decisión final, puede ser probado y lo puede ser por cualquier medio de prueba"[29], en otras palabras, este principio "se sustenta en el criterio de que todo se puede probar por cualquier medio; es decir, no requiere de un medio de prueba determinado, ya que todos son admisibles"[30]. La Corte Interamericana de Derechos Humanos ha señalado que los medios probatorios no deben ser ajenos a los avances tecnológicos dirigidos a facilitar la gestión eficiente y económica del proceso[31].

Ahora bien, la obtención de la evidencia debe ser legítima y por ello la normativa procesal establece pautas para que pueda ser utilizada en el proceso[32], a diferencia de la obtenida ilícitamente: "fruto del árbol envenenado".

En efecto, las medidas que pueden adoptarse legalmente para obtener y preservar

---

26 Este principio aparece en varios códigos procesales provinciales de la República Argentina, a guisa de ejemplo, art. 209 Código Procesal Penal (CPP) de la Provincia de Buenos Aires, art. 199 CPP de la Provincia de Chaco; art. 165 del CPP de Chubut, art. 192 CPP de Córdoba, art. 250 CPP de Entre Ríos, art. 205 CPP de Mendoza, art. 159 CPP de Santa Fe, entre otros. De los códigos procedimentales de Sudamérica, puede observarse el principio de libertad probatoria, por ejemplo, en el art. 171 del Código de Procedimiento Penal del Estado Plurinacional de Bolivia, art. 173 del Código Procesal Penal de la República del Paraguay, art. 198 del Código Orgánico Procesal Penal de la República Bolivariana de Venezuela, entre otros.

27 CAFFERATA NORES, La prueba en el proceso penal, p. 4.

28 MAIER, Derecho procesal penal. Parte General. Actos Procesales, Tomo III, p. 79.

29 MAIER, Derecho Procesal Penal, tomo I, p. 864.

30 ORÉ GUARDIA, Manual de Derecho Procesal Penal, p. 437.

31 Corte IDH, caso Bayarri vs. Argentina, sentencia de 30 de octubre de 2008, párr. 41.

32 PICCIRILLI, Ausencia de regulación procesal penal aplicable a la evidencia digital y su correlación con los delitos informáticos. Legislación vigente, anteproyectos y convenio de Budapest.

prueba digital (como cualquier otra prueba) pueden ser explicadas como una intromisión gradual que hace el Estado en la esfera de intimidad de las personas. Esto abarca desde una medida como la orden de conservación de datos electrónicos, incluidos los datos de tráfico de las comunicaciones, hasta la medida extrema de intervenir comunicaciones y obtener su contenido en tiempo real.

Como consecuencia de lo expresado, si bien el principio de libertad probatoria existe en el proceso penal, tiene un límite debido a las intromisiones que genera, por lo que debe respetar las garantías constitucionales. Es por ello que el modo de incorporación de las pruebas debe responder a medios reglados y, ante la ausencia de pautas legales para la obtención de una prueba, se deberá aplicar por analogía las pautas establecidas para otra prueba similar. En este sentido, Cafferata Nores dice: "El ingreso del dato probatorio en el proceso deberá ser realizado respetando el modo de hacerlo previsto en la ley (o el analógicamente más aplicable en el caso de que el medio de prueba utilizado no estuviera expresamente regulado)"[33].

En función de lo expuesto, se debe interpretar que la ley no establece un sistema taxativo ni contiene fórmulas cerradas sobre cuál es el camino adecuado para probar un hecho, por lo tanto, en materia probatoria ha de interpretarse que todo lo que no resulta prohibido se encuentra permitido.

Sin embargo, la libertad de medios de prueba no significa arbitrariedad en el procedimiento probatorio, pues a éste se lo concibe como una forma de asegurar la eficacia de la prueba y los derechos de las partes. Cada prueba se ajustará al trámite asignado, y cuando se quiera optar por un medio probatorio no previsto, como se señaló precedentemente, se deberá utilizar el procedimiento señalado para el medio expresamente regulado que sea analógicamente más aplicable, según la naturaleza y las modalidades de aquél. Además, se deberá observar las disposiciones tendientes a garantizar la defensa de las partes, como requisito para la válida utilización del medio de prueba.

6 INFORMACIÓN EN LA "NUBE". ACCESO TRANSFRONTERIZO. REGISTRO REMOTO DE DISPOSITIVOS TECNOLÓGICOS. PROBLEMAS DE COMPETENCIA Y JURISDICCIÓN

Debe diferenciarse el caso o evidencia digital donde se analiza la información que se encuentra en un dispositivo (computadora, móvil, Tablet, etc.) de los casos en los cuales se debe analizar o investigar datos que se almacenan en los que se denomina "nube".

El primer gran desafío al que se enfrenta la persecución penal en la Era Digital radica

33 CAFFERATA NORES, La prueba en el proceso penal, p. 21.

en la deslocalización de la información digital a conseguir, ya que la misma puede ser "accesible" desde nuestros hogares sin necesidad de estar "localizada" dentro de los confines de nuestro domicilio.

