Daniela Dupuy

Doctora en Derecho Penal y Procesal Penal Universidad de Sevilla, España. Fiscal Coordinadora Unidad Fiscal Especializada en Delitos y Contravenciones Informáticas de la Ciudad Autónoma de Buenos Aires. Directora del Observatorio Cibercrimen y Evidencia Digital en Investigaciones Criminales (OCEDIC) de la Universidad Austral. Directora de la Diplomatura Internacional en Ciberdelincuencia de la Universidad Austral

Litigación & cibercrimen

I. Introducción

En un mundo cada vez más digitalizado, donde las posibilidades para cometer delitos en el ciberespacio se encuentran facilitadas por herramientas disruptivas al alcance inmediato de los ciberdelincuentes, existen dos desafíos fundamentales: 1) la utilización de medios de investigación innovadores para enfrentar el fenómeno de la cibercriminalidad y contrarrestar sus consecuencias sin afectar derechos fundamentales y garantías constitucionales; 2) llevar los casos a juicio luego de efectuar una investigación en la que los autores actúan en el ciberespacio y la evidencia recolectada es digital, electrónica.

En América Latina se inició un proceso profundo de transformación de los sistemas de justicia criminal de tipo acusatorio, siguiendo el modelo que se ha consolidado en Europa continental a partir de la segunda mitad del siglo XX. Sus principales características han sido establecer el juicio oral y público como elemento central del proceso; la diferenciación de roles entre jueces y fiscales; la entrega de algunas facultades discrecionales limitadas a los fiscales para poner fin anticipadamente a la persecución penal; el reconocimiento de las víctimas y de las garantías básicas del debido proceso a favor de las personas objeto de persecución penal[1].

El derecho penal y procesal clásicos se han construido sobre la base de un modelo de delincuencia física e individual. Hoy, la dinámica del cibercrimen y su constante evolución ha propiciado que delincuentes que hace poco actuaban de manera aislada, sin coordinación, con alcance local, en la actualidad formen parte de organizaciones transnacionales complejas. De hecho, la aparición de la informática, de Internet y ahora de las tecnologías disruptivas[2], ha resquebrajado aquel paradigma tradicional, al mismo tiempo que los organismos encargados de su persecución se han ido enfrentando a una forma de ejecución penal cuyos principios para la investigación penal se tornan desafiantes.

1 Duce, Mauricio, *La prueba pericial*, Colección Litigación y enjuiciamiento penal adversarial. Editorial Didot, Buenos Aires, 2015, p. 25.

2 Christensen fue el creador de la expresión *disruptive technologies* en 1997 para referirse a aquellas tecnologías que exigen un cambio radical respecto del pasado para iniciar una nueva etapa. Se trata de tecnologías rupturistas, y no de forma gradual, como el *blockchain*, la robótica, la inteligencia artificial, el *cloud computing*, el *big data*, las *smart cities*, la impresión 3D, los coches autónomos, cit. Barrio, Andrés, Moisés. (2020). *Ciberdelitos 2.0. Amenazas criminales del ciberespacio.* 2ª edición actualizada y ampliada, Astrea, Buenos Aires, p. 4.

Una de las características fundamentales de la evidencia digital, y que la distingue de la prueba física, es su volatilidad; su lógica es diferente, siendo de vital importancia su preservación, extracción, análisis y presentación en el marco de una investigación penal.

En ese sentido, el tiempo es su peor enemigo: entre que el hecho se comete en entornos digitales, se descubre el acto delictivo y es entregado a las autoridades competentes para su correspondiente investigación, es factible que la evidencia digital, cuando sea necesaria, se haya borrado.

En efecto, en este escenario, aparece el sector privado como un nuevo actor. Las *ISP*[3] como *Microsoft, Facebook, Yahoo, Twitter, TikTok,* entre otras, tienen en su poder la información básica y necesaria de los usuarios, indispensable para identificar a quienes infringen la norma penal y eventualmente atribuirles responsabilidades.

Sin embargo, no existe legislación alguna que obligue a las empresas prestatarias de servicio de Internet a guardar, por un tiempo específico y determinado, la información referida a los datos de tráfico o de contenido de los usuarios sospechosos.

La necesidad de que sea obligatorio para las *ISP* que la información sea almacenada durante cierto tiempo, tiene como fin evitar que aquellos datos sean borrados y, en consecuencia, no se cuente con ellos como evidencia en el marco de una investigación. No obstante, en la actualidad, es costumbre internacional que los requerimientos judiciales se efectúen a través de las plataformas oficiales *online* de las empresas y éstas suministran voluntariamente la información de sus clientes sometidos a una investigación criminal; cada una bajo sus propias políticas, pero de una manera más ágil si se compara con los trámites tradicionales que demandan los Tratados de Asistencia Mutua de Cooperación Internacional en materia penal.

Otra importante particularidad del fenómeno digital es la transnacionalidad, la ubicuidad: el autor del hecho puede encontrarse en un lugar, las víctimas distribuidas en diferentes países y la evidencia digital que se necesita para comprobar uno de los aspectos de la teoría del caso de cualquiera de las partes, puede estar alojada en un servidor en otra ciudad, o bien los datos pueden estar fragmentados y ubicados en diferentes servidores en varios Estados[4].

En este sentido, los límites o fronteras se vuelven difusos entre la comisión del evento delictivo y su resultado, debilitándose el tradicional principio de territorialidad y soberanía nacional[5]. En razón de ello, es destacable la relevancia de profundizar los mecanismos de cooperación internacional entre los Estados.

A los desafíos señalados, debo agregar una carencia legislativa procesal en la República Argentina y en la mayoría de los países de la región, en cuanto a la regulación de la recolección y valoración de la evidencia digital en el sistema procesal penal, y de los medios de investigación modernos adaptados a las nuevas tecnologías. Ello conlleva a la aplicación sistemática del principio de libertad probatoria, debiendo adaptar analógicamente las normas

3 *Internet Service Provider.*

4 La solución puede encontrarse determinando en qué lugar se entiende cometido el hecho. Hay tres teorías: 1) la teoría de la *actividad:* el delito se entiende cometido donde el sujeto lleva a cabo externamente la conducta delictiva; 2) la teoría del *resultado:* el delito se perpetra donde tiene lugar el resultado; y 3) la teoría de la *ubicuidad:* el delito se entiende cometido donde se lleva a cabo la actividad o se manifiesta el resultado. La última tiene mayor aceptación en derecho comparado (9.1 del Código Penal alemán; TS España sala 2, del 30/11/2017)

5 Para mayor información, Dupuy, Daniela, Kiefer Mariana. (2018). La Nueva Ley "Cloud Act: su impacto en investigaciones en entornos Digitales. En *"Cibercrimen II, Nuevas conductas penales y contravencionales. Inteligencia Artificial aplicada al Derecho penal y procesal penal.* Dir. Dupuy, D, coord. Kiefer,M. BdeF, Buenos Aires, p.357 y ss.

previstas para la recolección de prueba física en investigaciones que requieren de evidencia digital, con la posibilidad de poner en riesgo garantías constitucionales tradicionales, que amerita una nueva interpretación y redefinición a la luz de las nuevas herramientas tecnológicas[6].

