Evidencia Digital, Investigación de Cibercrimen y Garantías del Proceso Penal

Jornada de trabajo

por los Derechos Civiles

Área Digital
Asociación por los Derechos Civiles

Diciembre 2017
https://adcdigital.org.ar

Este trabajo fue realizado como parte de un proyecto financiado por Ford Foundation.

Índice

Jornada de Trabajo: "Evidencia Digital, Investigación de Cibercrimen y Garantías del Proceso Penal"*

I. Introducción

El día 9 de marzo de 2017 se llevó a cabo la Jornada de Trabajo "Evidencia Digital, Investigación de Cibercrimen y Garantías del Proceso Penal" en la Ciudad de Buenos Aires.

El encuentro fue organizado por la Asociación por los Derechos Civiles (ADC) debido a la relevancia de los desafíos planteados por la irrupción de la tecnología informática en el proceso penal, y la difícil delimitación entre "la eficiencia en la investigación de los delitos" y la necesidad de "protección de las garantías procesales en el mundo digital".

Con la finalidad de realizar un aporte que resulte beneficioso para todo el ecosistema de operadores que interactúa día a día en el quehacer de la investigación criminal, llevamos adelante esta Jornada de Trabajo en la que participaron integrantes de los equipos y laboratorios forenses de las fuerzas policiales federales y provinciales, fiscales y miembros del poder judicial y reconocidos abogados penalistas.

El evento consistió en diversos paneles que analizaban un aspecto particular de la temática y fue realizado bajo la regla Chatham House, bajo la cual los participantes tienen el derecho de utilizar la información que reciben pero no pueden revelar la identidad del orador ni de otro participante. En ese sentido, las personas que figuran con su nombre lo están porque dieron su autorización o participaron como panelistas.

El presente documento consiste en un resúmen de lo sucedido en la Jornada con las principales ideas y experiencias relatadas por los participantes. Si bien no es una transcripción literal de lo manifestado en el evento, se ha buscado mantener lo más fielmente posible el lenguaje coloquial utilizado por los expositores, el cual posee una fuerte impronta jurídica debido a la composición del público asistente.

*El presente informe fue compilado por **Eduardo Ferreyra**, abogado e investigador del Área Digital de la Asociación por los Derechos Civiles (ADC). El mismo contó con la colaboración de Jeannette Torrez y Marianela Milanes. Encargado de diseño y diagramación: Leandro Ucciferri.

Desde ADC esperamos que este documento contribuya a un necesario debate acerca de cómo lograr que la legítima tarea de investigar y prevenir delitos sea realizada con respeto por los derechos y las garantías procesales de las personas afectadas.

II. Panel "Evidencia Digital e Investigación del Cibercrimen. Estado del Arte. Análisis y desafíos técnico forenses"

Expositor: Miguel Justo, Policía Federal Argentina.

1. El uso de las nuevas tecnologías trae aparejado fenómenos novedosos entre ellos, modalidades delictivas que enfrentan las capacidades de los distintos miembros que conducen una investigación judicial.

2. La escasa interacción entre los operadores judiciales, los investigadores y los peritos dificulta la tarea de investigación, que además se ve comprometida por la falta de recursos para el investigador.

3. Para desarrollar investigaciones sobre cibercrimen más exitosas es necesario incorporar mejores herramientas judiciales y procesales que permitan proveer al perito de los elementos necesarios para que luego el operador judicial haga la valoración final de toda la actividad de investigación técnica. En este sentido, Estados Unidos y algunos países de Europa han adoptado herramientas que han sido útiles para ello.

4. Es importante tener en cuenta las facultades procesales que deben tener los investigadores en cibercrimen cuando deben ocuparse de delitos online en los cuales existe una multiplicidad de jurisdicciones por la propia naturaleza de internet. De esta manera, si un operador judicial debe validar una información generada en otro país, debe esperar una rogatoria internacional que demora la investigación judicial.

5. A partir de 2016, el Ministerio de Seguridad de la Nación publicó el Protocolo General de Actuación para las Fuerzas Policiales y de Seguridad en la Investigación y Proceso de Recolección de Pruebas en Ciberdelitos que es de aplicación obligatoria para las fuerzas federales y que se dicta en cursos con material para el conocimiento de todo el personal.

6. Pedagógicamente podemos clasificar a la evidencia digital en tres categorías: hardware, software y documental. Cada una de dichas clases de evidencia implican tratamientos diferenciados.

7. La evidencia digital documental puede ser provista por empresas proveedoras de servicio de internet u otros intermediarios, a la cual se la reviste de carácter procesal y es anexada a un

expediente. Es decir, que la evidencia documental es digital aunque se plasme en formato papel ya que es una operación de software que realiza en sus servidores la empresa intermediaria.

8. En lo que respecta al hardware, existe una diversidad de procedimientos técnicos que debieran utilizarse en cada oportunidad que se encuentra evidencia digital. De tal manera es necesario advertir algunas características del proceso de incautación para un correcto aseguramiento de la prueba y a pesar que el Protocolo publicado por el Ministerio de Seguridad provee ciertos lineamientos, existen muchas dificultades para aplicarlo. Por ejemplo, si bien las divisiones específicas dedicadas a este tipo de investigación en una fuerza de seguridad suelen tener los elementos necesarios, tales herramientas no están presentes en las demás dependencias de investigación.

9. En línea con lo anterior, la mayoría de las actividades delictivas -relacionadas o no con cibercrimen- involucran tecnología. En caso que una jurisdicción tome intervención en el delito, cabe la pregunta de si existen las capacidades y elementos para una correcta incautación y aseguramiento de la prueba para aportar al perito. Es por ello que debe reforzarse la inversión en elementos para investigación en cibercrimen, puesto que la tecnología y la evidencia digital queda involucrada en cualquier actividad delictiva y en cualquier expediente.

10. En relación a la incautación del hardware, debe atenderse a la continuidad y el resguardo de la prueba, es decir, que nadie pueda cuestionar que inequívocamente el contenido de un dispositivo es el que estaba en el lugar del hecho y el que va a llegar en esas condiciones al perito. En este sentido, durante el momento de la incautación no es posible hacer una interrupción, ya que cuando comienza el acto de allanamiento o el acto de secuestro no puede haber interrupciones hasta el término del proceso que a la vez, tiene que ser frente a testigos.