Una de las principales diligencias judiciales de investigación que se ordena cada vez más frecuentemente consiste en ordenar la clonación y el examen forense de los discos duros y elementos periféricos de los equipos informáticos aprehendidos tras un registro domiciliario, así como de cualquier otro dispositivo electrónico de comunicación o almacenamiento. Sin embargo, al movernos en un entorno digital e interconectado a nivel mundial, la óptica desde la que enfocar esas tareas de incautación de la información digital debe ser sustancialmente distinta al tradicional enfoque con el que se procede a un registro domiciliario en el mundo corpóreo, pues la protección constitucional y legal del domicilio es claramente insuficiente para la salvaguardia del entorno digital[34], pues está claro que el contenido vendría constituido por la información digital, con independencia del tamaño o formato utilizado, pero el continente no tiene por qué ser el equipo informático a través del cual dicha información fue creada, recopilada, transformada o emitida. Dicho equipo puede ser simplemente un medio a través del cual la información digital fue colocada en otro lugar, otro continente.

Es preciso tener en cuenta, además, que esta deslocalización de la información almacenada se hace cada vez más habitual en aquellos entornos que trabajan conforme a lo que se conoce como "técnicas de computación en la nube (Cloud Computing)", en donde la información se almacena de manera permanente en servidores alojados en cualquier parte del mundo y se envía, a través del acceso a Internet, a cachés temporales del ordenador de sobremesa del cliente, su portátil, PDA, etc. Es que cada vez es más común depositar nuestra información en lugares como *I Cloud*, *Google Drive*, *Dropbox*, *One Drive*, entre otros. Ello significa que subimos nuestros datos a un espacio virtual y dejan de alojarse en nuestros dispositivos (computadora, *tablet*, celular), cuestión que puede tornar infructuosa la realización de allanamientos que tengan por objeto el secuestro de dispositivos con el objetivo de incautar la información que estos contengan.

La trascendencia jurídica de la ubicación física de las pruebas electrónicas, a los efectos de lograr su incautación cuando se encuentran en el extranjero, nos hace recordar que la expresión "Internet no conoce fronteras" favorece al delincuente, porque en el plano policial las fronteras nacionales se convierten en auténticos obstáculos para las legítimas labores de investigación y recogida de las evidencias de dichos delitos. Las fuerzas y cuerpos de seguridad deben respetar la soberanía de otros países y, como norma general, no pueden llevar a cabo actividades de investigación y obtención de

34 GONZÁLEZ-CUÉLLAR SERRANO, Garantías constitucionales en la persecución penal en el entorno digital, p. 891.

pruebas fuera de su jurisdicción[35]. Se hace preciso una inmediata colaboración internacional, que no siempre llega a tiempo, bien porque el país requerido no disponga de la tecnología adecuada para cumplir con la orden solicitada, bien porque el tiempo que transcurra hasta su realización no impida que las pruebas puedan alterarse o destruirse, o bien porque dicho país simplemente no atienda a la ayuda reclamada.

Ahora bien, determinar en dónde se encuentra esa *cloud* es fundamental para determinar las cuestiones de competencia territorial respecto a las investigaciones penales.

Antes de adentrarnos en este tema es importante destacar que, cuando se está ante información o evidencia digital a la que se debe acceder para su recolección, deben destacarse dos posibilidades: **a)** que la misma se encuentre en el territorio en el cual se está llevando a cabo la investigación judicial o bien, **b)** que se encuentre en otra jurisdicción. En el primer caso no se presenta ninguna problemática, mientras que, en este segundo caso, el remedio procesal previsto es el exhorto, lo que implica que el juez que investiga solicita a otro magistrado sito en el lugar en el cual se encuentra la evidencia o donde se debe llevar a cabo un acto procesal, su cooperación. Este trámite que puede darse entre provincias de un mismo estado o entre distintos países, requiere varios pasos formales a seguir que muchas veces se extienden en el tiempo (a veces tardan años) y no permiten una eficaz recolección de evidencia digital, la cual se caracteriza, tal como se dijo, por su volatilidad.

Como consecuencia de lo expuesto, resulta importante identificar en qué lugar físico se encuentra la evidencia. Si bien esto parece obvio, hay casos en los cuales no es tan fácil establecer su localización. La información en la "nube" es uno de ellos. Cabe preguntarse entonces, ¿qué debe entenderse por lugar físico?: a) desde el cuál se accede a la información, o b) el lugar en el cual se encuentran los servidores que alojan la evidencia. Esta problemática no posee una solución en la normativa procesal, por lo que resulta importante abordarla.

De considerar correcta la primera opción (lugar desde dónde se accede a la información), podría entenderse que puede hacerse desde cualquier lugar del mundo con acceso a Internet, con lo cual con el simple acceso se garantiza la jurisdicción.

Por otro lado, de entender que la respuesta es la segunda (ubicación del servidor) correspondería solicitar la cooperación interjurisdiccional o internacional toda vez que de intentar extraer o recabar información almacenada en la "nube", podría considerarse, que se vulnera el principio de territorialidad.

En este sentido, cabe destacar que el Convenio sobre Ciberdelito del Consejo de

35 En el mismo sentido, CSONKA, The Council of Europe´s Convention on Cyber-Crime and other european initiatives, p. 477. También, GERCKE, Understanding cybercrime: a Guide for Developing Countries, www.itu.int/ITUD/cyb/cybersecurity/legislation.html

Europa[36] establece en su art. 32 (cap. III - Cooperación Internacional) el acceso transfronterizo a datos almacenados sin requerir la autorización del otro estado, en los siguientes casos: 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.

Como consecuencia, entre los Estados que hayan aprobado e incorporado en su legislación interna, la referida Convención, se vislumbra una opción al interrogante planteado (vinculado al lugar desde el cuál se accede a la información), por el cual no se requiere la tramitación de un exhorto para el acceso transfronterizo a los datos almacenados, pero solo para los dos supuestos allí contemplados.

