Revista Difusiones, ISSN 2314-1662, Num. 21, 2(2) julio-diciembre 2021, pp.59-75
Fecha de recepción: 25-10-2021. Fecha de aceptación: 17-11-2021

Evidencia digital de la nube. El aporte probatorio en Santiago del Estero

Digital evidence in the cloud: a probationary contribution in Santiago del Estero

Lilia Eugenia Palomo[1]
lilia.palomo@ucse.edu.ar
Universidad Católica de Santiago del Estero, Santiago del Estero, Argentina

Sergio Mario Guillet[2]
smguillet@yahoo.com.ar
Universidad Católica de Santiago del Estero, Santiago del Estero, Argentina

1 Esp. en Ing. Web; UCSE 2018. Esp. en Enseñanza de la Ed. Sup., UCC 2003. Ing. en Computación, UCSE 1999. Profesor Asociado FCID y FCSPyJ. Investigación "Del Big Data al Fast Data: enfoques modernos de Streaming de datos para el procesamiento de datos masivos en tiempo real" (2019-2021). "Hacia una economía digital: integración de los negocios, las operaciones y la tecnología en nuevos modelos operativos para el futuro" (2019). "Aproximación teórica de las Estrategias de Delivery de Datos Unificados del ámbito organizacional" (2018). Producción: WICC-2019 Big Data como tecnología disruptiva en los nuevos modelos operativos organizacionales. WICC-2018 Estudio y análisis de técnicas de modelado de grandes volúmenes de datos jurídicos. Divulgación: "Conversatorio sobre la enseñanza de la Ingeniería en tiempos de Covid-19 (2020). "El Big Data y sus Implicancias en el Contexto Jurídico y Empresarial" (2019). Gestión: Director Ing. en Informática, FCID, UCSE.

2 Abogado, UCSE, 1986. Investigación UCSE: "Evidencia digital de la nube" (FCID 2020). "Implicancias jurídicas del Big Data en la evidencia digital y su incidencia en el proceso judicial" (FCPSJ 2019). "Protocolo de Actuación para la Extracción de Evidencia Digital y su vinculación con los Códigos de Procedimientos, de Sgo. del E., en materia de prueba científica, en un Gabinete de Investigación Forense" (FCID 2018). Publicación: WICC-2020 Guía de Recomendaciones para el tratamiento del Big Data como evidencia digital. WICC-2019 Big Data desde la perspectiva de sus implicaciones jurídicas en evidencia digital. CIIDDI 2018 Articulación entre la Evidencia Digital y el Código de Procedimiento, en Materia de Prueba Científica. Desempeño en gestión: Secretario de Información Jurídica. PJSE.

Resumen

Al navegar en internet no hay barreras, aduanas, ni fronteras físicas entre países. El uso de datos en la nube, trajo consigo incidentes de seguridad, mayor tráfico de datos personales, terrorismo y delitos cibernéticos entre otros problemas, y como respuesta existen aplicaciones de forensia electrónica pensadas para recolección, análisis y conservación de archivos digitales que se encuentran alojados en la nube fuera de las fronteras de los países.
En materia de prueba judicial, resulta que la evidencia electrónica, es toda aquella información con valor probatorio almacenada o trasmitida de forma digital o binaria. El objeto de estudio de la Informática Forense, constituye la adquisición, preservación, recopilación y presentación de datos electrónicos y su posterior ofrecimiento como aporte probatorio.
Los códigos de procedimientos vigentes en nuestra provincia regulan aspectos de la prueba y del contexto dentro de cuyos límites se desarrolla la acción de peritos y consultores técnicos, cuando son incorporados al proceso. Hasta la fecha, aún no contienen disposiciones que se refieran a la prueba digital en general, o a la extracción de evidencia de medios informáticos en particular, así como protocolos de actuación a los fines de garantizar la seguridad jurídica y el debido proceso legal.
Este artículo se presenta, como línea de investigación, en el marco del proyecto de investigación de cátedra, "Evidencia Digital de la Nube" (UCSE, 2019-2021). Nos abocaremos al análisis de esta cuestión, a fin de brindar una guía para extraer evidencia digital contenida en servidores alojados fuera de la Nación Argentina, independiente que se encuentre bajo la tutela de una persona jurídica estatal o en poder de empresas privadas que operan servicios web.

Palabras clave

Evidencia digital, Cloud Computing, Prueba Digital, Forensia Electrónica.

Abstract

When browsing the Internet there are no barriers, Customs, or physical borders between countries. The use of data in the cloud brought security incidents, increased traffic of personal information, terrorism, and cybercrimes among other problems. There are forensic applications designed for the collection, analysis, and conservation of digital files located in the cloud outside country borders.
In terms of judicial evidence, it turns out that electronic evidence is all information with a probative value stored or transmitted digitally or binary. The object of study of Forensic Informatics constitutes the acquisition, preservation, compilation, and presentation of electronic data and its subsequent offer as evidence.

The Procedural Codes in force in our province regulate the aspects of the test and the context within whose limits the action of experts and technical consultants takes place when they are incorporated into the process. To date, they still do not contain provisions that refer to digital evidence in general or to the extraction of evidence from computer media in particular, as well as protocols for action to guarantee legal certainty and due legal process.
This article is a line of research within the framework of the chair research project: "Digital Evidence from the Cloud" (UCSE, 2019-2021). We will focus on the analysis of this issue to provide a guide to extract digital evidence contained in servers hosted outside the Argentine Nation, regardless of whether it is under the tutelage of a state legal entity or in the power of private companies that operate web services.

Key Words

Digital Evidence, Cloud Computing, Digital Evidence, Electronic Forensics.