11. Existen algunos debates acerca de si es viable realizar una copia bit a bit de un dispositivo en el lugar de la incautación. Sin embargo, como dicho proceso tomaría varias horas, el aseguramiento del dispositivo con un envoltorio o franjado se torna sustancial.

12. Es necesario establecer la diferencia entre pruebas de cargo y prueba de redireccionamiento en la investigación, debido a que en nuestro sistema procesal los expedientes en una prueba de cargo pueden demorar mucho tiempo. El problema surge cuando una evidencia digital que debe ser tratada para redireccionar la investigación se puede realizar en el mismo laboratorio que está realizando ese otro tipo de pericias, es decir, prueba de cargo. Entonces la única manera de evitar listas de espera, es dividir laboratorios que realizan pericias forenses conocidas como pruebas de cargo y otros laboratorios que se dediquen exclusivamente al apoyo en la investigación.

13. Cuando se dispone del secuestro de dispositivos es muy común el secuestro de teléfonos, memorias, pendrives pero generalmente no se tiene en cuenta el secuestro y análisis de información

que pudieran contener impresoras, y/o smartwatchs.

Expositor: Ingeniero Gustavo Presman, experto en Informática Forense.

1. En la escena del hecho usualmente no se realizan pericias, lo que no quiere decir que no pudiera hacerse, pero en tal caso, se requerirá de un perito (o un operador técnicamente formado) y además hay que valorar la viabilidad de acuerdo a lo que se está pretendiendo obtener. Los recursos de los cuales se disponen -y que muchas veces no se trata de recursos físicos- tiene que ver también con la débil comunicación entre operador judicial y perito. En caso que se realicen pericias en la escena del hecho es fundamental valorar la presencia de los peritos de parte garantizando el derecho a defensa y evitando posteriores nulidades.

2. Además de infraestructura y espacio físico, los laboratorios necesitan de áreas donde se pueda mantener el control de la cadena de custodia y que se pueda mantener el sellado de la evidencia. En este sentido, es requerido un depósito donde haya un control de quien extrae los elementos y quién los guarda.

3. Por otro lado, en relación a los recursos humanos, existe una falta de capacitación en las herramientas y procedimientos que se utilizan, es por eso que sería ideal que el personal estuviera certificado.

4. La certificación es un proceso académico no formal que diferentes instituciones y diferentes fabricantes de herramientas dan sobre procedimientos de informática forense y sobre procedimientos de uso de las herramientas. Es relevante contar en los laboratorios forenses con graduados universitarios en carreras afines. Actualmente, no existe una universidad que enseñe informática forense, existen algunos cursos, especializaciones o diplomados pero no tienen de alguna manera el rango una carrera universitaria.

5. La certificación requiere de un apoyo por parte de las autoridades para que la persona estudie debido a los cuestionamientos del dictamen pericial que pueden surgir.

6. Los Protocolos son problemáticos cuando establecen normas muy rígidas y taxativas, debido a que pueden dejar un margen muy escaso para manejar situaciones no contempladas. Sin embargo, hay una cuestión que tiene que ver con la metodología de trabajo de cada laboratorio que requiere alguna pauta de estandarización.

7. Un protocolo podría funcionar como un marco de referencia. No obstante, cuanto más se abunde en detalle en definitiva lo que sucede es que por un lado se brinda un marco en el cual se acomoda la tarea investigativa, pero por otro lado encorseta y muchas veces impide hacer la tarea. El protocolo tiene que definir claramente qué cosas no se deben hacer y qué cosas

son el marco para hacer. La mecánica exacta de cómo se debe hacer es parte de la decisión del propio perito.

8. En cuanto a las responsabilidades de los peritos, primero debe emplear procedimientos que sean técnicamente reconocidos por la comunidad internacional y documentar cualquier intento de usar algún procedimiento que colisione con lo anterior, con el objeto que la interacción con el dispositivo no sea confundida como una contaminación. Entonces cada vez que hay que interactuar con un dispositivo, hay que solicitar la autorización y es responsabilidad del perito explicar al operador judicial las necesidades de ello.Por lo tanto, se vuelve fundamental, explicar con claridad el alcance de los procedimientos en especial aquellos que puedan alterar los elementos de prueba. Si bien existen situaciones de emergencia -por ejemplo, casos donde peligra la vida de una persona- en las cuales debe agilizarse los procesos, es el operador judicial quien debe decidir.

9. Las responsabilidades del operador judicial, por otro lado, son respetar y escuchar al perito, promover la comunicación, solicitar procedimientos viables, redactar puntos de pericias claros y posibles. Sería ideal una mayor interrelación entre el perito y el operador judicial. Por ejemplo, facilitar la información para tener mejor posibilidad de investigación antes de ir a la escena del hecho y por último entender el alcance de aquellos procedimientos que puedan alterar el estado de la prueba. No es necesario que los operadores judiciales sean expertos en informática pero sí que entiendan el impacto de los procedimientos.

III. Panel "Prácticas actuales de investigación y recolección de evidencia digital versus garantías de debido proceso"

Moderador: Marcos Salt, abogado especialista en evidencia digital.

Expositores: Cristina Caamaño, Fiscal de la Dirección General de Investigaciones y Apoyo Tecnológico a la Investigación Penal; Fernando Díaz Cantón, abogado penalista; y Carlos Christian Sueiro, Secretario Letrado de la Defensoría Oficial ante la Corte Suprema de Justicia de la Nación.

Marcos Salt: Vamos a plantear un caso hipotético, en el cual están incluidos elementos presentes en investigaciones reales. La idea es trabajar exactamente sobre situaciones donde se mezclan cuestiones jurídicas con cuestiones tecnológicas. Hay un problema que afectaba de alguna manera el sentido común de cualquiera que trabaje con Informática, es decir, hablarle de fronteras físicas y el principio de territorialidad. Desde el punto de vista de lo que establecen los códigos, hasta que los logremos cambiar, Internet no tiene cabida en los códigos procesales. Entonces, la idea es plantear distintos supuestos que se dan en una investigación de un delito complejo o un delito económico.