Por otro lado, los problemas de jurisdicción pueden plantearse incluso cuando la información está almacenada en un dispositivo, pues existen técnicas forenses para acceder o recolectar evidencia digital ya sea que aquel se encuentre en el territorio en la cual se está llevando a cabo la investigación o que esté ubicada en extraña jurisdicción sin la necesidad de solicitarla a otro magistrado o estado o si quiera desplazarse físicamente: *remote forensic* (o registro remoto en español). Esto significa que el desarrollo de las nuevas TIC ha generado herramientas o 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 geolocalización que permitan la ubicación geográfica de un dispositivo)"[37]. Es posible entonces acceder a datos informáticos contenidos en un dispositivo a distancia, de manera remota, es decir sin el contacto físico con el soporte que contiene la información y sin necesidad de librar un exhorto para ello. La manera técnica de llevar a cabo el *Remote Forensic* consiste en la instalación de un software "malicioso" (malware)[38] en el dispositivo al que se quiere acceder sin que el usuario o propietario del mismo lo sepa.

Si bien esta herramienta parece algo novedosa, hay países como el caso de España que ya la han reglamentado como una herramienta a fin de recolectar evidencia digital en un proceso penal. En este sentido, la Ley Orgánica 13/2015 que modifica la Ley de

36 Conocido como Convenio de Budapest. La argentina aprobó con reservas este Convenio, mediante Ley 27.411.
37 SALT, Nuevos Desafíos de la evidencia digital: Acceso transfronterizo y técnicas de acceso remoto a datos informáticos, p. 53.
38 El término Malware es la abreviatura de malicious software y este término engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento; dentro del grupo de malwares podemos encontrar términos como, por ejemplo, virus, troyanos, spyware, gusanos (worm), keyloggers, botnets, ransomwares, entre otros.

Enjuiciamiento Criminal española, prevé en su art. 588 septies a).1, la autorización judicial para

> la instalación de software, que permitan, de forma remota y telemática, el examen a distancia y sin conocimiento del 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 se persiga la investigación de alguno de los siguientes delitos: Delitos cometidos en el seno de organizaciones criminales, de terrorismo, los cometidos contra menores o discapacitados, contra la Constitución, de traición y relativos a la defensa nacional y los cometidos a través de instrumentos informáticos o de telecomunicación[39].

Esta herramienta, no se encuentra legislada en el código procesal penal federal de la República Argentina, aunque sí lo hace el proyecto de reformas promovidas por el Ministerio de Justicia y Derechos Humanos a través del Programa "Justicia 2020", en el art. 21 del proyecto se establece la incorporación del título VI "Medidas especiales de investigación" que establece, previo un examen de razonabilidad que deberá efectuar el juez, la posibilidad de disponer medidas de vigilancia remota sobre equipos informáticos, la cual no podrá ser mayor a un mes (prorrogable a un máximo de 3 meses)[40]. Tampoco se encuentra normado en los Código procesales en materia punitiva de las provincias que conforman la República Argentina, con excepción del art. 153 del CPP de Neuquén[41].

La realidad indica que este tipo de herramientas que si bien son beneficiosas para la investigación deben resultar regladas para legitimar su incorporación al proceso judicial y para resguardar las garantías del sospechoso, pues la prueba que se obtiene ha sido recolectada mediante un acceso a distancia; máxime, asimismo, porque no sólo sirve

39 https://www.boe.es/buscar/act.php?id=BOE-A-1882-6036

40 https://www.justicia2020.gob.ar/wp-content/uploads/2016/09/texto-final-del-proyecto-reforma-CPP.pdf

41 Esta es la única provincia argentina que lo ha incorporado en su CPP (Ley 2.784), en su art. 153 dispone: "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.**
A cualquier persona física o jurídica que preste un servicio a distancia por vía electrónica, podrá requerírsele la entrega de la información que esté bajo su poder o control referida a los usuarios o abonados, o los datos de los mismos.
La información que no resulte útil a la investigación, no podrá ser utilizada y deberá ser devuelta, previo ser puesta a disposición de la defensa, que podrá pedir su preservación. Regirán las limitaciones aplicables a los documentos" (el resaltado me pertenece).

para el registro y secuestro de datos (archivos, registro de búsquedas, entre otros) sin tomar contacto físico con el dispositivo de almacenamiento, sino que también posibilitan la interceptación de datos de tráfico y contenido[42], como así también pueden activarse remotamente las cámaras y micrófonos incorporados al dispositivo accedido.

Además, pueden obtenerse elementos de gran importancia como contraseñas o claves de acceso y de encriptación[43] que son fundamentales para la obtención y posterior utilización de la evidencia digital. Por lo demás, esta herramienta también posibilita "identificar al autor de una comunicación por Internet que se hubiera realizado con técnicas especialmente diseñadas para enmascarar la dirección IP desde la que se produce la comunicación"[44]. Como consecuencia, la herramienta permite ver el pasado: las huellas, es decir, los archivos o búsquedas almacenadas en el dispositivo, el presente: el tráfico de datos en vivo y el futuro: luego de que se insertó el *malware*, toda la actividad posterior a la autorización de la medida se sigue recolectando, lo cual podría exceder el cumplimiento de una orden de registro o allanamiento, si la se la piensa análogamente, aunque -cabe reiterar-, por las particularidades de este medio y la evidencia digital, no es posible asimilarlo a los institutos probatorios reglados hoy en día. En este sentido, la búsqueda de información que pueda realizarse tomando esta herramienta debe circunscribirse a los elementos que sean pertinentes a la investigación, por lo que debería establecerse para cada caso una suerte de orden de allanamiento electrónica a fin de evitar abusos y violaciones a las garantías del sospechoso. Por lo demás, no debería dejarse que la herramienta actúe sola recolectando información indiscriminadamente, sino que resulta fundamental que se asigne personal de investigación junto con un experto en informática para controlar que el funcionamiento de aquella se desarrolle en el marco de la autorización judicial.