Introducción

El presente estudio procura abordar aspectos relacionados con la evidencia electrónica, la investigación digital de delitos o sucesos cuya prueba se halle contenida en la nube, la importancia del análisis de los log de un servidor Web, la dirección IP, el acceso transfronterizo a los datos, las herramientas que se pueden utilizar para el análisis forense en la nube y la minería de datos para encontrar patrones de conducta criminal en red, entre otros aspectos, constituyen verdaderos desafíos de la actividad forense electrónica en la nube. Claro está, contrastando la utilización del enorme potencial de la informática y la electrónica en el esclarecimiento de la verdad, y el rol de la justicia en su mirada tuitiva de derechos personalísimos, la intimidad y las garantías del debido proceso de los ciudadanos.

En ese orden de ideas y como aporte académico, se proyectarán o propician buenas prácticas para el resguardo, la protección y conservación, o frezado de datos en el extranjero.

Asimismo, se esbozarán sugerencias procedimentales, presentando un análisis de los protocolos de acción disponibles en la comunidad forense para extraer evidencia digital almacenada en el extranjero.

Computación en la nube y evidencia digital

De acuerdo con Ruan, K., Baggili, I., Carthy, J. y Kechadi, T. (2011), la computación en la nube, Cloud Computing, tiene el potencial para convertirse en una de las tecnologías informáticas más transformadoras, siguiendo los pasos de los mainframes (computadora central), los portátiles, internet y los teléfonos inteligentes, transformando radicalmente la forma de crear, entregar, acceder y gestionar servicios.

El avance tecnológico ha generado nuevas formas de almacenamiento, ya no en la memoria física de los dispositivos, sino en “la nube”. Entonces, la posibilidad de acceder a esa nube aumenta las chances de encontrar evidencia digital”, así lo entiende el Superior Tribunal de la provincia de Río Negro y lo expresa en la nota periodística en ADN (Agencia Digital de Noticia) de fecha 12 de julio de 2019[3].

Como definición se puede decir que “la computación en la nube es un modelo para permitir el acceso de red ubicuo, conveniente y bajo demanda a un grupo compartido de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que pueden aprovisionarse y liberarse rápidamente con un mínimo esfuerzo de gestión o interacción del proveedor de servicios. Este modelo de nube se compone de cinco características esenciales, tres modelos de servicio y cuatro modelos de implementación” Mell, P. and Grance, T. (2011), definición aceptada por la comunidad científica y

3 Vease nota periodística comentando Acuerdo SYJ Rio Negro que dispuso resguardar evidencia digital en la nube relacionada a causas penales. civiles, laborales y de familia https://www.adnrionegro.com.ar/2019/07/es-evidencia-la-prueba-digital-almacenada-en-la-nube/

perteneciente a una agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos (NIST) Instituto Nacional de Estándares y Tecnología.

En la Guía de obtención, preservación y tratamiento de evidencia digital (Conf.: Res 756/16 P.G. Nación), este tipo de evidencia se define como: "conjunto de datos e información, relevantes para una investigación, que se encuentra almacenada en o es transmitida por una computadora o dispositivo electrónico. Una de las características de la evidencia digital es su volatilidad. Esto conlleva a que la misma, por su propia naturaleza, sea frágil, fácil de alterar y dañar o directamente de destruir".

También entra en juego, como evidencia digital, la dirección IP, por cuanto, antes de proceder al cotejo de dicha dirección, es necesario un análisis forense, que consistirá en focalizarse sobre los ficheros de log[4] de los sistemas atacados o mediante los que se ha cometido el delito.(Amarillo Rubio, 2015).

Por lo expuesto se puede ver que existe una tensión y límites entre la investigación digital y los Derechos Constitucionales. Se afirma, que ninguna actividad desplegada por los órganos estatales encargados de la persecución penal es absoluta, en el sentido de que siempre debe encuadrarse dentro de los límites que fija la Constitución de la Nación Argentina, como garantía para las personas que habitan este suelo. (Autores, 2019). Esto se fundamenta en que ningún derecho es absoluto. Las normas iusfundamentales tutelan aspectos de la vida humana indispensables para un desarrollo digno de la personalidad. Por esa razón, una vez establecidas en la Constitución, se deben respetar (Juan Cianciardo, 2001).

También en el derecho argentino como en el español "la validez de cualquier prueba está sometida a la condición de no afectar los derechos y libertades de los ciudadanos que se concretan, en esta materia, en el art. 18 de la Constitución cuando establece la garantía del: "1. (...) derecho al honor, a la intimidad personal y familiar y a la propia imagen. 2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en el sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito. 3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial. 4. La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos" (Puig Faura S., 2014).

Son los jueces, quienes van perfilando con sus fallos en cada caso la línea de lo que se considera legítima intromisión a la privacidad y datos de los ciudadanos. En este sentido, respecto del uso de imágenes obtenidas de Facebook considerando el perfil público de la página, fallo Bejarano[5]; o que esas imágenes están destinadas a la difusión y exhibición, ver

[4] Archivos de registro (o archivos de log): son archivos que registra todas las actividades de un sistema informático, contienen mensajes sobre el sistema, incluyendo el kernel, los servicios y las aplicaciones que se ejecutan en dicho sistema.

[5] Cámara Federal de Casación Penal, Sala IV. Registro Nº 2328/15.4. Causa Nº 17200/2013. Bejarano, Alexis E.. 4 de diciembre de 2015. https://www.cij.gov.ar/nota-19281-La-C-mara-Federal-de-Casaci-n-Penal-confirma-condena-por-homicidio-cometido-con-alevos-a.html

comentario fallo Rambaldi[6]; o diferenciando entre mail privado y laboral, cediendo este último, el derecho a la intimidad del trabajador (Nievas L., 2017), siempre permitiendo el aporte y valorando esta particular evidencia, en dos etapas, la de permitir su introducción a la causa y la de merituar la prueba científica. Bajo la premisa de atender a la ley de Datos Personales Nº 25326, la cual en su artículo 20 (Impugnación de valoraciones personales), establece que: "las decisiones judiciales o los actos administrativos que impliquen apreciación o valoración de conductas humanas, no podrán tener como único fundamento el resultado del tratamiento informatizado de datos personales que suministren una definición del perfil o personalidad del interesado, y además, agrega que los actos que resulten contrarios a la disposición precedente serán insanablemente nulos".