Primer supuesto: el experto en informática le explica que es necesario obtener los datos de tráfico de comunicaciones telefónicas y electrónicas de varios de los directivos de las empresas investigadas y que tiene el temor de que en el futuro puedan ser borradas ¿es posible pedir a las empresas proveedoras de servicio que de manera urgente esos datos se aseguren por un período de tiempo?

Marcos Salt: ¿Se entiende el supuesto? Nadie quiere ver los datos, lo único que quieren es asegurarlos porque los pueden necesitar en el futuro y saben que se pueden llegar a borrar.

Cristina Caamaño: Por el art. 212 del Código Procesal Penal, el fiscal está capacitado para pedir el aseguramiento de los datos pero no su adquisición. En este caso, tendrá que solicitar la orden al juez, de acuerdo al art. 213. Si bien el fallo "Halabi" estableció que las prestatarias no tienen la obligación de mantener toda la información de los llamados por diez años, no es lo mismo que solicitar el resguardo de una llamada en particular. Esa es una facultad que puede tener el fiscal. Ahora bien, en el momento en que necesite adquirir esa información, voy a necesitar la orden del juez.

Fernando Díaz Cantón: Yo opino que el "quick freeze" es una restricción de los derechos fundamentales. La facultad que da el art. 212 de requerir los informes que estime pertinente y útiles, disponer las medidas que considere necesarias en el ejercicio de sus funciones es una descripción demasiado amplia como para poder permitir que con la invocación de esa disposición se pueda hacer un quick freeze. Soy de la idea de que tiene que haber una casuística legislada, no una casuística dejada de una manera etérea a la voluntad de los operadores. No podemos dejar librado a facultades genéricas o cheques en blanco para poder realizar una injerencia en los derechos fundamentales

Carlos Christian Sueiro: La discusión se enmarca en una falencia que se presenta a nivel legislativo en el Estado argentino. El Estado ratificó el Convenio de Cibercriminalidad de Budapest, que se quiere incorporar desde el 2010. Y este convenio le solicita a los Estados la adaptación de sus legislaciones a nivel material, procesal y de cooperación internacional. Lo único que se logró adaptar desde la ley 26.388 es a nivel material pero nos hace falta la reforma procesal. La reforma de la ley 27.063 que se propuso el año pasado –que establece la posibilidad de vigilancias electrónicas en operaciones complejas- empieza en este sentido pero posee algunas falencias en función de que no regula lo que es la evidencia digital.

Marcos Salt: En el fondo, lo que está en discusión es lo que significa el principio de libertad probatoria en los códigos –es decir, que todo se puede probar de cualquier manera- y cuáles son sus límites cuando pueda afectar garantías individuales. El fallo "Halabi" tiene que ver con retención de todos los datos de los ciudadanos y el tribunal europeo también lo ha declarado de alguna manera en contra de las garantías individuales. La tendencia en el mundo hoy es que en la medida en que no haya un exhibición hacia un tercero del dato, que no haya un ser humano que haya podido ver el dato, no hay violación de la intimidad y por tanto entra dentro del principio de libertad probatoria, se puede aplicar por analogía alguna disposición del código.

Fernando Díaz Cantón: Sigamos con el supuesto "En los sistemas procesales en los que el fiscal está a cargo de la investigación ¿puede solicitar el fiscal a las empresas proveedoras de servicios de comunicaciones que me remitan los datos de tráficos de comunicaciones y los datos de abonados de diferentes cuentas o debo previamente obtener una orden judicial? Yo entiendo que si está expresamente previsto por el Código la posibilidad de hacerlo sí. Caso contrario, no.

Cristina Caamaño: Creo que es según el caso. Si se va a afectar la intimidad de la persona, hay que pedir la orden judicial. Ahora, si es un caso de secuestro extorsivo, lo puede pedir el fiscal y después el juez lo va a convalidar. En un caso de secuestro extorsivo la ley establece que el fiscal puede pedir la medida.

Marcos Salt: Todos los días pedimos datos de tráfico de comunicaciones. Ahora, la Corte Suprema en el fallo "Halabi" ha dicho que los datos de tráfico los tiene que pedir el juez. Por eso, si soy fiscal o policía y necesito un dato de tráfico de comunicaciones, tengo que pedir autorización judicial. Si no, el fallo se va a caer por nulo en la Corte. Y esto empieza a ser una tendencia mundial porque diferentes organizaciones no gubernamentales han explicado que los datos de tráfico de comunicaciones son más valiosos que un dato de contenido.

Gustavo Presman: Hay una discusión respecto a dato de tráfico y dato de contenido. Durante mucho tiempo el dato de tráfico incluía la dirección IP, más los DNS más los sitios visitados. Hoy por hoy se entiende que la dirección IP es un dato de conexión, no es un dato de tráfico.

Marcos Salt: La línea que se ha trazado en el mundo es que los datos de los abonados los pide la fiscalía o la policía directamente. Dato abonado se considera un dato prácticamente abierto, dato de tráficos y dato de contenido con autorización judicial. En Argentina se mantiene la idea en muchas provincias de que el dato de tráfico lo pide la fiscalía. El agravante es que en nuestro país tenemos el fallo "Halabi" de la Corte. Entonces, tenemos sistemas acusatorios que han avanzado muchísimo hacia mayores facultades para la fiscalía y tenemos un fallo de la Corte que pareciera volver –por lo menos en esa parte- hacia la idea de dar mayor protección a la autoridad judicial.

Fernando Díaz Cantón: Por más que esa autorización judicial respete todos los principios de necesidad, razonabilidad, si no está previsto legalmente, si el Parlamento que es donde todos nosotros estamos representados, no ha dado la autorización, entonces no alcanza con que el juez además de una orden razonable. Todo esto tiene que pasar por una discusión parlamentaria previamente. Y la analogía no es aplicable en estas cuestiones novedosas. Debe haber una ley que determine lo más casuísticamente posible los tipos de injerencia para que después la orden judicial que debe respetar todos los demás requisitos sea válida.