Finalmente, y en relación al tiempo que debe durar la medida, el malware debe estar programado por un determinado tiempo, no puede permitirse un acceso irrestricto sin limitación temporal. De tal modo deberá establecerse en la orden que lo permita, un límite temporal de duración donde se permita recabar evidencia digital y no extenderse en el tiempo innecesariamente, pues ello, vulneraría las garantías del imputado.

42 Mientras que los datos de contenido serían los datos relativos al mensaje en sí, los datos de tráfico tienen que ver con elementos que permiten conocer el lugar y horario de la comunicación, entre otros.

43 Cabe señalar que no tiene utilidad un documento que esté cifrado si no es posible leerlo y por ende utilizarlo como evidencia en el proceso de investigación. Los métodos para desencriptar sin las claves necesarias pueden ser muy engorrosos y tomar mucho tiempo del que a veces no disponen las investigaciones. Cfr. PICCIRILLI, María Eugenia, Ausencia de regulación procesal penal aplicable a la evidencia digital y su correlación con los delitos informáticos. Legislación vigente, anteproyectos y convenio de Budapest, en: SJA 11/03/2020, 45 - LLOnline AR/DOC/509/2020.

44 SALT, Nuevos Desafios de la evidencia digital: Acceso transfronterizo y técnicas de acceso remoto a datos informáticos, p. 72.

7 LA IMPORTANCIA DE LA COPIA FORENSE (*BIT A BIT*) - ALGORITMO *HASH*

Las técnicas forenses permiten realizar una copia *bit a bit* o copia forense, que implica, como se señaló anteriormente, la creación de un duplicado íntegro de la información que se recolecta.

En este sentido, la información que puede contener cualquier tipo de archivo (documento, video, foto) no es solo la que un simple usuario puede ver, es decir, no solo contiene datos visibles, sino que también posee metadatos que no son advertidos ni conocidos por el ojo del simple usuario. Estos últimos son definidos como los datos acerca de los datos, por ejemplo, en una foto el dato que percibe cualquier persona es la imagen, pero los metadatos contienen información como las coordenadas GPS del lugar en donde se tomó la foto, el modelo de la cámara que se utilizó, la fecha y hora, el software que se implementó para editar la imagen, el usuario utilizado, entre otros.

Consecuentemente cabe realizarse los siguientes interrogantes: a) ¿Cómo pueden visualizarse los metadatos de un archivo?; b) ¿Pueden modificarse los metadatos de un archivo pero que siga pareciendo igual a simple vista?; y c) ¿Cómo saber si dos archivos son exactamente iguales?

Con respecto al primer interrogante, cabe decir que los metadatos se pueden observar y recolectar mediante el empleo de herramientas forenses como, como pueden ser, los *software EXIF reader*, *EXIF Viewer*, *EXIF Image Viewer*, *FIV Forensic Image Viewer*, entre otros. Es por ello que para un simple usuario los metadatos permanecen escondidos, esperando a ser encontrados.

En cuanto a la siguiente pregunta, resulta importante señalar que, por ejemplo, un archivo que contiene una foto puede ser modificado sin que aquello sea visible ante un simple usuario. A modo de ejemplo han podido descubrirse archivos de imagen que contenían una foto a la cual se le habían agregado mensajes que eran prácticamente invisibles al ojo humano con el fin de que narcotraficantes se contactaran sin ser descubiertos[45].

Dado que es posible alterar un archivo siendo muy difícil su detección, corresponde adentrarnos en la última pregunta, en este sentido hay herramientas forenses que permiten determinar, mediante la utilización de un algoritmo matemático de autenticación hexadecimal denominado *hash*, este algoritmo transforma cualquier bloque arbitrario

45 Cabe destacar la utilización de fotografías que, si bien en principio parecen inocentes, esconden mensajes ocultos con el fin de organizar y ejecutar el plan delictual (lugares de encuentro, fechas, etc.), enviadas a través de correos electrónicos. Una de las herramientas que puede permitirnos establecer la existencia de estos mensajes es el *hash* que determina si estamos ante una foto que es idéntica o no a la que tenemos presentada en un correo. Para mayor información ver https://www.securityartwork.es/2010/04/15/introduccion-a-la-esteganografia-i/

en una nueva serie de caracteres con una longitud fija, si se está ante dos archivos idénticos tanto en sus datos como en sus metadatos; las herramientas disponibles actualmente son MD5, SHA1 y SHA256[46]. Esto significa que, si el archivo en cuestión sufre alguna modificación, por más mínima que sea (como puede ser un punto o un solo *bit*), el resultado que arroja el algoritmo es completamente diferente, lo que nos permite concluir que el archivo no es el mismo, que ha sido modificado.