El tema no es menor ya se citan casos policiales como el de la policía local de Gainesville (EEUU), que involucraron a un ciudadano, Zachary McCoy[7], que paso tres veces con su bici por delante de la casa asaltada a lo largo de una hora y con su celular configurado a una cuenta Google de la app RunKeeper[8] (para seguimiento deportivo). Esto fue suficiente para ser considerado sospechoso y mediante una orden de registro de geofencing (geovallado)[9] emitida por un juez se solicitaron sus datos privados.

Las naciones del viejo continente persiguen el objetivo de concreto de fomentar la cooperación internacional global en materia de lucha contra la ciberdelincuencia, y más recientemente con el Plan de Estocolmo (Ortiz Pradillo J. C., 2013), en el que la Unión Europea ha retomado la tarea de impulsar importantes medidas a adoptar frente a la ciberdelincuencia, y ha dado lugar a la creación del Centro Europeo de Ciberdelincuencia (EC3) en la Oficina Europea de Policía, Europol, en La Haya. Habiéndose también adherido también al Convenio de Budapest (2001).

En la práctica una investigación forense debe superar el estándar fijado por la Corte Suprema Estadounidense en el caso Katz (1967) que refiere a una "expectativa razonable de privacidad"[10], y se formulan reparos constitucionales entre otras medidas a -por ejemplo- la prueba consistente en grabar las conversaciones ambientales directas o "vigilancia acústica".

6 Tribunal de Casación Ciudad de Buenos Aires, Sala 1. [TCPBA]. Causa Nº 67393. Rambaldi German L s/recurso de Casación. 9 de abril de 2015. http://www.pensamientopenal.com.ar/system/files/2018/12/doctrina47272.pdf

7 Merino, Marcos (9 Marzo 2020). Datos de localización cedidos por Google a la policía señalaron como sospechoso a un ciclista sólo por pasar frente a una casa robada. https://www.genbeta.com/seguridad/datos-localizacion-cedidos-google-a-policia-senalaron-como-sospechoso-a-ciclista-solo-pasar-frente-a-casa-robada

8 ASICS Digital, Inc. (2021) RunKeeper - GPS Correr Caminar. [Aplicación móvil]. Google Play. https://play.google.com/store/apps/details?id=com.fitnesskeeper.runkeeper.pro&hl=es_AR&gl=US

9 Las órdenes de registro de geovallas son solicitudes de la policía para obtener información general de todos los usuarios de dispositivos móviles en una ubicación específica en un momento determinado. (https://en-m-wikipedia-org.translate.goog/wiki/Geo-fence_warrant?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es-419&_x_tr_pto=ajax,sc) Las órdenes de registro que utilizan datos de ubicación de terceros se utilizan a menudo en investigaciones penales federales. A menudo se les pide que identifiquen a posibles sospechosos o testigos de delitos. Con las órdenes de geolocalización, es probable que los usuarios inocentes no sepan que la información de su ubicación privada se comparte con el gobierno. https://www.pagepate.com/geofence-warrant/

10 Suprema Corte de Estados Unidos Debido Proceso Penal. Prueba. Admisibilidad. Allanamientos y Registros. Derecho a la Intimidad. United States v. Jones; 23 de enero de 2012. https://www.csjn.gov.ar/dbre/Sentencias/usJones.html

La aplicación de mecanismos formales (rogatorias/exhortos) e informales entre gobiernos de diferentes países y/o empresas privadas con motivo del tránsito o desplazamiento de información en formato electrónico se rige por acuerdos o convenios entre naciones cuando existen, o se acude a los principios de reciprocidad o buenos oficios. Siendo menos formal cuando se trata de hacer circular datos cuyo hosting sea una empresa privada.

El derecho penal sustantivo está pensado con barreras soberanas en los límites del estado, pero como la informática no conoce fronteras, el derecho procesal debe flexibilizar y agilizar sus medidas, ya que además con el advenimiento del cloud computing, ciertamente ocurrirá con frecuencia que se ignore en qué país está realmente el servidor que posee los datos que la investigación requiere. Estas solicitudes de datos tanto a gobiernos como a empresas privadas se deben dinamizar y ser creativas. Otorgando soluciones modernas que tengan en cuenta el balance necesario entre la "eficiencia en la investigación de los delitos" y la necesidad de "protección de las garantías procesales en el mundo digital". Especial atención deberá darse a la hora de buscar soluciones al derecho a la intimidad de los ciudadanos (estándares de protección de datos personales) y el derecho a la libertad de expresión, pilares básicos de la sociedad democrática, que pueden verse afectados seriamente por normas sin un adecuado balance de los principios en juego. (Salt M., 2013)

Investigación y medidas procesales

Frente a una situación concreta de investigación judicial, en la cual contamos con indicios suficientes como para requerir el acceso a esa información alojada en servidores ubicados fuera de las fronteras de nuestro país. Debemos considerar –prima facie- que tipo de medida de prueba es la más adecuada para solicitar en cada etapa del proceso, sin perjuicio de que al avanzar la causa se puedan incorporar nuevas probanzas ampliando la solicitud de datos a circunstancias (nuevos sospechosos involucrados) más puntuales. Entre las medidas disponibles están regladas las de: el aseguramiento de datos, o el informe u orden de presentación de datos, o su registro y secuestro, hasta llegar a la interceptación o recopilación en tiempo real de datos.