En consecuencia, en la actualidad, el fenómeno de la ciberdelincuencia nos enfrenta a retos constantes pues las conductas en el ciberespacio son cada vez más sofisticadas y complejas, como el alojamiento de datos en la nube, la utilización de mecanismos de encriptación o el uso de la *deep web* para asegurar el anonimato de los delincuentes; En este marco, los Estados deben responder técnicamente para mitigar sus efectos nocivos y violatorios de derechos fundamentales de los ciudadanos: intimidad, privacidad, patrimonio, autodeterminación informática, indemnidad sexual, etc.

En efecto, las modalidades delictivas producida en entornos digitales nos enfrenta a retos constantes relacionados, entre otras cosas, con la expectativa de privacidad, sus límites y la búsqueda permanente para encontrar un equilibrio entre la persecución penal del Estado y los derechos fundamentales. A su vez, debemos sumar que en la actualidad es necesaria una regulación específica que trate pautas sobre la creación y uso de los innovadores instrumentos de última tecnología, pues su profundo análisis permitirá concluir si la metodología utilizada para arribar a ciertos resultados probatorios son explicables, trazables y válidos.

En este escenario, de por sí diferente a un ámbito de investigación tradicional, resta analizar su impacto en un mundo adversarial, es decir, cómo se valida y se explica una lógica poco usual de investigación criminal cuyas pruebas deberán exhibirse ante un tribunal y el control estricto de la contraparte.

Este trabajo no tiene como fin transmitir técnicas ni destrezas de litigación pues ya hay mucho escrito por parte de quienes tuve el privilegio de aprender y capacitarme[7]; sino más bien, y sobre la base de mi aprendizaje, delinear algunos aspectos básicos del tratamiento y presentación de la evidencia digital en el juicio oral y la necesidad de demostrar una trazabilidad clara, precisa y concreta del paso a paso de la investigación fiscal, cuya complejidad y particularidad hacen poco sencilla su puesta en escena en las audiencias orales.

II. La investigación digital de cara al juicio oral

Partiendo de la base de un sistema procesal penal moderno, como es el acusatorio ya

6 El principio de libertad probatoria es reconocido por la doctrina mayoritaria y se encuentra previsto expresamente en algunas regulaciones procesales penales argentinas, como el Código Procesal Penal de la Nación –art. 193–, y en los de algunas provincias tales como Córdoba –art. 192– o la Ciudad Autónoma de Buenos Aires –art. 106–. Consiste en la posibilidad de incorporar prueba al proceso penal ya no únicamente por los medios de prueba que se encuentran expresamente regulados, sino también mediante cualquier otro no reglamentado que sea idóneo para contribuir al descubrimiento de la verdad, siempre que no se vulneren garantías constitucionales ni sean contrarios a la ley. Para ello, se deberá buscar el medio de prueba analógicamente más aplicable que sí se encuentre regulado, y se utilizará el procedimiento allí señalado, respetando sus formas y bajo las mismas sanciones. En este sentido, ver Cafferata Nores, José I. – Hairabedián, Maximiliano. *La prueba en el Proceso Penal.* Abeledo-Perrot, Buenos Aires, 6a ed., pp. 49 y ss. Sin embargo, este principio es cuestionado por algunos autores, entre ellos Gabriel Pérez Barberá, quien sostiene que en materia procesal penal también debe regir la protección constitucional amplia de prohibición de analogía de la ley *in malam parte*, ya que incluir por analogía normas procesales que no han sido expresamente previstas genera un perjuicio a la posición del imputado en el proceso. En esta línea, véase Pérez Barberá, Gabriel. (2009). Nuevas Tecnologías y libertad probatoria en el proceso penal. En ponencia llevada a cabo en el *IV Encuentro de Profesores de Derecho Procesal Penal, Salta.*

7 Baytelman, Andrés y Duce Mauricio (2005). *Litigación penal, juicio oral y prueba.* Colecciones de Derecho, Universidad Diego Portales, Chile. Binder, Alberto. (2012). *La implementación de la nueva justicia adversarial.* Ad Hoc, Buenos Aires. *Colección Litigación y enjuiciamiento penal adversarial,* dir. Binder, Alberto, (2014); Cafferata, José y Hairabedian, Maximiliano. (2011). *La prueba en el proceso penal*, Abeledo Perrot, Buenos Aires; Chow, Andrew LT. (2009). *Evidence.* Oxford University Press, Oxford, entre otros.

instalado en muchos países de la región y en provincias argentinas, en el cual las audiencias orales constituyen el método de trabajo central del sistema, la investigación del caso se encuentra en cabeza del fiscal, quien fija una hipótesis o línea de investigación cuya estrategia deberá ser discutida con las fuerzas especializadas, tendientes a corroborar la comisión del hecho e identificar al autor o los autores que intervinieron.

Es fundamental que al recibir los casos, la fiscalía haga una proyección de la investigación de cara al juicio oral. Es decir, que elabore su propia teoría del caso o hipótesis de investigación, con sus fortalezas y debilidades, en concordancia con el área informática, siendo de vital relevancia que, en las investigaciones en entornos digitales, el binomio jurídico-técnico atraviese el caso desde el principio hasta su fin. Por su parte, la defensa hará idéntico trabajo de acuerdo a su propia teoría del caso.

En este sentido, en el ámbito del ciberespacio, los objetivos primarios son los siguientes:

1) Identificar y determinar el hecho denunciado y los posibles autores de acuerdo a la hipótesis del acusador.
2) Resguardar la evidencia digital: la importancia de su inmediato resguardo radica en que se puede perder debido a su carácter volátil –a diferencia de la prueba física-.
3) Proyectar y realizar diferentes medidas de investigación para identificar al usuario sospechoso: requerimientos a *ISP*, orden de presentación, allanamiento, análisis de fuentes abiertas, agente encubierto digital, búsqueda de información en Internet, uso de herramientas informáticas con Inteligencia Artificial para extraer los datos de los dispositivos de almacenamiento informático, etc.