Segundo supuesto: "Un testigo ha aportado información de la existencia de prueba relevante para la investigación en los archivos informáticos de una institución bancaria ¿es posible solicitar al juez que ordene el secuestro de todas las computadoras y dispositivos de almacenamiento informático que encuentre en el lugar? ¿Puede limitar el alcance de la orden al registro y secuestro de los archivos y

datos relevantes contenidos en las computadoras y los dispositivos informáticos que se encuentren en la oficina identificada por el testigo? ¿Con qué límites pedirían la medida? ¿Qué requisitos debería tener la orden de allanamiento?

Cristina Caamaño: La medida es posible pero también es ridícula. La idea no es ir a la pesca en ningún momento. A mayor precisión, vamos a tener más limitación y más rapidez para relevar.

Carlos Christian Sueiro: Si el juez decide tomar esta medida –que aun no está regulada- debería tratar de identificar qué es lo que está buscando, cuánto puede durar la medida y qué técnicas se van a usar para llevarlo adelante.

Fernando Díaz Cantón: Hoy los jueces con las reglas del Código Procesal Penal se pueden llevar las computadoras pero no pueden acceder al contenido de los sistemas y de los equipos de comunicación. Por el principio de "nulla coactio sine lege", si no hay previsión legal específica como la contemplada, no se puede. La orden judicial requiere previamente de una habilitación legal. Ese juez está actuando sin ley que lo respalde. No puede haber una injerencia en un derecho fundamental sin una ley del Congreso nacional que lo prevea.

Carlos Christian Sueiro: debemos contemplar el tema de la progresión normativa. Existen un montón de aparatos que no existían cuando fue sancionado el art. 18 de la Constitución y quedan protegidos por progresión normativa del mismo modo.

Fernando Díaz Cantón: Pero la progresión normativa es para ampliar el margen de amplitud de las garantías, no para restringir los derechos. Para eso necesitas una regla el nulla coactio sine lege, no puede haber una injerencia en un derecho fundamental sin una ley del Congreso Nacional que la prevea.

Marcos Salt: Debemos tener en cuenta qué es lo que se hace en el lugar, porque lo que se hace en el lugar es una medida de búsqueda. El juez llega y se encuentra con cien computadoras. Acá hay dos caminos o llevarse todo que es lo que dijo el juez – lo cual es ridículo- o que alguien se ponga a buscar. Si la búsqueda es nada más una operación técnica que pueda hacer cualquiera estamos más o menos dentro de lo normal; si en la búsqueda tengo que llamar a un experto forense para que aplique software y hardware especial de búsqueda estamos muy parecido a algo que llamaríamos una mini pericia, una pericia chiquita, lo que a los expertos les gusta llamar triage, que es una operación en el lugar para determinar qué de todo esto sirve y qué no. Y esto no está habilitado en el Código Procesal. Ahora la pericia si está prevista o sea que si vos te llevaste la computadora, si vos ya te llevaste el aparato, no hiciste las operaciones en el lugar, yo no veo por qué no se podría mandar a un perito a buscar datos dentro de esa computadora, es una operación técnica sobre un aparato.

Fernando Díaz Cantón: Pero es un acceso a un sistema o un equipo informático

Marcos Salt: Pero si no es lo mismo que cuando le entrás con una pericia posterior a cualquier elemento que lo mandas a peritar. Porque no tenés herramientas como jurista para analizarlo sin

recurrir a un especialista, pero te llevaste el aparato físico avalado por una norma y después hacés una pericia que pasa a ser una operación técnica que sí está prevista en el código.

Fernando Díaz Cantón: pero implica un acceso a un sistema informático de acceso restringido.

Marcos Salt: Si uno analiza el tema desde un punto de vista netamente académico tenemos problemas entre el principio de libertad probatoria y la nulla coactio sine lege. Es cierto que el principio de libertad probatoria te permite extender y eso está en tensión todo el tiempo, en el fondo la discusión es esa. El principio de libertad probatoria contra nulla coactio sine lege y la interpretación que vos hagas de esto, y de que intérpretes qué significa la pericia. Ahora lo que sí queda claro es- y esto es un error que se ha cometido muchísimo- que llevarse la computadora no es entrar en la información. El secuestro de un teléfono o una computadora no implica la posibilidad de ingresar a su contenido sino que requiere una orden judicial adicional.

Fernando Díaz Cantón: uno se podría replantear la relación del Estado con el ciudadano y decir que en el pasado el Estado era más fuerte frente al ciudadano débil. Pero cuando la policía ingresa a un domicilio a las patadas, uno lo oye , los vecinos escuchan; cuando uno entra en un entorno digital esto es absolutamente silente, es decir que la vulnerabilidad de esta nueva forma de la esfera de privacidad que tenemos ahora requiere de una mayor protección. O sea que si la Constitución histórica exigía una ley especial con los casos, con los justificativos, mucho más se tiene que exigir ahora.

Tercer supuesto: ¨suponga que la orden judicial para realizar el allanamiento a una de las compañías tiene como objetivo secuestrar toda documentación o información tanto física como contenida en archivos informáticos relacionadas con el delito investigado. Al comenzar con las tareas de análisis el sistema informático de la empresa comprueba que los archivos que le pueden ser de utilidad se encuentran almacenados en un servidor ubicado en otra provincia o en un país extranjero. Aunque usted puede acceder desde la terminal ubicada en la sede de nuestro país que es objeto de allanamiento ¿es posible continuar con el registro y secuestro de datos o deberán utilizarse los mecanismos de cooperación interjurisdiccional?".

Cristina Caamaño: acá tiene que ver con el delito, si el delito es trasnacional como si fuese el narcotráfico, la trata de personas o algún tipo de secuestro extorsivo, sí voy a poder acceder; si no, no.