La medida del aseguramiento o conservación rápida de datos consiste en ordenar a los titulares o administradores de sistemas informáticos donde se hayan alojados datos informáticos de utilidad en la investigación, que los preserven por un tiempo determinado (de hasta 90 días renovable) para evitar que sean borrados o alterados (Ley 27411, 2018). Conceptualmente prevista en el Convenio de Budapest Título 2 Artículo 16 - Conservación Inmediata de datos informáticos almacenados.

El requerimiento de informe u orden de presentación de datos es la medida por la cual se dispone a ordenar a los proveedores de servicios de internet o los titulares de cualquier sistema de alojamiento de información en formato digital que entregue o informe datos

que estén en su poder o bajo su control relacionado al abonado.

En el art 18, título 3 sobre Mandato de comunicación dentro de la sección 2da. Derecho Procesal del Convenio de Budapest, la expresión "datos relativos a los abonados" designa cualquier información, expresada en datos informáticos o de cualquier otro modo, poseída por un prestador de servicio y que se refiere a los abonados de sus servicios, así como a los datos de tráfico o relativos al contenido. Lo que se refiere a los datos almacenados o existentes en un momento determinado y, por lo tanto, excluye a los datos de tráfico o contenido todavía no generados que implican supuestos de intercepción de datos, así lo plantea Sergi N. (2018) en su Análisis jurídico situación evidencia digital en proceso penal en Argentina.

El registro y secuestro de datos informáticos: tiende a habilitar, en el marco de una investigación penal concreta, el registro de dispositivos o sistemas informáticos con el fin de copiar o secuestrar "datos" que puedan resultar útiles y pertinentes para el objeto procesal. (Salt M., 2017)

La recopilación en tiempo real de datos informáticos (interceptación) es la medida por la cual ante delitos graves se procura:

a) grabar datos de tráfico utilizando medios técnicos en tiempo real, o

b) interceptar datos relativos al contenido de una comunicación específica.

En ambos supuestos se complementa la medida con el requerimiento a fin de asegurar que el prestador de servicios se obligue a mantener en secreto la orden (Convenio Budapest, Titulo 4 y 5).

Estas medidas basadas en la cooperación entre países sitúan a la Convención de Budapest como el primer texto normativo internacional vinculante que logra plasmar situaciones de acceso transfronterizo de datos. (Sergi N. 2018) Aunque no todos los caminos para obtener información (datos) almacenada en otros países requieren autorización de las naciones. También la misma convención prevé una suerte de excepción al principio de territorialidad y necesaria autorización del estado dentro de cuyas fronteras están los servidores que alojan datos. Se refiere al caso de las fuentes abiertas.

En efecto, cualquier Estado podrá sin autorización de otro, acceder a los datos informáticos almacenados de libre acceso público (código abierto), independientemente de la localización geográfica de esos datos. Asimismo, se podrá acceder a los datos almacenados en otro estado si se obtiene el consentimiento legal y voluntario de la persona autorizada para divulgarlos. Previsto en el Título 2 sobre Asistencia en relación con los poderes de investigación, apartado a y b del Art.32, Acceso transfronterizo, del Convenio Budapest.

Se entiende como datos de fuentes abiertas, a toda la información disponible -usando internet- de una persona, grupo, empresa, sociedad, etc. Datos a los cuales se accede utilizando fuentes de acceso público como redes sociales, buscadores, foros, fotografías, wikis, bibliotecas online, conferencias, metadatos, etc. Se ha desarrollado aspectos

vinculados a fuentes abiertas y su vinculación con las herramientas de Open Source Intelligence (Osint) referidas a programas que buscan información personal como: http://www.pipl.com y http://www.peekyou.com, OSint framework, Online Internet Search Tool, Tinfoleak, Shodan, Kismet, Xerosploit, Maltego CE, What´s their ip, HashCheck, Osint –Spy, entre otras (Autores, S. M., 2020).

Acceso transfronterizo: NCMEC y los informes del CyberTipline

Los acuerdos para persecución de actividades ilícitas vinculadas a niños utilizando internet celebrados entre organismos públicos y recientemente la Ley N° 27.411, de adhesión al Convenio de Budapest[11] han posibilitado la obtención de datos almacenados y en tráfico de red por jurisdicciones pertenecientes a múltiples países. En el marco de estos convenios se disponen procedimientos específicos para obtener informes, aseguramiento, secuestro y recopilación transfronteriza. En nuestro país -aproximadamente desde el año 2013- instituciones de la órbita judicial, como el Ministerio Público Fiscal de la Ciudad Autónoma de Buenos Aires, resolución FG Nº 435 de 2013, el Ministerio Publico de Defensa y Fiscal de la Nación, mediante la Unidad Fiscal Especializada en Ciberdelincuencia[12], creada por Resolución PGN N°3743/15, y otras instituciones, suscribieron convenios con el Centro Nacional para Niños Desaparecidos y Víctimas de Explotación Sexual (NCMEC por sus siglas en inglés) a fin de perseguir delitos relacionados con la explotación de menores. Este centro es una ONG estadounidense que suscribió acuerdos con las fuerzas de seguridad de Estados Unidos y con las principales empresas de Internet (por ejemplo: Google, Facebook, Snapchat) a fin de monitorear el contenido que circula por la web y detectar potenciales situaciones de pedofilia. Para esta observación de tráfico de red se utiliza inteligencia artificial y sistemas expertos como el “PhotoDNA” para detectar huellas de imágenes previamente identificadas con un código numérico único obtenido por hash, generándose a partir de allí reportes conteniendo las IP vinculadas al tráfico potencialmente ilícito[13]. Argentina puede acceder a esos informes desde por un punto de contacto vinculado remotamente al website www.cybertipline.com[14].