Seguramente con una simple lectura estaremos ampliamente familiarizados con el primer objetivo, pero quizás no tanto con el resto. El motivo se debe a que las medidas de investigación y la lógica que se utiliza para el análisis de la evidencia electrónica, es muy diferente a los casos tradicionales; y ello impacta fuertemente a la hora de generar una estrategia que demuestre la trazabilidad inalterable en las audiencias orales.

Abordemos cada punto.

1) Teoría del caso

La teoría del caso es el conjunto de actividades estratégicas que debe desarrollar un litigante frente a un caso, que le permitirá determinar la versión de los hechos que sostendrá ante el tribunal y la manera más eficiente y eficaz de presentar persuasivamente las argumentaciones y evidencias que la acreditan en un juicio oral[8].

Es decir, la versión de los hechos del litigante que será sostenida ante el tribunal; lo que a su juicio aconteció en un lugar, día hora y personas determinadas, que configurarían la comisión de un ciberdelito.

Ahora bien, en primer lugar, nos encontraremos con un nivel de dificultad inicial en razón del entendimiento acabado que amerita un comportamiento en un espacio virtual.

En segundo lugar, la estrategia ocupa un lugar primordial, pues a diferencia de lo que ocurre con la prueba física, la evidencia digital suele ser de gran magnitud y de complejo análisis, y si no es presentada en juicio de una manera eficaz y clara, arriesgamos confundir al tribunal, y si no se coloca el foco en lo indispensable, el riesgo es perder el caso.

8 Moreno Holman, Leonardo. (2014). *Teoría del caso.* Colección Litigación y enjuiciamiento adversarial. Dir. Binder. A, Ed. Didot, Buenos Aires, p.29.

Tercero, el *lugar* al que hice referencia en párrafos anteriores no se trata de un espacio físico sino virtual y por ende el hecho se pudo haber cometido transnacionalmente y, así, todas las víctimas y victimarios podrían hallarse en diferentes países o ciudades.

Entender esta nueva lógica hará que los litigantes se replanteen la estrategia de la tradicional teoría del caso y, obligatoriamente, deberán mutar a otra que presenta aristas diferentes.

Los puntos que siguen se relacionan con aspectos básicos de las investigaciones en entornos digitales que requieren su correcta comprensión y manejo para así plasmarlo al tribunal mediante los testimonios de testigos y expertos.

2) Resguardo de la evidencia digital

Luego de delinear estratégicamente la teoría del caso, llega el momento de preservar la evidencia digital como requisito urgente y *sine qua non*. Entonces, contaremos con la información que nos ofrece la víctima o, de lo contrario, se deberán arbitrar los medios para individualizar al usuario sospechoso sin la colaboración de la parte denunciante, pues puede carecer de esa información.

Los datos con los que cuenta la víctima es la información que posee en su dispositivo de almacenamiento informático y la pone a disposición de los investigadores para su correcta preservación: chats, mensajes, mails, fotografías o videos recibidos, etc.

El término *preservar* es definido por el diccionario de la Real Academia Española como: proteger, resguardar anticipadamente de alguien o algo de un eventual daño o peligro. Ello significa que con la preservación de la evidencia digital se está previendo que existe la posibilidad de un daño o peligro[9].

A su vez, se debe asegurar la evidencia de forma tal que pueda demostrarse su trazabilidad a lo largo de todo el proceso.

En ese sentido, la información con la que cuenta la víctima en sus dispositivos de almacenamiento digital es de vital importancia para la investigación y, por ello, es fundamental proceder a su correcta preservación y, para ello, los denunciantes deben aportarla inmediatamente, intacta, y sin borrarla total o parcialmente, en razón de que su recuperación se torna dificultosa.

Claro que la forma de preservar esa información variará de acuerdo al medio utilizado para cometer el delito (*Instagram*, *WhatsApp*, *Yahoo, Facebook, Twitter, TikTok*, etc.)[10].

En consecuencia, la información referida permitirá solicitar los datos de tráfico[11]

9 Di Iorio, Ana. (2016). *Protocolos de preservación de evidencia digital y cuestiones forenses*. Cibercrimen II, dir. Dupuy, D., coord. Kiefer. M, BdeF, Buenos Aires, p.335 y ss.

10 Para mayor información al respecto cfr. Dupuy, Daniela, Neme Catalina. (2020). *Acosos en la red.* Vol.I, Hammurabi, Buenos Aires, p. 245 y ss.

11 Por datos relativos al tráfico "se entenderá todos los datos relativos a una comunicación realizada por medio de un sistema informático, generados por este último en tanto que elemento de la cadena de comunicación, y que indique el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente". Definición establecida en el art. 1 "d" del Convenio sobre la Ciberdelincuencia –disponible en www.coe.int-. Estos datos son generados por los ordenadores en la cadena de comunicación con el fin de encaminar una comunicación desde su punto de origen hasta su destino. Por tanto, son datos auxiliares a la comunicación misma. Los datos relativos al tráfico podrían tener sólo una duración efímera, lo que hace necesario ordenar su rápida conservación. La definición establecida en el convenio enumera de forma exhaustiva las categorías de datos relativos al tráfico que quedan comprendidos: el origen de una comunicación, su destino, la ruta, la hora (GMT), la fecha, el tamaño, la duración y el tipo de servicio subyacente. No todas esas categorías estarán siempre disponibles técnicamente, o podrán ser suministradas por un proveedor de servicios, o serán necesarias para una investigación penal en particular. El "origen" se refiere a un número de teléfono, dirección de Protocolo de Internet (IP), o a una identificación similar de una instalación de comunicaciones a la que un proveedor de servicios presta sus servicios. El "destino" se refiere a una indicación comparable de una instalación de comunicaciones a las que se transmiten las comunicaciones. El término "tipo de servicio subyacente" se refiere al tipo de servicio que está siendo utilizado en la red, por ejemplo, transferencia de archivos, correo electrónico o envío de mensajes instantáneos. Para mayor ilustración, ver artícu-

respecto del usuario identificado como sospechoso.

Es de destacar que los datos que se requerirán a las *ISP* se encuentran alojados en extraña jurisdicción y si bien el mecanismo habitual para pedir datos de usuario que se encuentran en otro país es través de rogatorias internacionales o mediante la utilización de Tratados de Cooperación Internacional de Asistencia Mutua en asuntos penales[12], se ha generado en la práctica una costumbre internacional de intercambio informal a través de los correspondientes portales de cada una de las empresas habilitados para las fuerzas a la ley[13]. Ello se debe a la necesidad de recibir los datos del usuario en el menor tiempo posible ante la posibilidad que se pierdan o sean borrados.