Fernando Díaz Cantón: Yo creo que la única manera de resolver esto es con los tratados de cooperación o colaboración internacional. Sobre todo en esto delitos que tengan que ver con la delincuencia organizada transnacional. Me parece que no queda otro camino que los convenios de colaboración. Convenios de colaboración que no se limitan a analizar la colaboración en sí, sino además si realmente existe doble incriminación, sino afecta la soberanía del otro estado. Hay una serie de cuestiones que hay que analizar y que en principio impiden avanzar salvo que exista una relación de reciprocidad clara y que no haya inconvenientes y no haya necesidad de tipificar en convenios de este tipo. Pero

me parece que es el principio del problema porque en este caso a lo mejor puede resolverse fácilmente pero en algún servidor que no sepa en qué país está estamos en una situación mucho más compleja que ya ahí no sé cómo se resuelve.

Marcos Salt: El criterio general que se está tratando de aplicar en el mundo es ver si el acto significó una actividad jurisdiccional de un Estado en otro. Por ejemplo, si implica destrabar una clave en el otro país no; si yo accedo libremente desde el lugar donde estoy sin destrabar la clave, sin mover nada, sí.Ahora en ley vigente todos los tratados de cooperación internacional prevén el régimen del exhorto con la doble incriminación. Entonces internet está yendo contra eso, contra esas normas. Entonces lo que hay que hacer obviamente es adecuar las normas. El problema es qué hacemos los operadores en el mientras tanto porque la información no está más acá en la Argentina. Dentro de cinco años cuando hagan un allanamiento, en la computadora no van a encontrar nada. Quedará todo en la nube.

Supuesto cuatro: una vez copiados los discos rígidos ordena que se realice un peritaje informático y envía los archivos informáticos a la división especializada de los delitos tecnológicos de la policía, al realizar el análisis de los archivos informáticos encuentra archivos de uno de los socios del estudio contable que muestra que hace dos años distribuyó archivos de pornografía infantil en una red de intercambio ¿es posible iniciar una nueva causa con la prueba así obtenida?"

Cristina Caamaño: Sí, claramente se puede iniciar una nueva causa.

Fernando Díaz Cantón: En la medida que se trate de un hallazgo casual, se puede de acuerdo a la doctrina de la ¨plain view¨.

Marcos Salt: tenés que hacer una nueva denuncia y el juez tendrá que evaluar si el encuentro fue casual o no. Si el encuentro fue casual la prueba se puede utilizar, si el encuentro no fue casual, no.

Supuesto cinco: "el experto le explica que los archivos pueden estar protegidos por un sistema de encriptación que difícilmente pueda ser descifrado y que parte del material se aloja en servidores fuera del domicilio, a los que sólo se puede acceder con las claves correspondientes. Por tal motivo le sugiere que solicite al juez una orden de registro y secuestro de datos mediante la instalación de un programa de recuperación de datos a distancia, troyano, en el sistema informático de los sospechosos con el fin de acceder a las claves de acceso, a lugares remotos de alojamiento de información y a las claves del cifrado de archivos. ¿Es la medida admisible jurídicamente?

Marcos Salt: Presencié una discusión entre jueces sobre este tema y fue muy interesante. El 70 % estaba por el no, casi todos diciendo que era un disparate que no podía ser eso de ninguna manera, hubo argumentos de que se parecía a una interceptación de teléfono. El problema que vos decís es una intercepción de teléfono, pero la intercepción de las comunicaciones es para las comunicaciones del futuro. Yo acá lo estoy usando para llevarme el archivo de Word que hiciste hace cinco años ¿en dónde hay una interceptación de comunicaciones? A mí me sigue pareciendo un error que esto

se pueda hacer por un tiempo como si esto fuera una intervención de comunicaciones. Yo estaría dispuesto a admitir la autorización para buscar un documento en el caso por ejemplo de utilización de anonimato, que yo ya se dé entrada que no voy a poder entrar. Digamos, si el perito me está diciendo aunque allanemos que yo no voy a poder entrar, yo podría hacer un acceso controlado para llevar un documento determinado. Pero no dejarle a la persona instalado en la computadora un programa troyano durante tres meses y que me mande todos los datos de lo que hace, a quién vio, etc.

Carlos Christian Sueiro: estaba pensando en que estaríamos todos de acuerdo como abogados que nadie puede interceptar las comunicaciones de otros, nadie puede entrar a la morada del otro, ni nadie puede interferir en las comunicaciones postales decía la ley, pero sí si el sistema ha autorizado a una persona que es el Juez a hacer todo eso. Ahora en la vida digital hay otras reglas y que si hay un criterio de proporcionalidad para lograr el objetivo seguramente el juez encontrará la manera de hacerlo por eso me parece razonable proceder de esa manera. Quería mencionar algo sobre una solución con la encriptación que están buscando los países. Después de los atentados del trece de noviembre de dos mil quince en París en donde el modo de reunión fue mediante mecanismo de encriptación que se realizó en las consolas de Wii que el Estado islámico lo utilizaba para intercambiar información encriptada reflotó una nueva idea de parte de Francia y también de Alemania que es tipificar como delito la encriptación. Y otro mecanismo que están utilizando para no utilizar el troyano, es geolocalizar a la persona que se está buscando, captarlo físicamente, saber dónde está y en el momento en el que ingresa a la computadora, o allanar el lugar, o si está en un lugar público, tomar la computadora.

IV. Panel participativo: Puesta en común de casos y experiencias compartidas en los laboratorios forenses

Departamento Cibercrimen de la Policía Federal 1: Era necesario dividir en dos grandes ramas las investigaciones tecnológicas que realiza la Policía Federal. Una es la que se dedica al delito tecnológico en general, que es la División del Delito Tecnológico. La otra es la División de Delitos Cibernéticos contra la Niñez y la Adolescencia, que trabaja con casos de grooming, pornografía infantil y trata de personas con fines de pornografía infantil, etc. -Esta última División cuenta con un grupo interdisciplinario de apoyo a la víctima compuesto por abogados, asistentes sociales, psiquiatras. Su función es asistir a la familia y dar una primera contención al momento del allanamiento, la detención y el resto de la actividad policial. En la parte de Delitos Tecnológicos, se empezó a hablar hace mucho tiempo y se comenzó a ponerle el nombre de lo que era la vigilancia tecnológica o ciberpatrullaje. Resulta que esto lo veníamos haciendo desde hace 15 años y no sabíamos que lo estábamos haciendo. Para darle una contención a esto, se creó la Sección Inteligencia Informática, uno de los nombres

que tuvo la Dirección de Delitos Tecnológicos hace mucho años atrás.