11 Art. 35 Red 24/7 contacto las 24 hs y los 7 días de la semana.

12 Punto contacto con (IberREd), con red Asoc Iberoamericana de M P (CiberRed) y punto contacto red de crímenes alta tecnología Grupo del G7 24/7 Network of High Tech Crime.

13 Ampliar en: OEA, documento elaborado por Albert Rees de la Sección de Delitos Informáticos y Propiedad Intelectual División de lo Penal, para el Departamento de Justicia de los Estados Unidos, http://www.oas.org/juridico/spanish/cyb20_network_sp.pdf. CyberTipline del NCMEC, sistema centralizado para denunciar la explotación infantil en línea, https://esp.missingkids.org/gethelpnow/cybertipline. ONG que desarrolla tecnología cívica abierta y defiende los derechos digitales por una Cultura Libre en Internet, https://www.tedic.org/pornografia-infantil-como-se-obtiene-este-tipo-de-evidencia-en-internet/

14 Ampliar en: documento La línea para Ciber-Tips: Su fuente para Reportar la Explotacion Sexual de Menores, http://centerforthemissing.org/wp-content/uploads/dlm_uploads/2017/02/CyberTipline-Spanish.pdf. Noticia diario digital El Tiempo, https://www.eltiempo.com/tecnosfera/novedades-tecnologia/facebook-abre-en-codigo-abierto-su-tecnologia-para-detectar-contenido-nocivo-396526.

Requerimiento de datos a principales redes sociales

En cada investigación las autoridades judiciales determinaran las necesidades de información digital a pedir de manera directa como datos registrales o los logs de conexión. Resultando habitual diferenciar entre:

a) datos del usuario de la red social (por ej. Facebook) con mención de la URL (dirección);

b) datos sobre Registro de Información Transaccional;

c) registro de direcciones IP utilizadas para el acceso, con indicación de las fechas y horas pertinentes; d) información registrada del usuario en cuestión;

e) abonado telefónico registrado por el usuario;

f) información de la empresa que valido el correo electrónico a fin de que aporte la información de registración y conexión de esa cuenta de correo (por ejemplo xxxxxxx@hotmail.com) para que una vez recibida la respuesta se oficie a las empresas proveedores de acceso a internet que correspondan que brinden los datos de las asignaciones de las direcciones IP que de ella resulten.

Esta solicitud de datos se debe efectuar por un Magistrado Judicial, a fin de que no se generen incidentes o planteos de nulidad entre la defensa técnica y las atribuciones del Ministerio Fiscal[15].

Las redes sociales de mayor trascendencia pública exponen en sus sitios un conjunto de reglas pensadas para las fuerzas del orden, litigantes en materia civil, acusados en materia penal y simples usuarios, estos últimos pueden descargar su propia información desde la configuración de su cuenta.

En este sentido resultan similares las modalidades sobre requerimientos de las empresas Facebook, Instagram y Messenger ya que comparten infraestructura, sistemas y tecnología con otras empresas de Facebook (incluidas WhatsApp y Oculus). En Twitter la situación es distinta, dada la naturaleza de la actividad de Twitter en tiempo real, la información (p. ej., los registros de IP) solo se almacenan durante un periodo breve. Y además se permite que el usuario cree perfil ficticio, dado que esta red social no se exige el uso de un nombre real, ni la verificación del correo electrónico, ni la autenticación de la identidad del usuario.

Las redes distinguen entre pedidos de datos efectuados en procesos jurídicos, dentro de USA e internacionales. El primero se rige por la ley federal estadounidense de almacenamiento de datos (Stored Communications Act, "SCA"), U.S.C. 18, artículos 2701-2712. Los demás requerimientos deben superar el criterio de la empresa sobre la orden judicial coherentes con estándares reconocidos internacionalmente.

Las medidas que formalmente se aceptan son: la conservación (congelamiento) de datos durante 90 días, efectuadas por medio del sistema de solicitudes por internet. Aunque en el

15 Vease Diario Judicial Online Nulidad oficio Fuero Contravencional Ciudad Bs As., https://www.diariojudicial.com/resultados/?q=documentos%20geolocalizaci%C3%B3n%202018

caso de Instagram, dicha red no almacena información, salvo requerimiento formal. Los requerimientos urgentes, de envío de informes, en casos de daño inminente a un menor o riesgo de muerte o lesiones físicas graves a personas, pueden solicitarse también a través del sistema de requerimientos juridicos por internet (https://legalrequests.twitter.com/forms/landing_disclaimer).

Básicamente el modelo de solicitud debe contener: datos identificados con la mayor precisión posible, por ejemplo: Dirección de correo electrónico, número de teléfono, número de identificación de usuario. Nombre de la autoridad requirente, su correo electrónico institucional y teléfono de contacto directo. Atendiendo a que es política de las empresas es notificar a los usuarios cuando se solicita información sobre su cuenta, se debe agregar a la solicitud la prohibición de notificación al usuario de la red.

Por cierto, cada semestre Google, Apple y Microsoft dan a conocer el Informe de Transparencia, que contiene las "solicitudes que les hacen jueces y policías sobre datos de usuarios. Sin embargo, están obligados a callar, por la Ley Patriot (2001), si hay solicitudes de los servicios de inteligencia de EE UU"[16].