Los requisitos para solicitar información a todas las empresas internacionales *(Facebook, Twitter, TikTok, Microsoft, Google, Yahoo, etc.)* varían según sus políticas internas; toda vez que la colaboración es voluntaria[14].

Ahora bien, con la información recibida por parte de la *ISP* requerida, se solicitará a la empresa prestataria de servicio nacional o local que administra esa dirección IP que informe los datos de abonado de ese usuario, es decir los datos del cliente al que le fue asignada esa dirección IP –dinámica o estática- en ese preciso día y horario determinado (nombre, dirección, celular, forma de pago, etc.).

La precisión con la que se lea esa información recibida será fundamental para evitar errores en la individualización de los sospechosos, teniendo en cuenta que la asignación de una IP "dinámica" implica que puede cambiar constantemente la asignación a distintos usuarios y, además, no debemos olvidar el requisito de convertir el horario al local. En el caso de Argentina, cuando la empresa extranjera informa el horario en formato UTC, se deben restar 3 horas, ya que el huso horario argentino es UTC-3[15].

En consecuencia, esta información permite dar con el lugar físico de conexión del usuario investigado que utilizó para cometer el delito en entornos digitales.

lo 1.d). Datos relativos al tráfico, Informe explicativo del Convenio sobre la Ciberdelincuencia (STE Nº 185).
Cabe destacar que estos datos difieren de los llamados datos de contenido, que se refieren al contenido de la comunicación, es decir, el mensaje o información transmitidos por ella, por ejemplo, el contenido de un chat de *WhatsApp* o el cuerpo de un correo electrónico. Son los datos que merecen mayor protección en cuanto al derecho a la intimidad y privacidad, en virtud del tipo de información del que hablamos. Por su parte, los datos relativos a los abonados corresponden a cualquier información que posea un proveedor de servicios y que se refiera a sus abonados –diferentes de los datos relativos al tráfico o al contenido- y que permiten determinar el tipo de servicio utilizado, el período de servicio, la identidad, el domicilio de facturación y/o instalación del servicio, el número de teléfono del abonado y los datos relativos a la facturación y al pago. Art. 18.3 del Convenio sobre Ciberdelincuencia.

12 La Convención Interamericana sobre Asistencia Mutua en Materia Penal del 23 de mayo de 1992, vigente desde el 14 de abril de 1996, establece que los Estados miembros de la Organización de Estados Americanos (OEA) se comprometen a brindarse asistencia mutua en materia penal, tanto en investigaciones, actuaciones como en juicios penales, estableciéndose allí también el ámbito de aplicación, dentro de los cuales se encuentra la remisión de documentos, informes, información y elementos de prueba (art. 7.h). A su vez, la Argentina ha suscripto con Estados Unidos, país donde se encuentran alojadas la mayoría de las empresas cuya información necesitamos en investigaciones de este tipo, el Tratado de Asistencia Jurídica Mutua en Asuntos Penales, Ley 24.034, sancionada el 27 de noviembre de 1991, donde también se establece el mecanismo de cooperación para requerir información o documentación en el marco de investigaciones penales de un Estado al otro. Sin embargo, en la práctica, este medio para solicitar información no resulta idóneo cuando lo que estamos requiriendo es evidencia digital, ya que el procedimiento tiene formalidades y es largo, tardando meses entre que se requiere la información y se recibe.

13 Dupuy, Daniela, Kiefer, Mariana. (2020). La transferencia transfronteriza de datos en el marco de investigaciones criminales. *Revista Derecho y Nuevas Tecnologías*, N° 2. CETyS. Universidad de San Andrés. Dir. Palazzi, P.

14 Para mayor información sobre los aspectos formales que exige cada empresa cfr. Dupuy, Daniela, Neme Catalina. (2020). *Acosos en la red.* Vol.I, Hammurabi, Buenos Aires, p.245 y ss.

15 Cabe señalar que las empresas extranjeras informan en distintos husos horarios (UTC, GMT, PDT, EST, EDT), el que se deberá determinar previo a realizar la conversión horaria. A fin de conocer correctamente cómo realizar esta conversión según el huso horario informado por cada empresa, visitar https://www.worldtimebuddy.com/

Trasladémonos a un escenario de juicio. Solo algunas cuestiones para destacar:

- La explicación del rompecabezas acerca de cómo llegamos al domicilio del acusado debe ser desarrollada paso a paso y desde el primer momento.
- Los testigos suelen ser investigadores propios de la fiscalía, pues son ellos quienes conocen los procedimientos a seguir para preservar la evidencia digital y ellos deberán explicar acerca de por qué esa evidencia –preservada– no es otra, es decir, no fue alterada.
- En estos casos, y para preservar la evidencia, no es necesario ser técnico ni informático. Un investigador entrenado puede realizarlo y explicarlo luego a través del examen.
- El uso de protocolos para preservar la evidencia digital es fundamental: la demostración que en todos los casos hay un idéntico proceder trazable e inalterable para su conservación es información de alta calidad y utilidad para los jueces.
- La utilización de videos demostrativos y gráficos resultan un complemento indispensable mientras se desarrolla el examen del testigo que realizó la preservación.
- No contaremos en el juicio con ningún representante de *Facebook, Microsoft* o *Google*, que se expidan acerca del contenido de la información brindada. Dichos informes carecen de firma y se reciben por canales informales. ¿Ello podría representar un problema? Si se llegó a un acuerdo entre las partes para incorporarlos, no. De lo contrario, la defensa podría sembrar dudas acerca de su origen y legitimidad.
- La conversión horaria no es sencilla de explicar; el uso de gráficos por parte de testigos es fundamental y su procedimiento deberá ser irrefutable para que al tribunal no le quede duda alguna de la vinculación de los datos iniciales con el domicilio de conexión utilizado para delinquir.
- El litigante no debe dejar en manos de "testigos expertos" la suerte del caso. Cada parte será quien domine la escena a través de los exámenes y contraexámenes, pues deberán tener desde el inicio un conocimiento acabado de las maniobras técnicas que arribaron a resultados informáticos relevantes para su teoría del caso.

3) Proyección y realización de diferentes medidas de investigación

Las medidas de prueba y los medios de investigación se modernizan con el avance de las tecnologías.

Ahora bien, la recolección de evidencia digital no se limita a los delitos incluidos en la Ley de Delitos Informáticos Nº 26.388[16]; sino que para la investigación de todos los delitos se requiere de la prueba electrónica para comprobar algún aspecto de las teorías del caso del fiscal y defensa, o bien para complementar lo adquirido a través de la prueba física.