Antes, el producto de los allanamientos sólo servía para producir pruebas sobre las personas investigadas en la causa hasta ese momento, pero no para encontrar otras personas que podrían estar involucradas en la actividad delictiva. Entonces, entendimos que era necesario crear un laboratorio específico para el departamento de cibercrimen, con la diferencia que no vamos a realizar pericias sino que nos vamos a dedicar exclusivamente a la investigación de la evidencia digital obtenida.

La idea es que la prueba obtenida en el allanamiento pueda ser trabajada en forma urgente para continuar con la investigación y por eso salió la necesidad de crear una unidad móvil. Esta unidad va a servir para procurar elementos de evidencia digital que los operadores policiales normales no están capacitados para obtener y va a trabajar en los allanamientos que se hagan en Capital y el interior del país.

Hemos creado un área que va a hacer la capacitación para el personal nuevo y actividades de docencia respecto a la prevención de estos delitos en el tercer sector, ONGs, escuelas o academias.

En el caso M.J.[1] se comenzó por dos informaciones: una proveniente del Departamento de Justicia de los Estados Unidos -a través del FBI- y otra que venía desde Alemania. Ellos interpretaban que era producido en Argentina porque habían hecho una primera visualización, en donde aparecían elementos que los llevaban a pensar que estaba en el norte de Argentina.

Departamento de Cibercrimen de la Policía Federal 2: La información nos llegó a partir del departamento de Justicia, mediante un grupo de imágenes que habían sido obtenidas en un procedimiento. Estas imágenes mostraban la camiseta de un club de Argentina. Otro dato de interés que muchas veces es recolectado por los investigadores es la metadata. En este análisis teníamos la fecha, la hora y el equipo con el que había sido obtenida la imagen. Por otro lado, recibimos información, vía Interpol, de un caso que estaban investigando en Australia. Allí se obtuvieron documentos acerca de un usuario que se estaba conectando desde Argentina. Acá teníamos cuenta de correo, usuario de Facebook y la cara del victimario. De esta manera, descubrimos que estaba ubicado en Jujuy. Continuamos trabajando con fuentes abiertas, analizando los contactos que tenía el imputado. Allí encontramos dos contactos que eran una pareja amiga, que tenían un hijo, del cual el sospechoso era el padrino.

Departamento de Cibercrimen de la Policía Federal 1: Este chico no es el mismo que aparecía en la denuncia que venía de Australia-EEUU ni la que nos habían aportado desde Alemania, a través de una investigación que habían realizado en forma encubierta, con un agente encubierto digital. Esto salió del análisis de diferentes investigaciones que teníamos en nuestras unidades.

Departamento de Cibercrimen de la Policía Federal 2: Son cosas que van apareciendo sobre la marcha y que nos dan otros indicios. Más o menos teniendo una idea de que el victimario podría allí

[1] El caso M.J. trató sobre producción y distribución de pornografía infantil.

llegar, ser el que produce y distribuye... con todo eso se va armando el rompecabezas.

Departamento de Cibercrimen de la Policía Federal 1: Nosotros teníamos el interior del lugar y teníamos un vehículo en donde se veía la madre del menor. En el trabajo nuestro de campo, encontramos una casa que haciéndola al revés, teníamos la ventana y la puerta, del mismo tipo de ventana, del mismo tipo de postigos, y al mismo tiempo el vehículo del cual no teníamos dominio porque estaba pixelado. Pero encontramos un vehículo, vivienda, que era parte externa y que tenía relación con las imágenes del cumpleaños del menor que estábamos pensando también podía ser víctima.

Departamento de Cibercrimen de la Policía Federal 2: A través de las imágenes, aparece otro actor más, que es otro niño. que había aparecido en un video aportado por Australia. De los comentarios que aparecen en la foto, aparecen cuatro niños y en el comentario aparece el nombre de cada uno. Empezamos a analizar otros usuarios con el mismo apellido de quien teníamos como imputado y nos aparece que este usuario sería el hermano, y nos aparece una geolocalización que coincidía con las IP que nos daba para el imputado.

Departamento de Cibercrimen de la Policía Federal 1: Cuando un operador judicial mira las imágenes o los videos, lo primero que le llama la atención es el niño siendo víctima pero hay que mirar todo. Porque la presencia de un piso específico, de un techo, un aparato de televisión, de un cobertor de la cama, etc., nos va a poder determinar que un lugar que allanamos es el lugar donde se produjeron las violaciones o los abusos. Es decir, el tema del análisis es muy importante pero el trabajo del investigador de ver las circunstancias de hecho es fundamental.

Departamento de Cibercrimen de la Policía Federal 2: Ante este fundamento, no suena tan descabellado cuando nosotros pedimos como medida filmar toda la casa o sacar fotos de todos los ambientes, porque en la pericia posterior podemos encontrar imágenes que fueron sacadas en este ambiente. Bueno, acá tenemos datos aportados por uno de los proveedores donde se alojaban algunas de las imágenes denunciadas. Acá el tema de la cuenta de correo electrónico, las IP, ya teníamos el lugar de conexión, la geolocalización, esto nos daba ya en la parte del lugar sospechado, en las afueras de la ciudad. Respecto al allanamiento, esta fue una de las primeras medidas que tomamos, donde llevamos personal especializado porque sabíamos que el menor estaba en ese hogar. La medida fue hecha a primera hora de la mañana, a las cinco de la mañana, porque este muchacho iba a trabajar a las seis. Entonces irrumpimos, inmediatamente el personal especializado fue a contener al menor, lo sacó del lugar y lo puso en lugar a resguardo.