La vía diplomática

Para que un requerimiento llegue a destino, se debe seguir el camino de la vía diplomática. No obstante, como una buena práctica, se recomienda seguir todas las vías, utilizando medidas conjuntas o en paralelo, solicitando -por ejemplo- la información del suscriptor por oficio a la red social y la de contenido por exhorto. En este punto se abren dos opciones:

a) Si el país donde está alojada la información digital, tiene suscripto tratado con la República Argentina, entonces esta normativa "se aplicará al trámite de colaboración. Argentina, celebró tratados con Rusia, países integrantes de la OEA (Ley 26139), Mercosur (Ley 25095) Chile y Bolivia (Ley 26004 - Acuerdo de Asistencia Mutua en Asuntos Penales del MERCOSUR) Sudáfrica (Ley 27018) Corea y Túnez (Leyes 26782 y 26611) y Suiza (Ley 26781)" entre otros[17].

b) De lo contrario estamos en otro supuesto, que es la opción para cuando nuestro país no tiene firmado convenio de colaboración en materia penal. En la cual se aplica la Ley N° 24767 (1997) de Cooperación Internacional en Materia Penal, referentes a principios rectores en materia de extradición y aseguramiento de prueba relacionada con el delito, la cual establece un procedimiento diplomático para efectuar estas peticiones a otros estados con los cuales no existen tratados vinculantes en materia penal.

Si la materia no penal, es decir, alcanza competencias de fueros como el civil y comercial, laboral, familia, o de género. En estos litigios, también tenemos opciones diplomáticas,

16 Castelo, V.. (13 NOV 2013). Buscando un guardián para la nube. El Pais. https://elpais.com/sociedad/2013/11/14/actualidad/1384383731_820058.html

17 Véase Listado de Tratados en la página https://www.mpf.gob.ar/cooperacion-ai/normativa/

según se tenga o no tratado con el país de hosting. Es posible hallar prueba informática, alojada en el extranjero. Podemos estar ante un ofrecimiento probatorio digital, que se solicite, por ejemplo, como prueba anticipada o como medida cautelar innominada. El Código Procesal Civil y Comercial de Santiago del Estero, (2017) establece ciertos supuestos para que en una Diligencia Preliminar (Art. 330) pueda solicitarse anticipadamente una prueba, así en su inc. 2 puede leerse "dictamen pericial para hacer constar la existencia de documentos" esta posibilidad quizá sirva para abrir la puerta a la pericia informática y en consecuencia activar la preservación y posterior requerimiento de datos con servicios de hosting en el extranjero. Relacionando también el juego interpretativo con la expresión del inc. 4 del citado artículo, que refiere al "resguardo o secuestro de documentos" los que válidamente pueden tener formato digital. En el mismo sentido la normativa procesal de la Nación (CPCCN) y la de la provincia de Córdoba (art. 486). Chialvo Tomás Pedro (2009).

La perspectiva del registro y secuestro de datos en las jurisdicciones locales

En nuestro derecho interno, si bien en la mayoría de los códigos de procedimiento –hasta el presente- no se contemplan todavía disposiciones referidas a recolección y análisis de medios electrónicos, la realidad es que se acude a la analogía con las probanzas materiales. Cada vez, más normas procesales incorporan disposiciones sobre prueba digital en general y en particular, por ejemplo, el Código Procesal Penal de Provincia de Neuquén, refiere al secuestro de información digital, su copia, la conservación por 90 días, y la posibilidad del registro del dispositivo por medios técnicos y en forma remota. Ley Nacional N° 27063, que sanciona el Código Procesal Penal Federal, el cual se aplicara en forma progresiva en el país, incorpora en sus artículos 143/144, la interceptación y secuestro de correspondencia electrónica, contempla el deber de confidencialidad y secreto de la medida para funcionarios y empresas que brinden servicios de comunicación, contemplando la incautación de datos, registro, obtención de copias y su preservación. Y más recientemente La Pampa (10/01/2020) en su nuevo Código Procesal Penal (Ley 3192) dispone sobre registro de dispositivos en forma remota, secuestro, obtención de copias forenses o reproducciones, incluyendo la posibilidad de requerir la entrega de información (datos) de abonados a cualquier persona física o jurídica que preste un servicio a distancia por vía electrónica.

Extracción de las evidencias

La extracción de las evidencias se puede realizar de dos maneras, dependiendo de si las herramientas empleadas permiten o no el acceso remoto a la memoria del sistema a analizar. "En el caso de las herramientas de adquisición remota, éstas tienen la capacidad de

acceder al sistema en la nube utilizando un agende desplegado o mediante una conexión remota, y realizan la adquisición completa de todas las evidencias forenses". En el caso de herramientas de adquisición que no permitan el acceso remoto, debe obtenerse una imagen, preferentemente una captura del sistema (snapshot) "esta opción ofrece mayores garantías de integridad de las evidencias adquiridas y generalmente no provoca modificaciones en la información dentro del sistema. En caso de que no sea posible obtener una snapshot, existen métodos alternativos que implican la creación de discos virtuales secundarios montados en modo solo lectura en los que se vuelque toda la información". (Castaño Delgado P., Blanco Arenas B. Robles del Amo I., Sanz Alcober A., 2018)

Buenas prácticas

Entre las propuestas que la doctrina esboza, nos parece razonable plantear como sugerencias mínimas alguna secuencia o alternativa de pasos para una correcta incorporación de evidencia electrónica.

Es una formulación que pretende servir de guía dinámica para orientar al perito y a los operadores del sistema judicial, ya sea fuerzas policiales de seguridad, miembros del Ministerio Público, Magistrados y todos aquellos vinculados funcionalmente con la temática de la prueba digital científica.

La construcción que se formula es una primera aproximación a una guía de buenas prácticas para obtener evidencia en el extranjero, la cual versa sobre la comparación y respeto, a los instrumentos vigentes en materia internacional, a tono con la Ley Nacional N° 27411 de adhesión al Convenio de Budapest y al Convenio Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de Prueba en materia de Ciberdelincuencia, suscripto por Argentina.

- Propiciar desde el primer momento de la tarea investigativa se incluya información proveniente de los denominados datos de fuentes abiertas, independientemente de la localización geográfica de estos.

- Paralelamente se debería avanzar en la obtención del consentimiento legal y voluntario de la persona autorizada para divulgar otros datos, de acuerdo a lo estipulado por el Título 2, Art.32 del Convenio Budapest.