En ese sentido, los ciberdelincuentes complejizan su *modus operandi* en el ciberespacio y utilizan las tecnologías disruptivas para concretar las actividades delictivas; y ello exige que los Estados estén a la altura tecnológica para contrarrestar aquellos efectos, debiendo lograr un equilibrio entre la persecución penal y los derechos fundamentales de los ciudadanos.

Actualmente, hay una carencia legislativa procesal en la Argentina y en la mayoría de los países de la región, en cuanto a la regulación de la recolección y valoración de la evidencia digital en el sistema procesal penal y de los medios de investigación modernos adaptados a las nuevas tecnologías, debiendo acudirse al principio de libertad probatoria, adaptando las normas previstas para la recolección de prueba física en investigaciones que requieren

16 La llamada Ley de Delitos Informáticos, que incorpora varias figuras al Código Penal de la Nación Argentina y modifica algunas otras, fue sancionada el 2 de junio de 2008 y promulgada de hecho el 24 de junio del mismo año.

de evidencia digital. Ello, a pesar de la diferencia existente en relación a la expectativa de privacidad entre la prueba física y la digital, con la posibilidad de poner en riesgo garantías constitucionales[17].

En este escenario, sería conveniente incorporar a los Códigos de Procedimiento Penal las medidas de investigación específicas y los medios y formas de recolectar la evidencia digital que se adecuen a los desafíos que enfrentan los actos cometidos en un ámbito virtual[18]. Claro que en el mientras tanto, los litigantes deberán reforzar sus habilidades y destrezas para demostrar y justificar en el juicio la trazabilidad de la investigación.

Es importante que los investigadores elijan estratégicamente las opciones para individualizar a los sospechosos. Algunos de los medios más frecuentes son los que siguen, todos ellos con particularidades que los diferencian de los medios tradicionales, cuya explicabilidad acerca de la metodología utilizada para arribar a resultados contundentes, deberá ser expuesta correcta y claramente en las audiencias orales a través de los testimonios, para descartar todo tipo de duda acerca de la vulneración de derechos fundamentales.

a) OSINT (Open Source Intelligence)

Es una técnica de entrecruzamiento de la información pública disponible en Internet respecto de los sospechosos, su relación con posibles coautores o contactos que tengan relación con la víctima y otras posibles víctimas, y el resto de las evidencias recabadas hasta ese entonces, sumando también información de bases de datos oficiales, tales como el Registro Nacional de las Personas, Registro Automotor, etc. Todo ello, se relaciona con las evidencias existentes y tienden a coadyuvar y complementar la investigación e identificar el sospechoso, vinculando a un usuario virtual con una persona física.

b) Allanamiento

No es lo mismo secuestrar prueba física que evidencia digital; y su demostración en el juicio debe marcar esa diferencia.

Comparemos un allanamiento para secuestrar estupefacientes con otro para registrar fotografías o videos de abuso sexual de niños, niñas y adolescentes, o conversaciones entre el *groomer* y eventuales víctimas en los dispositivos de almacenamiento informático.

Cuando culmina el primero de los allanamientos, se puede determinar inmediatamente si se encontraron o no los elementos provenientes del delito investigado. Sin embargo, no ocurre lo mismo cuando termina el procedimiento para registrar la evidencia digital.

Ello es porque si bien se incautan las cosas u objetos (computadoras, teléfonos celulares, *tablets, pendrives*, etc.), lo que se busca en

17 Este principio de libertad probatoria es reconocido por la doctrina mayoritaria y se encuentra previsto expresamente en algunas regulaciones procesales penales argentinas, como el Código Procesal Penal de la Nación –art. 193–, y en los de algunas provincias tales como Córdoba –art. 192– o la Ciudad Autónoma de Buenos Aires –art. 106–. Consiste en la posibilidad de incorporar prueba al proceso penal ya no únicamente por los medios de prueba que se encuentran expresamente regulados, sino también mediante cualquier otro no reglamentado que sea idóneo para contribuir al descubrimiento de la verdad, siempre que no se vulneren garantías constitucionales ni sean contrarios a la ley. Para ello, se deberá buscar el medio de prueba analógicamente más aplicable que sí se encuentre regulado, y se utilizará el procedimiento allí señalado, respetando sus formas y bajo las mismas sanciones. En este sentido, ver Cafferata Nores, José I. – Hairabedián, Maximiliano. *La prueba en el Proceso Penal.* Abeledo-Perrot, Buenos Aires, 6a ed., pp. 49 y ss. Sin embargo, este principio es cuestionado por algunos autores, entre ellos Gabriel Pérez Barberá, quien sostiene que en materia procesal penal también debe regir la protección constitucional amplia de prohibición de analogía de la ley *in malam parte*, ya que incluir por analogía normas procesales que no han sido expresamente previstas genera un perjuicio a la posición del imputado en el proceso. En este sentido, véase Pérez Barberá, Gabriel (2009). Nuevas Tecnologías y libertad probatoria en el proceso penal. Ponencia llevada a cabo en el *IV Encuentro de Profesores de Derecho Procesal Penal.* Salta.

18 Por medio de la Ley 27.411 (B.O. 15/12/2017), Argentina adhirió al Convenio sobre la Ciberdelincuencia de Budapest del 23 de noviembre de 2001, vigente en el país desde el 1 de octubre de 2018.

realidad son datos; los datos que contienen aquellos objetos. Entonces, cuando se concluye el allanamiento no se tiene conocimiento, en ese preciso momento, de si lo que se busca está efectivamente en el interior de las cosas, en razón de que el verdadero registro se lleva a cabo en el laboratorio forense (salvo algún caso en el que, excepcionalmente y por motivos de extrema gravedad, se decida efectuar el registro en el lugar).

En ese sentido, tiene lógica que con el resultado de las tareas de constatación y de la búsqueda en fuentes abiertas se solicite el allanamiento para secuestrar los dispositivos de almacenamiento informático para luego, y ya en el laboratorio informático, se proceda a registrar, extraer, obtener, analizar y presentar los datos almacenados en aquellos.

Lo expuesto incluye en el pedido de allanamiento los puntos técnicos de análisis, como así también la modalidad de registro de esos datos: copia forense para posterior análisis o bien análisis en el lugar -*triage* o búsqueda rápida- para casos donde pueda existir un riesgo concreto por la presencia de niños o niñas conviviendo con el sospechoso, por ejemplo.