Analizadas las cuestiones anteriores, corresponde adentrarse en la copia forense o *bit a bit*, una herramienta útil que permite copiar de manera total y exacta la información contenida en un disco rígido (*bit a bit*, es decir con sus datos ya sean visibles o no visibles -borrados, pero no sobre escritos-, sus metadatos, etc.) en una o más copias, siempre utilizando herramientas forenses que deben ser manipuladas exclusivamente por expertos en informática[47]. Como consecuencia la pérdida de la información es casi imposible y permite que varias partes (la defensa, la fiscalía, el juez, la querella) tengan acceso irrestricto a las copias efectuadas de manera simultánea, las cuales pueden garantizarse que son copias exactas del original, lo que resulta ser una de las características ventajosas de la evidencia digital. El elemento que posibilita efectuar ese control de identidad de la copia es el ya mencionado *hash*.

8 ALGUNOS PROBLEMAS PROCESALES VINCULADOS CON LA EVIDENCIA DIGITAL

Teniendo en cuenta lo expuesto precedentemente, la obtención de evidencia digital nos coloca en una situación sumamente compleja en términos procesales, y por qué no, constitucionales, ya que no se encuentra previsto legalmente un método específico para su recolección y tratamiento.

Señala Saín que la evidencia digital "está representada por los datos e información digital que se almacena, transmite o recibe en un dispositivo electrónico"[48]. Por ende, las dos características fundamentales son la volatilidad y la sensibilidad de la evidencia. Muchas veces también son pruebas transfronterizas, ya que por ejemplo puede entrar en juego que una empresa proveedora de servicios de internet tenga sus servidores en un país distinto al lugar donde se investiga la comisión del delito. Ello, sumado a que no se cuenta al día de la fecha con un convenio de cooperación sobre esta temática, genera que

46 La diferencia radica en la cantidad de bits que trabaja, mientras que MD5 lo hace con 128, SHA 1 con 160 y SHA 256 con 256. Para más información ver: https://www.gaussianos.com/algoritmos-hash-i-introduccion/

47 En este sentido, debe aclararse que tanto la realización de las copias *BIT a BIT* como la preparación de los discos rígidos (ya sea el original o sobre los cuales sea harán las copias) deben manipularse por el experto en informática sin excepción, ya que de efectuarse por una persona sin los conocimientos y herramientas específicos podría afectarse la prueba recolectada, alterando su contenido original, o bien perjudicando las copias, las cuales podrían no ser iguales a la evidencia.

48 SAIN, Delito y nuevas tecnologías. Fraude, narcotráfico y lavado de dinero por internet.

la evidencia muchas veces tenga que solicitarse por vía de exhortos en más de un país, lo que afecta tanto el proceso de averiguación de la verdad, como bien el plazo razonable al que tiene que estar sujeto un proceso.

Es menester, entonces, estandarizar estos procedimientos, ya que, por el contrario, habría un sinfín de técnicas de investigación y de recolección de evidencia obligando así a un imputado a prever otras tantas estrategias de defensa lo que en principio no luce ni legal, ni congruente, ni igualitario, ni mucho menos, justo. Si bien rige en el derecho procesal el principio de libertad probatoria, lo cierto es que ello no otorga la posibilidad a ningún investigador de obtener pruebas por cualquier medio[49].

En efecto, siempre que la medida probatoria coloque en una situación de crisis a los derechos y garantías de los justiciables, se transformará en una medida de coerción o de injerencia. Es por ello que mientras no sean medidas legalmente previstas, deben ser analizadas con el prisma de cualquier medida de coerción, como por ejemplo el del principio de proporcionalidad y última ratio del derecho penal.

8.1 La doctrina de la *plain view* en el registro de dispositivos electrónicos

Resulta sumamente ilustrativo para comenzar este acápite el ejemplo que brinda Marcos Salt, citado en la obra de Christian Sueiro:

> Si en el registro y secuestro de evidencia en entornos digitales yo pretendo utilizar las normas del secuestro de evidencia física o la jurisprudencia de la CS, seguramente las soluciones a las que arribe no van a ser siempre las más adecuadas. Por ejemplo, pensemos para el caso de hallazgos casuales y toda la doctrina de la plain view. No podemos aplicar la doctrina de la Corte de la misma manera para un ámbito físico que para un ámbito digital. Si allano esta aula en la que estamos sentados para buscar un elemento físico, obviamente por más que busque y busque solo vamos a encontrar lo que está

49 "Isto se dá porque o ordenamento a partir do momento que permite restrições a determinados direitos fundamentais, deve fazê-lo de forma descrita em lei, em respeito ao princípio da legalidade, bem como adequando-o estas restrições ao direito positivo, em respeito também o princípio da proporcionalidade.
Este é o grande marco da temática da proibição de determinadas provas e a seus métodos de obtenção, que nem sempre seguem o os princípios do estado democrático de direito, regidos pela Carta Magna de 1988.
Portanto, para estipular um regime adequado para recolha e produção de provas digitais é fundamental definir quais os dados são produzidos e atrelados a uma determinada comunicação na rede, a saber, se são dados de apenas cadastrais —aqueles necessários por exemplo para efetuar um cadastro no Facebook para abertura de conta, ou dados de localização —aqueles que revelam a localização do emissor da mensagem, meio eletrônico utilizado, podendo citar os IP's ou se são dados de conteúdo —aqueles que revelam o conteúdo das mensagens de whatsaps", cfr. EMMERICH de SOUZA, Tatiana Lourenço, A prova digital no processo penal e seus efeitos colaterais na preservação dos direitos fundamentais, en: DPyC 2019 (noviembre), 05/11/2019, 106; LLOnline AR/DOC/2887/2019.