- Si la hipótesis trabajada se relaciona con legislación de los Estados Unidos de América, debe recordar que allá, los registros se clasifican por la mayor o menor invasión a la privacidad del usuario. Es decir, "a mayor intrusión se requiere satisfacer, más altos estándares para obtener la información. Distinguimos tres grupos de información: básica, transaccional y de contenido. La importancia de la clasificación previa radica en que el canal que deba utilizarse dependerá de la información solicitada", como se indica en la Guía de Buenas Prácticas para obtener Evidencia Electrónica en el Extranjero propuesta por la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI), Dirección General de

Cooperación Regional e Internacional (DIGCRI) de la Procuración General de la Nación (2017).

- Si la vía utilizada es un exhorto, el Departamento de Justicia solicita que previamente, se identifique el lugar donde se encuentra la información.
- Decidida la medida de recolección probatoria en el extranjero, se elige la medida a solicitar que abarca desde: el aseguramiento de datos, o el informe u orden de presentación de datos, o su registro y secuestro, hasta llegar a la interceptación o recopilación en tiempo real de datos. Hipótesis en la cual se observan las reglas procesales referidas en el apartado sobre Acceso transfronterizo: el NCMEC y los informes del CyberTipline, de este documento, siempre planteando en la primera providencia, el requerir la preservación de los datos por un tiempo determinado y renovable a fin de evitar que sean borrados o alterados.
- Si el requerimiento debe hacerse a redes sociales, estas tienen en sus sitios reglas para solicitar información distinguiendo según se trate de fuerzas del orden, litigantes en materia civil, acusados en materia penal y simples usuarios. Agregándose en su caso la solicitud la prohibición de notificación al usuario de la red.
- Es también una práctica atinada el intentar medidas conjuntas o en requerimientos en paralelo, solicitando -por ejemplo- la información del suscriptor por oficio a la red social y la de contenido por exhorto.

Conclusiones

La facilidad de acceso a Internet y el desarrollo del mercado relacionado con los dispositivos móviles que permiten acceder a ella, no sólo permitió el auge del comercio electrónico, sino también la forma en la que los delincuentes cometen sus crímenes. Cada vez más el microcosmos digital se ve involucrado en cuestiones delictivas informáticas. La prueba dentro del proceso penal es de especial importancia, ya que desde ella se confirma o desvirtúa una hipótesis o afirmación precedente, se llega a la posesión de la verdad material

Nos enfrentamos a nuevas modalidades delictivas, dado que en la era de la “Sociedad de la Información” la criminalidad ocupa medios informáticos como Hacking, Phishing, Software malicious, Pharming, Cyber Stalking, Bullying, Piratería de software, Sextorsión, entre otros. Los hechos criminales se preparan en el mundo digital y las comunicaciones entre delincuentes se encriptan para protegerlas de la justicia. En la Deep Web, no solo el ciberterrorismo opera traficando armas, explosivos y otras sustancias peligrosas, sino que se ofrecen toda clase de servicios desde homicidios, trata de personas, divulgación de datos personales, fotos, historial, virus, recetas para atentados químicos, alquileres de servicios criminales, pornografía infantil y otras ofertas que pueden encontrarse si utilizamos navegadores anónimos como Tor, PGP y FreeNet u Orbot.

Investigar digitalmente nos acerca a problemas jurídicos, relacionados con la posible vulneración de derechos personalísimos y garantías de privacidad, reconocidas constitucional y convencionalmente a los ciudadanos de este país.

Con perfil técnico propio dentro del panorama actual, la ciencia informática nos acerca cada vez más herramientas para investigar delitos avanzando sobre garantías constitucionales. Por ello, los procedimientos judiciales resultan aún más complejos cuando conllevan casos que presentan contacto con elementos tecnológicos ubicados fuera del país.

Existen numerosas razones que pueden llevar a cometer errores en la identificación y preservación de potencial evidencia digital en el extranjero, así como también en el aseguramiento de la cadena de custodia. Lo que se agrava cuando además tenemos ausencia de procedimientos formales en jurisdicción santiagueña, y sumamos la dificultad para obtener documentación en lenguaje nativo y claro para exponer conceptos ante directivos de empresas privadas radicadas en el extranjero.

Por lo expuesto, es necesario hacer un esfuerzo para adaptar la situación legal de aspectos como la seguridad y protección de la privacidad entorno a estos sistemas.

Se están investigando y desarrollando mecanismos políticos como guías, códigos de conducta, estándares internacionales e iniciativas auto-reguladoras. Pero conseguir la mezcla correcta de políticas, a tiempo y aun así de una forma duradera y facilitadora, es un todo un reto.

En esta cosmovisión, con el objetivo de identificar todas las operaciones que se realizan para asegurar y recolectar evidencia electrónica alojada en servidores ubicados en el extranjero, independiente que se encuentre bajo la tutela de una persona jurídica estatal o en poder de empresas privadas que operan servicios web; las buenas prácticas descritas procuran homogeneizar lo legal con lo técnico, aportando ciertos criterios de intervención básicos, de carácter eminentemente prácticos, y fundamentados científicamente, a los fines de garantizar la seguridad jurídica y el debido proceso legal.

Bibliografía

Ruan, K., Baggili, I., Carthy, J. y Kechadi, T. (2011). Survey on cloud forensics and critical criteria for cloud forensic capability: A preliminary analysis. In 6th annual conference of the ADFSL Conference on Digital Forensics, Security and Law, Richmond, Virginia, USA.

Mell, P. and Grance, T. (2011). The NIST Definition of Cloud Computing. Special Publication (NIST SP). National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.SP.800-145

Resolución N° 756/16 [Procuración General de la Nación]. Guía de obtención, preservación y tratamiento de evidencia digital. 31 de marzo de 2016. https://www.fiscales.gob.ar/wp-content/uploads/2016/04/PGN-0756-2016-001.pdf

Rubio Amarillo J. (2015). La dirección IP en el Peritaje Informático. Perito Informático Judicial https://peritoinformaticocolegiado.es/?s=direccion+ip.