También, durante el allanamiento es fundamental el modo en el que se secuestran los objetos materiales dentro de los cuales se encuentran los datos que queremos obtener. Recordemos que allí se inicia la cadena de custodia y todo lo que sigue hasta la presentación del informe técnico deberá ordenarse con miras a su presentación en el juicio oral y público.

c) Obtención y preservación de evidencia digital: protocolo de buenas prácticas

La evidencia digital se compone de registros que fueron procesados en un dispositivo informático y se encuentran almacenados o fueron transmitidos a través de un medio de comunicación informático[19].

Presman complementa esta definición con algunas características propias de la evidencia digital, que debemos considerar:

- Está conformada por un conjunto de bits, la mínima expresión de almacenamiento que solo puede tener un valor binario: cero o uno. Esta característica es clave en el sentido de que todo registro digital puede ser duplicado y las copias que se realicen del mismo, si siguen las buenas prácticas, serán idénticas e indistinguibles del original.
- Es intangible. El disco rígido es el envase que soporta a los bits de información allí almacenada.
- La evidencia digital posee metadatos, esto es, el dato del dato; por ejemplo, la fecha de creación del documento.
- Permite almacenar grandes volúmenes de información en contenedores de dimensiones reducidas, como es un disco rígido, circunstancia que exige una correcta identificación para no perder evidencia valiosa[20].

Brenner señala que la intangibilidad es lo que distingue los documentos digitales de los de papel, que son relativamente refractarios a la alteración involuntaria y más resistente que la evidencia generada electrónicamente. Esta última es muy vulnerable, dado que incluso en ausencia de intentos de destrucción, el uso normal del sistema informático conduce a la destrucción de grandes cantidades de información[21].

19 Presman, Gustavo. D. (2018) *La cadena de custodia en la evidencia digital*. Cibercrimen II, dir. Dupuy, D., coord. Kiefer, M. B de F, Buenos Aires, p.304 y ss.
20 Presman, Gustavo, D., ob. cit., p.304/5.
21 Brenner, Susan W. Frederiksen, Bárbara. A, (2002). Computer searches and seizures: some unresolved issues. *Michigan Telecommunications & Technology Law Review*, vol. 8, N° 1, p.65

Para la recolección y posterior tratamiento de la evidencia digital es fundamental atender a protocolos específicos. En ese sentido, cabe mencionar un documento que presenta normativa metodológica para la escena del hecho, procedimientos de recolección y tratamiento de la evidencia digital. Es el estándar ISO/IEC 27037:2012 *Guía para la identificación, recolección, adquisición y preservación de la evidencia digital*[22].

El protocolo elaborado por el Instituto Nacional de Justicia del Departamento de Justicia de Estados Unidos[23] fue especialmente preparado para asistir al personal de las fuerzas de la ley y responsables de identificar y preservar dispositivos que contengan evidencia digital en el lugar del hecho. El documento establece una clasificación de diversas fuentes de evidencia digital, proporciona lineamientos para la recolección de material probatorio, manejo de cadena de custodia y otras consideraciones especiales sobre evidencia digital.

En Europa, para la recolección de la evidencia digital se recurre a los lineamientos establecidos por la Association of Chief Police Officers del Reino Unido[24].

Es de destacar que, más allá de las guías de buenas prácticas, la recolección de evidencia digital no es un proceso lineal que siempre se hace de la misma forma: las metodologías en cada caso concreto pueden diferir unas de otras.

Es fundamental respetar la cadena de custodia. Es un registro minucioso de cada movimiento de la evidencia en un proceso probatorio, que indica con exactitud las actividades realizadas, las personas que intervinieron y el estado de la evidencia. Es el conjunto de documentos sobre los elementos de prueba que permitirán asegurar y demostrar la identidad, integridad, preservación y registro de la evidencia digital[25].

La normativa procesal vigente aplicable a nivel federal no especifica la incorporación de la evidencia digital.

En Estados Unidos, las normas procesales federales requieren que la parte que solicita la incorporación al proceso de pruebas digitales demuestre su autenticidad acreditando el respeto a la cadena de custodia, siendo que el incumplimiento a esta exigencia puede determinar la inadmisibilidad de la evidencia[26].

En el juicio es fundamental que las partes demuestren a través de las declaraciones de los expertos informáticos, el paso a paso y el respeto de la cadena de custodia, con específica y detallada referencia a cada fase.

En esta línea, es de destacar la presencia de dos escenarios: uno en la escena propiamente dicha o en el domicilio allanado, y el otro en el laboratorio.

En el primero se procederá a asegurar la escena, protegiendo la evidencia digital de toda modificación o destrucción; identificando los sistemas informáticos que pueden tener información relevante; y capturando y realizando copias exactas de las evidencias identificadas a través del empleo de herramientas forenses que garantizan la inalterabilidad de la evidencia original. Será una decisión estratégica del fiscal que la última fase señalada se lleve a cabo en la misma escena o bien en el laboratorio forense.

22 *Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence*, www.iso.org

23 Electronic Crime Scene Investigation, a guide for first responders http://www.ncjrs.gov/pdffiles1/nij/219941.pdf.

24 Ver https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf.

25 Presman, Gustavo, D., ob.cit., p. 308

26 United State v. Salcido, 506 F.3d 729,733, Corte Federal de Apelaciones del 9no. Circuito, 2007, citado en Blanco, Hernan. (2020). *Tecnología informática e investigación criminal*. Buenos Aires, Thomson Reuters, La Ley, p. 748.

En el segundo, es decir, en el laboratorio, se preservará las evidencias, detallando en documentos todo tratamiento y procedimiento que se realice en ellas, garantizando la cadena de custodia; se analizarán las evidencias siguiendo una metodología forense especializada y empleando las herramientas de análisis forense adecuadas para cada caso; y por último, se presentarán los resultados obtenidos en forma clara y precisa a través de un informe técnico elaborado por los especialistas informáticos.

Cada fase debe explicarse al detalle en el juicio oral, demostrando su intangibilidad y trazabilidad desde el primer momento hasta la entrega del informe técnico a las partes.

En ese sentido, del Convenio para la Ciberdelincuencia de Budapest[27] surge que las medidas procesales sobre prueba digital reguladas en el convenio tienen como fin salvaguardar los datos, es decir, preservar su integridad o mantener la cadena de custodia de estos, lo que significa que los datos copiados o extraídos serán conservados e inalterados mientras duren los procedimientos penales.

d) Copia forense o bit a bit

Una de las principales discusiones que se suscitan antes de analizar los dispositivos secuestrados es si al momento de efectuarse la imagen forense[28] -o copia *bit a bit*-, es necesaria la presencia de la defensa.