> en el ámbito físico en este momento. Si el registro lo realizo sobre una computadora, voy a poder encontrar lo que está alojado digitalmente en este momento, lo que estaba hace un año, lo que estaba hace cinco años, lo que se trató de borrar, lo que introdujo el usuario anterior de la computadora, y voy a poder encontrar todo de manera tal que el hecho de la incorporación de datos accidentales encontrados en un sistema informático no puede ser regulado de la misma manera que en el caso de la evidencia física[50].

La doctrina de la *plain view* -plena vista- supone en términos prácticos la posibilidad de incautar evidencia descubierta durante un registro válido si la naturaleza incriminatoria del elemento que hay que incautar, suficiente para crear una causa probable de que este constituye una prueba, es inmediatamente aparente.

De este modo sería válida la incorporación de evidencia al proceso que haya sido encontrada de conformidad con el objeto delimitado en la orden de registro, siendo nulo todo aquello que se obtenga más allá de esos límites. La doctrina de la *plain view* convalida aquella evidencia que no se encontraba dentro de esa delimitación previa, pero que fue hallada "a simple vista o casualmente" mientras se realizaba el procedimiento original.

En relación con la búsqueda de evidencia digital se presenta un primer problema y es aquel vinculado al formato. Por ello un procedimiento como el que se encuentra previsto en Argentina o en otras legislaciones similares, no es apto para distinguir previamente el objeto de la búsqueda, por lo que coloca al investigador en la posición de poder revisar la totalidad de los datos de cualquier dispositivo informático, lo que genera un estado de indefensión total del individuo respecto de su propia privacidad.

El desafío es que el procedimiento seleccionado sea capaz de conjugar tanto con las garantías constitucionales de defensa en juicio, debido proceso, legalidad, así como también con las exigencias procesales que se establezcan en cada legislación procedimental.

Actualmente, existe un nivel interesante de consenso en las costumbres, buenas prácticas forenses y la comunidad científica, respecto de cómo proceder para incautar la información en entornos digitales; que tal como se expresó anteriormente es la creación de una copia *hash*.

Sin embargo, y más allá de la eficacia de este mecanismo, se presentan dos importantes limitaciones. En primer lugar, no está regulado en la mayoría de los ordenamientos

50 SALT, La relación entre la persecución de los delitos informáticos y el derecho penal internacional. Delitos informáticos. Aspectos de derecho penal internacional, en: Revista Informática y Delito, p. 240.

procesales (tal como ocurre en la República Argentina, salvo la excepción señalada) por lo que más allá del consenso que reúne, no se cuenta hoy en día desde la perspectiva de la defensa, de un remedio procesal para invalidar un procedimiento que se aparte de estos saludables estándares. Finalmente, no se encuentra aún una respuesta al interrogante sobre cómo analizar esa información obtenida sin afectar los derechos de los justiciables.

Y aquí debe recordarse que la Corte Suprema de los Estados Unidos de América ha ocupado de delimitar el alcance de la doctrina de la *plain view*. En el caso "Estados Unidos v. Carey"[51] -precedente de los primeros en ocuparse del registro en entornos digitales- un analista forense descubrió una imagen de pornografía infantil mientras estaba realizando un registro a través del disco duro de un ordenador buscando evidencia de venta de estupefacientes. Seguidamente abandonó el registro original y comenzó a buscar por otras imágenes. Consecuentemente, abrió una cadena de archivos adicionales que contenían pornografía infantil. La Corte sostuvo que la primera imagen descubierta era admisible, pero los archivos abiertos subsiguientes estaban más allá del alcance de la orden.

Como puede observarse, la idea de mecanismos legalmente previstos *ex ante*, exigibles para cualquier investigación no resulta antojadiza, sino que de lo contrario se está en una zona gris entre la utilización de la información obtenida para combatir el crimen y la utilización como práctica estatal abusiva.

Ha dicho a su vez la Corte Estadounidense que "esta práctica discriminatoria e ineficiente era justo el tipo de mal uso de los poderes de gobierno que la Cuarta Enmienda fue creada para detener"[52], deviene que la misma línea de pensamiento puede ser utilizada para proteger lo establecido en las diferentes Constituciones Nacionales de países que establecen el Estado Constitucional de Derecho[53].

En suma, se entiende desde aquí que una regulación legal previa sobre los mecanismos de investigación es estrictamente necesaria, de manera tal que se permita saber cómo debe procederse en pos de averiguar la verdad sin afectar garantías individuales

51 "United States v. Carey", Decided: April 14, 1999, 172 F.3d 1268 (10th Cir. 1999).
52 "Coolidge v. New Hampshire", 403 US 443 (1971, voto del juez J. Stewart).
53 En la República Argentina, es a partir del art. 18 de su Constitución Nacional, como también a partir del art. 75 inc. 22 de dicha carta fundamental, en razón de que en dicha norma, a partir de la reforma año 1994, se incorporaron, con igual Jerarquía, varios Tratados Internacionales. Es así que en algunos de ellos encontramos disposiciones protectoras del domicilio. Así, el artículo 9º de la Declaración Americana de los Derechos y Deberes del Hombre establece que toda persona tiene derecho a la inviolabilidad del domicilio. A su vez, el artículo 12 de la Declaración Universal de Derechos Humanos dispone que nadie puede ser objeto de injerencias arbitrarias en su domicilio y que las leyes deben proteger a las personas contra tales actos. El artículo 11, inc. 2, del Pacto de San José de Costa Rica establece que "nadie puede ser objeto de injerencias arbitrarias o abusivas... en su domicilio...". También, se puede relacionar con la reserva de la intimidad, puesto que protege todo aspecto de la vida privada de un individuo que este quiera preservar del conocimiento e intrusión de los demás (Art. 11. 1, CADH).

tanto en la obtención de la información como en su análisis[54].