Departamento de Cibercrimen de la Policía Federal 1: Es importante tener en cuenta la rapidez que nos da la cooperación internacional. Imagínense que obtener esa información que nos vino de Australia, que nos vino de Alemania, que nos vino de Estados Unidos, si hubiera sido a través de la obtención de una rogatoria, para que ese cuerpo que habían obtenido de elementos en Australia lo pasaran a través de Cancillería, esos chicos hubieran estado siendo vulnerado durante tres, cuatro, cinco años más. ¿Qué herramientas tenemos ahora que en esa época no teníamos? Esto para que

se den una idea, la condena fue hace un año y medio y lo investigamos un año y medio atrás. Hoy tenemos una herramienta que nos facilitó Interpol que es una base de datos que se llama ICSEC. Hasta hoy lo que teníamos era el FTP del NCMEC que baja en el Ministerio Público de la Ciudad, que tira información de denuncias. Te da unos datos básicos técnicos, las imágenes, pero nada más. La diferencia con el ICSEC es que ahora nos permite trabajar sobre las imágenes, compararlas con otras investigaciones que se están haciendo en este momento, verificar si las imágenes son nuevas, verificar si las imágenes fueron tergiversadas para que no se obtengan metadatos.

Departamento de la Policía Federal 2: ICSE es una base cooperativa y es alimentada por todos los países que forman parte del convenio Interpol y que adhieren a esta base de datos. Es alimentada por los resultados de los allanamientos, se suben estas imágenes obviamente con una orden judicial, y lo que hacen los investigadores o los grupos de trabajo de cada país, es analizar estas bases, estas fotos, y tratar identificar víctima y victimario, o por lo menos geolocalizarla para que por lo menos el país que le corresponda pueda tomar una intervención. Esta imagen es subida cruda, como se la encuentra, entonces hay muchísima información que tiene sus metadatos e incluso hay alguna que tiene hasta el geoposicionamiento de la imagen, y eso facilita muchísimo llegar a intervenir. Lo que hace esta base es hashear todas las fotos, generar todo una tabla de hashes de todas las imágenes, también trabaja con Photo DNA, o sea tenemos distintas maneras de abordarla. Entonces, yo tengo un gran caso, la justicia me provee de mucho material, yo puedo hashear todas mis imágenes y directamente comparar con los hashes de la base de datos y tengo un proceso sumamente rápido y de esa manera yo puedo establecer si alguna de las imágenes que yo he secuestrado ya están en la base y si están en la base puedo consultar y ver qué es lo que ha pasado, si esas imágenes fueron o están ahí cargadas y tildadas como que fueron distribuidas por tal usuario de tal país, si víctima o victimario están identificados... Una cuestión muy interesante es que en lo que se carga en la base de datos, hay imágenes de fotos o videos, que son del 2008, 2009, o sea, que ya la víctima hoy en día ya es mayor de edad, pero hay otro caso que nos está pasando dónde analizando imágenes hemos llegado a la víctima, pero resulta que el victimario está muerto. Entonces se nos plantea el conflicto de qué pasa con víctima, porque nosotros trabajamos también para rescatar a la víctima, entonces ahí tenemos un gris muy importante, sobre el que habría que trabajar, porque muchas veces al no haber victimario se corta la acción.

Departamento de Cibercrimen de la Policía Federal 1: Y si se da que el victimario está muerto, el operador judicial dicta el sobreseimiento en la causa, pero nosotros no queremos que se termine la causa porque necesitamos encontrar a ese chico, por la sencilla razón de que no sabemos si es el único victimario y si el muerto fuera el único victimario, hay que conseguir que esa víctima reciba el tratamiento psicológico, psiquiátrico, médico correspondiente.

Moderadora: ¿Alguien tiene alguna pregunta para los expositores?

Pregunta del público: ¿Tienen la experiencia de una orden en la que digan llevensé también o

revisen a la gente si tienen algo extraíble encima o saquenle los teléfonos para que no puedan modificar nada?

Departamento de Cibercrimen de la Policía Federal: Hay una diferencia muy grande cuando hay una reunión con los técnicos antes que la orden de allanamiento se labre y cuando los técnicos se enteran de la orden al momento de recibirla.

Pregunta del público: ¿Qué tan seguido ocurre la reunión previa?

Departamento de Cibercrimen de la Policía Federal: No tanto. En nuestras investigaciones sí pero lo que hay que entender es que hay investigaciones que hacemos nosotros pero otras en donde el delito no es específicamente tecnológico sino que tiene un componente tecnológico. En estos casos, como se sabe que es posible que en un allanamiento se encuentren computadores, nos piden que enviemos a alguien de nosotros a colaborar. Es un abanico muy grande de cosas que suceden pero lo más importante es que haya una relación amplia entre el operador judicial y el investigador policial. En el tema de la pericia, cuando hablamos de ella, es una actuación técnica para obtener una prueba de cargo. Ahora, nosotros estamos hablando de investigaciones en un ambiente digital, no una pericia. Porque todos los actos de los que hablamos son reproducibles, yo estoy haciendo una operación que internacionalmente se sabe que no afecta al original del secuestro, que es la obtención de la copia forense bit a bit, y después busco ahí y si encuentro que está cometiendo otro delito, tengo la obligación de informarle al juez. Si no le damos a las fuerzas policiales las herramientas como para producir lo más parecido a la verdad...después hay control de la legalidad de los actos.