Esto claramente dependerá de si ese acto se concibe como irreproducible o no. En este sentido, y más allá de la extensa discusión que rodea este punto, la cual excede el objetivo de este trabajo, adelanto que a mi entender es la clonación o la copia de la evidencia digital que se encuentra en el dispositivo de almacenamiento informático del sospechoso. Es una medida reproducible, pues se pueden hacer tantas copias como sean necesarias, siempre que se utilicen herramientas forenses que garanticen mediante un valor *hash*, la inalterabilidad del original[29].

En ese sentido ya se ha expedido la Cámara Nacional de Apelaciones Criminal y Correccional, Sala IV[30] y, en idéntica línea, se pronunció el Tribunal Supremo de España[31].

No obstante, en la práctica es común notificar a la defensa de su realización para demostrar un procedimiento que garantiza la cadena de custodia de los elementos secuestrados y cuya copia se efectuará; como así también, con el fin de evitar futuros planteos que puedan dilatar el trámite del caso.

27 Informe Explicativo, consid. 197.

28 La imagen forense es la copia a un disco de la evidencia digital que se encuentra en el original que, por medio de un *hash* (algoritmo matemático que convierte una cadena de longitud variable en una cadena de longitud fija) se confirma que el contenido del disco no ha sufrido cambio alguno; en Velázquez, Andrés. (2016). *Los próximos paradigmas de las pruebas digitales.* En Cibercrimen II, dir. Dupuy, D, coord. Kiefer, M., B de F, Buenos Aires, p.314 y ss.

29 En este sentido ya se expidió el Tribunal Supremo español Sala de lo Penal. Madrid. 767/2019 de 12 de septiembre.

30 Cámara de Apelaciones en lo Criminal y Correccional, Sala IV, causa A, J.A y otros s/nulidad: *la apertura de los teléfonos celulares es valorada por el tribunal como la obtención de una copia de la información que obraba en los aparatos, es decir, la guarda de un soporte informático de los datos que estaban almacenados en el dispositivo... La omisión de notificar a la defensa no acarrea la nulidad del acto.*

31 TS Sala de lo Penal. Madrid. 767/2019 de 12 de septiembre: *Como recientemente recordamos en nuestra Sentencia 388/2018, de 25 de julio, hemos de indicar que esta Sala ha considerado que no es necesario que esté presente en la diligencia de volcado o clonado de datos el Letrado de la Administración de Justicia (STS 342/2013, de 17 de abril; o STS 165/2016, de 2 de marzo) y el nuevo artículo 588 sexies c) de la LECRIM no lo exige (cuando regula el acceso a la información contenida en instrumentos de comunicación telefónica, entre otros). Tampoco se ha considerado necesaria la presencia del interesado o su Letrado (STS 342/2013, de 17 de abril), porque ni la ley procesal anterior al año 2015 ni tampoco la nueva normativa de la Ley de Enjuiciamiento Criminal (Ley 13/2015, de 5 de octubre) imponen que estén presentes el letrado del imputado ni un perito nombrado por la parte en el momento de volcar el contenido del ordenador. Es más, el nuevo artículo 588 sexies c) ni siquiera requiere la presencia del Secretario Judicial en el momento de abrir el ordenador y obtener el disco duro. Y en cuanto al nombramiento de un perito de parte para que esté presente, la sentencia de esta Sala 342/2013, de 17 de abril, si bien considera que la parte puede designar un perito, de acuerdo con lo dispuesto en el art. 476 de la LECr. su no intervención no condiciona la validez de la diligencia (STS 165/2016, de 2 de marzo).*

Luego, puede ocurrir que los peritos informáticos de ambas partes analicen la evidencia digital en forma conjunta, o bien que se realice una copia para ser analizada individualmente por los técnicos de cada parte. Después, se presentarán y controlarán sus resultados a través del examen y contraexamen de los peritos informáticos en el debate oral.

e) Análisis de la evidencia digital. Doctrina de la *Plain View*

Frecuentemente, las órdenes judiciales están limitadas a determinados lugares físicos, (hogar del sospechoso, entidad bancaria o gubernamental, etc.).

Sin embargo, cuando se registran datos informáticos puede ocurrir que:

a) Los datos no fueron almacenados en discos duros locales, sino en un servidor externo al cual accedió por Internet.
b) Los datos fueron almacenados en la nube.
c) Los datos fueron almacenados en un sistema informático en el extranjero.
d) Se ha utilizado de medios de comunicación anónimos: TOR o terminales públicas.

Por ese motivo, es fundamental que las órdenes de registro tengan cierta flexibilidad. Ello implica que si los operadores se encuentran ante cualquiera de las situaciones anteriores, deben poder extender el registro a ese sistema o acceder a otro cuando haya motivos para creer que los datos buscados se encuentran en otro sistema informático.

Y así lo establece el art. 19 de la Convención de Budapest:

> *Cada parte adoptará las medidas legislativas que resulten necesarias para facultar a sus autoridades a registrar o tener acceso de un modo similar:*
>
> *a) A todo sistema informático o parte del mismo, así como a los datos informáticos en él almacenados;*
> *b) A todo dispositivo de almacenamiento informático que permita almacenar datos informáticos en su territorio.*

Ahora bien, tal como venimos sosteniendo, la prueba física es diametralmente diferente a la evidencia digital.

Una requisa destinada a buscar datos en concreto no puede distinguir *ex ante* sobre el objeto de su búsqueda y por lo tanto, debe revisar la totalidad de los datos, siendo muy difícil circunscribir la búsqueda de modo tal de no invadir la privacidad del sospechosos; pues allí estará alojada prácticamente la vida del sospechoso, de algún familiar que también utilice ese dispositivo electrónico, o bien elementos provenientes del delito que se está investigando y quizás de otros cometidos hace años, por ejemplo.

La pregunta es: ¿cuál es el límite? ¿Cuál es la expectativa de privacidad? ¿Qué ocurre cuando se encuentran otras cosas que provienen de otro delito diferente del que se está investigando?[32].

Si bien su respuesta no es objeto de este trabajo, la idea es plantear situaciones complejas que los litigantes deberán estar preparados, entrenados y capacitados para su demostración en juicio oral pues, un contraexamen apuntando a debilidades de estas características podría generar un escenario de duda si no se tienen claros los alcances y la dinámica de lo que ocurre en el ciberespacio cuando se comete delitos.