8.2 El uso de las redes sociales por parte de las fuerzas policiales

Otra de las cuestiones a considerar en la recolección de la evidencia digital, está vinculado con el actuar de los agentes policiales en las diferentes redes sociales, como ser, *Facebook*, *Instagram*, *Twitter*, *TikTok*, entre otras; donde dichos funcionarios policiales realizan diferentes averiguaciones que luego son incorporadas al proceso.

Por lo general dicha actividad se realiza en hechos delictivos donde los presuntos autores son desconocidos, para luego atribuirles a individuos concretos las averiguaciones obtenidas de perfiles públicos de las redes sociales.

Esta técnica forma parte de lo que actualmente se conoce como OSINT (*Open Source Inteligence*) o búsqueda en fuentes abiertas. Se trata de búsqueda de información en fuentes públicas (redes sociales, buscadores, fotografías, medios de comunicación, etc.) sin autorización previa, ya que en principio son datos de acceso público.

Se utiliza no solo en procesos penales, sino que tiene aristas sumamente positivas en lo que tiene que ver, por ejemplo, con seguridad pública, investigaciones corporativas o procesos de negociación. Sus principales ventajas son el alto volumen de información que se puede analizar, la posibilidad de que este análisis sea prácticamente automatizable y que, a su vez, suelen ser herramientas gratuitas.

Lejos de la novedad la inteligencia sobre fuentes abiertas (OSINT; también se habla de SOCMINT, *Social Media Intelligence*) es una actividad desplegada con generalidad para la prevención e investigación de delitos que, por cierto, es conveniente que esté regulada con precisión, fijándole límites tanto en lo referente a los motivos que la habilitan como en la extensión o profundidad que puede alcanzar[55]. La jurisprudencia argentina ha validado la utilización de esta herramienta, al sostener que

> se advierte que en el caso particular de autos no puede aludir la defensa una expectativa razonable de privacidad, en tanto la información fue publicada voluntariamente por la imputada en una plataforma digital que, al no contar con restricciones para su acceso (como un usuario o contraseña), es accesible por cualquier persona. En definitiva, esa parte no realiza una crítica suficientemente fundada de la utilización de un dato que obtuviera la prevención mediante la investigación en fuentes abiertas (‘*Open-source*

54 MOLINAS, La obtención de evidencia digital y sus desafíos constitucionales. Una mirada defensista.
55 RIQUERT, Coronavirus: entre la prevención y el ciberpatrullaje.

intelligence' -OSINT-), práctica esta que conlleva el uso de un conjunto de técnicas que facilitan la recolección de información accesible en internet[56].

9 COLOFÓN

No existe duda alguna que los entornos digitales y los nuevos modos de comunicarse con los que se interactúan cada día y en los que se depositan y registran aspectos íntimos y privados de nuestro proyecto de vida, son ámbitos que merecen protección frente a la injerencia estatal.

Los entornos digitales encierran ámbitos de privacidad profunda de las personas, y cualquier injerencia estatal que pretenda obtener elementos probatorios en este contexto, deberá estar debidamente fundada, ser ordenada por autoridad jurisdiccional en el marco de una causa penal ya iniciada y con elementos objetivos que den sustento al interés. Estas injerencias "solo se justifican cuando razones de sospecha suficiente autorizan a sostener que en un proceso penal existen motivos bastante que ponderan aquel objetivo de la realización del derecho penal sustantivo"[57].

Además de ello, y por sobre todas las cosas, debe existir una ley que regule las condiciones y los procedimientos bajos los cuales el Estado podrá inmiscuirse en este ámbito de privacidad en procura de localizar elementos probatorios que permitan llegar a la resolución de un hecho criminal.

A EVIDENCIA DIGITAL NO PROCESSO PENAL E A PRESERVAÇÃO DOS DIREITOS FUNDAMENTAIS

RESUMO

As novas tecnologias da informação e da comunicação (TIC) modificaram o nosso cotidiano. O indivíduo social perdeu seu anonimato comunicacional para se converter em fonte comunicacional registrável. Desse modo, a constante comunicação do sujeito na modernidade, mediante estas ferramentas, permite claramente novos mecanismos de controle estatal. A prova digital é a informação dos dados que foram armazenados ou transmitidos em um formato digital ou através de um meio informático e que possua valor probatório. Consequentemente, a manipulação e o exame das provas eletrônicas são

56 Cámara Federal de Casación Penal, sala I, 23/12/2019, *in re* "T. S., F. s/ recurso de casación", *RDP* 2020-4, 162; *LLOnline* AR/JUR/52246/2019.
57 PETRONE, Prueba informática, p. 23.

uma tarefa que requer particular cuidado em consideração às características especiais da prova digital, porque, entre outras coisas, esta classe de prova pode se reproduzir e se alterar facilmente, dado que é maleável, o que a tornando vulnerável. Ao longo do presente trabalho, será possível identificar as diferenças que a prova digital tem em relação à prova física e, como consequência disso, é analisada a problemática que gera a aplicação da regulamentação atual com base na prova digital e a incidência que a ela tem nos diferentes crimes, especialmente nos crimes informáticos. Não há dúvida de que os ambientes digitais e as novas formas de comunicação, por meio dos quais há interação social que inclui aspectos íntimos e privados depositados e registrados, são áreas que merecem proteção contra a interferência do Estado.