Autores. (25 y 26 de abril de 2019). Titulo articulo. XXI Workshop de Investigadores en Ciencias de la Computación. Universidad Nacional de San Juan, Argentina.

Juan Cianciardo (2001). Los límites de los derechos constitucionales. Revista Dikaion-Revista de Fundamentación Jurídica. Bogotá. V. 10. Pág. 53. Facultad de Derecho de la Universidad de la Sabana. Id SAIJ: DACF030018. http://www.saij.gob.ar/juan-cianciardo-limites-derechos-constitucionales-dacf030018-2001/123456789-0abc-defg8100-30fcanirtcod

Sonia Puig Faura. (2014). La Prueba Electrónica: sus implicaciones en la seguridad de la empresa. [Tesis de Doctorado, Universitat Ramón Llull]. Repositorio TDX (Tesis Doctorals en Xarxa).
https://www.tesisenred.net/bitstream/handle/10803/285237/TESI%20DOCTORAL%20S%C3%92NIA%20PUIG%20FAURA.pdf?sequence=1&isAllowed=y

Nievas Laura (18 al 20 de septiembre de 2017). Tecnologías de la información y comunicación en el proceso laboral: Comunicación electrónica y derechos personalísimos. V Jornadas de Jóvenes Investigadoras/es en Derecho y Ciencias Sociales. Universidad de Buenos.
https://jornadasdejovenesinvestigadorasesenderechoycienciasblog.files.wordpress.com/2017/11/laura-nievas-tics-en-el-proceso-laboral.pdf

Ley N° 25.326 de 2000. Protección de los datos personales. Octubre 4 de 2000. BO Nº 29517. http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm

Ortiz Pradillo J. C. (2013). La investigación del delito en la era digital. Los derechos fundamentales frente a las nuevas medidas tecnológicas de investigación. https://www.fundacionalternativas.org/public/storage/actividades_descargas/5a687574bb9f245b66286372359596d4.pdf

Convenio sobre la Ciberdelincuencia. Convenio. Budapest, Hungría. 23 de noviembre de 2001. http://servicios.infoleg.gob.ar/infolegInternet/anexos/300000-304999/304798/ley27411.pdf

Salt M. (2013) Nuevos Desafíos de la evidencia digital. El Acceso trasfronterizo de datos en los países de América Latina. Revista de Derecho Penal y Procesal Penal. https://docplayer.es/691269-Nuevos-desafios-de-la-evidencia-digital-el-acceso-trasfronterizo-de-datos-en-los-marcos-salt-2.html#show_full_text

Sergi Natalia (2018) Análisis jurídico situación evidencia digital en proceso penal en Argentina. Área Digital Asociación por los Derechos Civiles (ADC). https://adc.org.ar/wp-content/uploads/2019/06/038-analisis-juridico-de-la-situacion-de-la-evidencia-digital-en-el-proceso-penal-en-argentina-vol-3-04-2018.pdf

Salt M. (2017) Nuevos Desafíos de la evidencia digital. El Acceso trasfronterizo de datos en los países de América Latina. Revista de Derecho Penal y Procesal Penal.

Autores (7 y 8 de mayo de 2020). Título Artículo. XXII Workshop de Investigadores en Ciencias de la Computación. WICC 2020. Universidad Nacional de la Patagonia Austral (UNPA), El Calafate, Santa Cruz, Argentina.

Ley N° 24767 de 1997. Ley de Cooperación Internacional en materia Penal. BO Nº 28565. http://servicios.infoleg.gob.ar/infolegInternet/anexos/40000-44999/41442/norma.htm

Código Procesal Civil y Comercial de Santiago del Estero [CPCC]. Ley 6910 de 2017. 28 de agosto de 2017 (Argentina). https://www.jussantiago.gov.ar/jusnueva/Normativa/2017-Ley6910-CgoProcCivilyCom-Modificacion-28-08-2017.pdf

Chialvo Tomás Pedro (2009). La prueba anticipada en el proceso de daños y su correspondencia con la historia clínica. http://www.saij.gob.ar/tomas-pedro-chialvo-prueba-anticipada-proceso-danos-su-correspondencia-historia-clinica-dacf090044-2009-07/123456789-0abc-defg4400-90fcanirtcod

Código Procesal Penal Neuquén [CPP]. Ley 2784 de 2017. Mayo de 2017 (Argentina). http://200.70.33.130/images2/Biblioteca/2784-TO-NoOficial.pdf

Código Procesal Penal Federal [CPPF]. Ley 27063 de 2017. 10 de diciembre de 2014 (Argentina). http://servicios.infoleg.gob.ar/infolegInternet/anexos/235000-239999/239340/texact.htm

Código Procesal Penal La Pampa. Ley 3192 de 2020. 10 de enero de 2020 (Argentina). https://justicia.lapampa.gob.ar/images/Sep3396.pdf

Castaño Delgado P., Blanco Arenas B. Robles del Amo I., Sanz Alcober A.. (2018) Cloud Audit & Forensics

https://www.ismsforum.es/ficheros/descargas/cloudauditforensics2018v41544463021.pdf

Unidad Fiscal Especializada en Ciberdelincuencia (UFECI), Dirección General de Cooperación Regional e Internacional (DIGCRI) de la Procuración General de la Nación. (2017). Guía de Buenas Prácticas para obtener Evidencia Electrónica en el extranjero. https://www.fiscales.gob.ar/wp-content/uploads/2017/01/Gu%C3%ADa-de-Buenas-Pr%C3%A1cticas-para-Obtener-Evidencia-Electr%C3%B3nica-en-el-Extranjero.pdf