32 Para mayor información sobre los alcances y jurisprudencia nacional e internacional sobre la *Doctrina de la Plain View*, cfr. Dupuy, Daniela, Neme Catalina. (2020). *Acosos en la red,* Vol.I, Hammurabi, Buenos Aires, p.297 y ss.

f) Algunas consideraciones para el juicio oral

Como hemos señalado en los puntos precedentes, y solo de forma inicial pues la complejidad y sofisticación de posibles medios de investigación y de herramientas informáticas crecen diariamente, será momento de tomar conciencia del alcance e impacto que sus aristas pueden revelar en las audiencias orales.

Veamos algunas:

- **Preparación de testigos expertos:** los técnicos e informáticos suelen ser figuras estelares en las audiencias orales y están acostumbrados a ser examinados y contraexaminados. No obstante, su preparación es fundamental pues permitirá a cada parte chequear la comprensión de la información que brindará a través de su testimonio. También se podrá delimitar lo más trascendente para el caso; recordemos que es vital circunscribir y acotar la explicación de los técnicos a lo estrictamente relevante para la teoría del caso, pues podría confundir al tribunal si hay sobreabundancia de información. Por último, pero muy importante, es el uso de un lenguaje claro. Si como litigantes no logramos preparar a un testigo para que su explicación sea sencilla y contundente, iremos directo al fracaso.
- **Acreditación del testigo:** la acreditación de los testigos técnicos e informáticos es trascendental, pues el objetivo es fortalecer su credibilidad como testigo y la de su testimonio. Es común que los técnicos e informáticos sean ingenieros, peritos o licenciados en sistemas; pero también hay algunos que carecen de un título universitario, pero poseen una formación terciaria y certificaciones internacionales, y en algunos casos son autodidactas; circunstancia que no invalida las evidencias que han obtenido para el caso si se logra explicar su procedimiento y legitimidad sólidamente. Si bien en un contexto tradicional podría verse como una debilidad, si efectuamos una correcta acreditación del testigo y se acompaña con un fuerte testimonio, deja de serlo. Preguntarle acerca de su experiencia laboral, antigüedad en la que desarrolla su *expertise* informática, cantidad de cursos y especializaciones efectuadas, horas de análisis de evidencia electrónica realizadas por semana, o por mes, efectuando una proyección al año. Aseguro que lo dicho sorprenderá aún más que tener un título universitario y poca experiencia en la materia. Así es el mundo cibernético hoy.
- **Examen directo:** al preparar el examen es fundamental tener presente la teoría del caso para acotar a ello la información. Cuando escuchemos al testigo en la entrevista previa, decidiremos qué tipo de examen efectuar: si nos limitaremos a realizar una sola pregunta pues bastará para que suministre toda la información concreta y ordenada o, de lo contrario, será un testigo que necesitará ser guiado en su examen, para evitar ingresar en temas irrelevantes para la teoría del caso. Lo importante es mantener la atención del tribunal; y como el examen suele durar más tiempo que ello, debe ser llevado adecuadamente.
- **Uso de gráficos:** es un excelente método para apoyar el relato y que el tribunal mantenga su atención. Asimismo, complementa una explicación técnica que suele tener cierto nivel de dificultad.
- **Demostración en tiempo real:** si el imputado para distribuir videos de abuso sexual infantil se valió de una red *peer to peer* como el software *E Donkey,* el fiscal deberá examinar a su testigo experto sobre qué es y cómo funciona esa red para compartir. Seguramente, si el técnico la explica, al tribunal le costará entenderlo a la perfección. Así, una herramienta a la que puede acudir el litigante es solicitar autorización al tribunal para que, mientras que el testigo la explica, efectúe una demostración en tiempo real acerca de su funcionamiento y alcance; accediendo para ello a Internet y al software específico.

- **Contraexamenes**: para contra examinar a los informáticos será necesario que las partes conozcan en profundidad las cuestiones técnicas que desarrollaron los testigos. Si se contraexamina sin ese conocimiento y se va de pesca, es probable que le demos ventaja a la contraparte. No hay margen de error: si decidimos contraexaminar es con certeza acerca de la línea de la teoría del caso de la contraparte que deseamos hacer tambalear.
- **Adelanto de debilidades**: como ya señalé, hay muchas cuestiones en las investigaciones en entornos digitales que no se han resuelto aún, sobre todo ante una carencia de leyes de forma que deberían adaptarse a las nuevas tecnologías. Pero también hay discusiones sobre si ciertos actos realizados en los dispositivos de almacenamiento informáticos son o no una pericia; si es o no irreproducible, si es válida la información suministrada desde extraña jurisdicción evitando los canales tradicionales; si es legítima la evidencia adquirida en otro país cuando el medio de investigación no está expresamente previsto en la legislación nacional, etc. Todo ello genera una adversarialidad constante entre las partes en las audiencias orales y es positivo adelantarlas con un fundamento lógico y sólido antes que la contraparte se encargue de destruir nuestra justificación de antemano.
- **Trazabilidad y explicabilidad**: dos objetivos fundamentales a la hora de examinar a los testigos e ir armando una línea completamente trazable y explicable del principio al fin.
- **Alegatos de clausura:** llegó el momento de relacionar toda la prueba producida en el juicio, empatarla con nuestro alegato de apertura y concluir nuestros resultados de manera clara, concreta y sin perder ningún eslabón de nuestra teoría del caso. Llegó la hora de que seamos los litigantes quienes le expliquemos al tribunal, en lenguaje llano, cómo y cuándo se cometió el delito en el ciberespacio y de qué manera se arribó a los resultados obtenidos, incluyendo cómo se preservó, se extrajo, se analizó y se procesó la evidencia electrónica.
- **Presentaciones:** el uso de presentaciones en *Power Point* o *Prezi* suele ilustrar al tribunal complementando el contenido del alegato de clausura.
- **Capacitación:** la formación de los operadores del sistema es fundamental para litigar este tipo de casos cuya nueva lógica no es "lo que vendrá"; ya está aquí entre nosotros y para investigar y litigar cualquier delito.

III. A modo de cierre

Este trabajo es una visión muy sintética y panorámica de la nueva lógica para investigar en el ciberespacio y luego ejercer las destrezas de litigación en un juicio oral en el marco de un proceso penal acusatorio.

Seguramente, a partir de su lectura, surgirá una serie de dudas que requerirán de mayor desarrollo en próximos trabajos.

Este artículo solo tuvo como fin realizar un sencillo muestreo de dos de los desafíos que entiendo son de gran importancia en el ámbito del procedimiento penal: conocer el mundo del cibercrimen en toda su dimensión y constante evolución, y adquirir destrezas para litigar los casos digitales en las audiencias orales.

Lo expuesto no se logra sin una continua capacitación de los operadores del sistema.