Policía de la Ciudad: La División de Análisis de Investigaciones Especiales es lo que antes se conocía como Cibercrimen de la Policía Metropolitana. Tras la unificación de fuerzas, se crea la Policía de la Ciudad y lo que era cibercrimen pasó a ser una Superintendencia. Esto significa que se amplió mucho la capacidad. Todo lo que hacíamos en una sola área ahora lo hacemos en nueve. El objetivo es que en cada área se encarguen específicamente de un tema y sean profesionales de ese tema. Respecto al caso, voy a contar un caso que quizás ya lo escucharon. Va una persona a comer a una parrilla y se olvida el celular. La camarera lo encuentra y lo lleva a la Comisaría porque el celular contenía imágenes aberrantes. La Comisaría da aviso a la Fiscalía, la cual nos entrega el teléfono. Nosotros hacemos la extracción de toda la información para resguardar la evidencia. El teléfono tenía chip a tarjeta, así que no había domicilio de facturación. Entonces, empezamos a buscar en las fotos algún indicio que nos permitiera dar con su ubicación. Ahí vimos que una de las fotos tenía la posición GPS de donde la sacaron y se veía un boletín de calificación. Fuimos a la escuela y pedimos el listado de los alumnos. Allí, había tres que no tenían Facebook, lo cual nos pareció sospechoso. A dos los ubicamos enseguida pero a uno no. En la escuela nos mostraron un papel en donde pedía una constancia de alumno regular y había dejado un número de teléfono. Hablando con la Fiscalía y por intermedio del Juzgado nos autoriza a hacer tareas telefónicas y tareas de encubierto, con el fin de encontrarlo. No es ya llamar a ver si vive o me paro en la puerta a ver si entra. Ya era llamar por

teléfono, ver cómo puedo sacarle datos... pero bueno. ¿Qué hacemos? Vamos a llamarlo y decirle que somos de una Universidad, que tenemos una beca y que le íbamos a dar una tarjeta de débito para que todos los meses saque plata y una notebook para que estudie y que tenía que cursar dos materias anuales.

Acordamos un encuentro con él y mientras tanto, obtenemos una orden de allanamiento. Ese día estaba él con sus parientes pero no estaba el niño de los videos. Nadie sabía donde vivía porque era la casa de la tía. Lo único que había era un teléfono. En ese momento, llamamos al juzgado a que nos autoricen a extraer información del teléfono. Empezamos a ver videos y fotos que tenían geolocalización, que era a dos o tres cuadras. Entonces, vamos y empezamos a preguntar si reconocían al nenito, hasta que la madre lo reconoce. El autor vivía en un local que le alquilaba a los padres del nene. Como ellos trabajaban, se lo dejaban a su cuidado. Al otro día, nos dan la orden de allanamiento y se hacen las comparaciones entre los ambientes. El autor fue detenido y condenado.

División Apoyo Tecnológico de la Policía Federal: En la división Apoyo Tecnológico tenemos dos grandes áreas: computación y teléfono. Al margen de las pericias, prestamos cooperación en campo a los agentes de policía. Me pareció interesante lo que se decía acerca de que "no se puede cortar la empresa"...Si no se puede cortar la empresa, yo no puedo hacer nada porque para buscar algo tengo que aislar ese servidor. Hay que plantear para qué se hace la imagen forense en el lugar. La imagen forense, a mi entender, es un mero documento de trabajo que me sirve como perito para buscar información. En un caso de homicidio, el muerto es la prueba y la tomografía son los datos que estudia el médico. Si un perito de parte me quiere plantear la imagen forense y la quiere hacer de vuelta, no va a poder porque ya se devolvió al usuario el disco rígido. Las mejores experiencias se dan cuando nos sentamos con los jueces y decimos lo que sirve y lo que no. Existen jueces que creen que nosotros podemos vender la causa pero a nosotros no nos interesan saber el domicilio, la empresa o quién es el imputado. Lo que nos interesa es saber con qué nos vamos a encontrar cuando llegamos o saber qué es lo que se quiere buscar. En ese sentido, necesitamos el respaldo de la Justicia. Si hay que parar algo, hay que pararlo. Hay grandes jueces que han hecho parar empresas de telecomunicaciones porque no se puede acceder a la información. El 90 % de las financieras acusadas de lavado de dinero tienen servidores en Panamá y actualmente estamos debatiendo cómo acceder a ellos. Han caído personas importantes y mientras estamos en el allanamiento, cierran la conexión con Panamá y no se llega a nada. Tenemos que empezar a trabajar en equipo y entender que hay tiempos que no se pueden apurar.

V. Conferencia final

Daniel Petrone (Camarista del Tribunal Oral Federal N° 2 de San Martín): Existe una discusión en relación al balance entre privacidad y seguridad. Existen en la delincuencia digital delitos tan

aberrantes en los que seguramente estamos dispuestos a ceder mucho más en pos de la seguridad. Pero lo cierto es que afuera de esos supuestos, hay un montón de circunstancias, en las que ninguno de nosotros se sentiría cómodo autorizando medidas que implican meterse en datos sumamente íntimos. Es verdad que vivimos en la época de la "*extimidad*"[2] como le dicen algunos, en la cual hay una exhibición de determinados datos. Pero por otro lado, hay la necesidad de preservar determinados datos como herramienta fundamental para poder decidir un plan de vida en un contexto de razonable libertad. Ese balance nuestros procesalistas clásicos lo tenían resuelto. Un ejemplo de ello es la fórmula clásica según la cual, para entrar forzadamente a una vivienda, se necesitan motivos bastantes para sospechar razonablemente que ahí se encuentran elementos relativo a un delito. Pero para entrar en los datos conservados en un teléfono, no hay un estándar tan unívoco. Y en un contexto en donde casi todos nuestros datos se conservan en teléfonos, el allanamiento de una morada, aparece en supuestos de delincuencia informática, casi como una obsolescencia.

En este contexto, podríamos pensar en ciertos criterios de proporcionalidad en las investigaciones que se desarrollan. A todos nos han formado bajo la premisa de la imposibilidad aplicar criterios de oportunidad procesal entre las distintas acciones penales. Pero tal vez tenemos que empezar a discutir si no hay que tener algún criterio de proporcionalidad que pueda aplicarse en algunos casos. Una pregunta que les puedo hacer es ¿es posible analizar esta realidad con las reglas que ahora tienen ustedes? ¿O tenemos que pensar en reglas nuevas? En criterios de proporción, en algo que nos dé certidumbre. Las posibilidades probatorias son infinitas y por eso, hay que analizar los casos para ver cómo juega la tensión entre seguridad y privacidad.

[2] El término "extimidad" es un neologismo acuñado por el psicoanalista Jacques Lacan y se refiere a la tendencia de las personas a hacer pública su intimidad. Con el desarrollo de las redes sociales el término ha recobrado popularidad en su uso.