Palavras-chave: Investigação. Evidência digital. Internet. Ciência e Tecnologia. Direito à intimidade. Direitos Humanos. Delitos informáticos. Processo Penal. Coleta de evidência digital e evidência física. Cooperação internacional.

BIBLIOGRAFÍA

ABDELCADER, Yamila L. **La evidencia digital en el proceso penal**. **A propósito del fallo mediante el que se condenó a Ricardo Russo, pediatra del Hospital Garrahan**. En: RDP 2020-3, 38, 09/03/2020; LLOnline AR/DOC/4223/2019.

BADENI, Gregorio. **Tratado de Derecho Constitucional**. 2º edición, La Ley, Buenos Aires, 2006.

BARLOW, John Perry. **A Declaration of Independence of Cyberspace**. Disponible en: https://projects.eff.org/~barlow/DeclarationFinal.html

BERGEAUD, Aurèlie. **Le droit à la preuve.** LGDJ-Lextenso éditions, París, 2010.

CAFFERATA NORES, José I. **La Prueba en el Proceso Penal, con especial referencia a la Ley 23.984**. 3º edición, Depalma, Buenos Aires: 1998.

CORTÉS, Carlos. **Vigilancia de la red**: ¿Qué significa monitorear y detectar contenidos en internet?, Investigación del Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE) de la Facultad de Derecho de la Universidad de Palermo, pp. 3 y ss., en: https://www.palermo.edu/cele/pdf/El-deseo-de-observar-la-red.pdf

CSONKA, Peter. **The Council of Europe´s Convention on Cyber-Crime and other european initiatives**. Revue Internationale de Droit Pénal, 2006, vol. 77.

EMMERICH de SOUZA, Tatiana Lourenço. **A prova digital no processo penal e seus efeitos colaterais na preservação dos direitos fundamentais.** en: DPyC 2019 (noviembre), 05/11/2019, 106; LLOnline AR/DOC/2887/2019.

FILLIA, Leonardo C., SUEIRO, Carlos C., MONTELEONE, Romina, NAGER, Hora-

cio S., ROSENDE, Eduardo E. **Análisis a "La reforma en materia de criminalidad informática al Código Penal de la Nación (ley 26.388)".** en: Sup. Penal 2008 (agosto), 15; *LL* 2008-E-938.

FLORIAN, Eugenio. **De las pruebas penales**. 3º edición, trad. Jorge Guerrero, Temis, Bogotá, 2002, tomos I y II.

GERCKE, Marco. **Understanding cybercrime:** a Guide for Developing Countries. 2011, en: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITU_Guide_A5_12072011.pdf

GONZÁLEZ-CUÉLLAR SERRANO, Nicolás. **Garantías constitucionales en la persecución penal en el entorno digital.** en AA.VV., Derecho y Justicia penal en el Siglo XXI. Liber amicorum en homenaje al Profesor Antonio González-Cuéllar García, Colex, Madrid, 2006.

HABERMAS, Jürgen. **Teoría de la acción comunicativa**: complementos y estudios previos. 3º edición, traducción de Manuel Jiménez Redondo, Ediciones Cátedra S.A., Madrid, 1997.

HASSEMER, Winfried. **Fundamentos del Derecho Penal**. trad. Arroyo Zapatero y Muñoz Conde, Barcelona, 1984.

JAUCHEN, Eduardo M., **Tratado de la prueba en materia penal**. Rubinzal-Culzoni, Santa Fe, 2002.

MAIER, Julio B. J., **Derecho procesal penal**. *Ad Hoc*, Buenos Aires, 2015, tomos I, II y III.

MOLINAS, Juan. **La obtención de evidencia digital y sus desafíos constitucionales.** Una mirada defensista. en: *DPyC* 2019 (abril), 03/04/2019, 96, *LLOnline* AR/DOC/392/2019

ORÉ GUARDIA, Arsenio. **Manual de Derecho Procesal Penal**. 2º edición, Editorial Alternativas, Lima, 1999.

PETRONE, Daniel Alberto. **Prueba informática**. 1ª edición, Didot, Buenos Aires, 2014.

PICCIRILLI, María Eugenia. **Ausencia de regulación procesal penal aplicable a la evidencia digital y su correlación con los delitos informáticos. Legislación vigente, anteproyectos y convenio de Budapest.** en: *SJA* 11/03/2020, 45 - *LLOnline* AR/DOC/509/2020

PICÓ I JUNOY, Joan. **El derecho a la prueba en el proceso civil**. Bosch, Barcelona: 1996.

RIQUERT, Marcelo A. **Coronavirus**: entre la prevención y el ciberpatrullaje, en: *DPyC* 2020 (diciembre), 15.

SAIN, Gustavo Raúl. **Delito y nuevas tecnologías. Fraude, narcotráfico y lavado de dinero por internet.** Editores del Puerto, Buenos Aires, 2012.

SALT, Marcos. **La relación entre la persecución de los delitos informáticos y el derecho penal internacional. Delitos informáticos. Aspectos de derecho penal internacional.** En: Revista Informática y Delito, Reunión preparatoria del XIX Congreso internacional de la Asociación Internacional de Derecho Penal AIDP, 2014.

SALT, Marcos. **Nuevos Desafíos de la evidencia digital: Acceso transfronterizo y técnicas de acceso remoto a datos informáticos**. *Ad Hoc*, Buenos Aires, 2017.

TARUFFO, Michele. Il Diritto allá prova. nel processo civile. En: **Rivista di Diritto Processuale XXXIX**. Supplemento al N. 4, 1984.