LA EXTRACCIÓN DE INFORMACIÓN CONTENIDA EN DISPOSITIVOS DE ALMACENAMIENTO DIGITAL

ANALISIS EN TORNO A LAS LIMITACIONES EN LAS INVESTIGACIONES PENALES. LA NECESIDAD DE UNA REFORMA EN EL CÓDIGO PROCESAL PENAL DE SANTA FE

Matías ***Ocariz***

Fiscal - Ministerio Público de la Acusación de Santa Fe

Resumen

La investigación penal transita un cambio de paradigma donde la evidencia digital cobra una importancia que nunca antes tuvo. Esto requiere una reforma urgente del Código Procesal Penal de Santa Fe, a pesar de que este tipo de evidencia pueda utilizarse en razón de lo dispuesto por el art. 159, del citado cuerpo normativo. Los dispositivos que almacenan información masivamente son verdaderas "cajas negras" de nuestras vidas, conteniendo abundante información íntima, protegida por la expectativa razonable de privacidad. El dilema medular se centra en la imposición de límites ex ante (previos a la búsqueda) o controles ex post (posteriores a la búsqueda) al análisis de la evidencia digital que se encuentra en esos "contenedores". Se desaconsejan fuertemente los límites ex ante debido a la naturaleza impredecible y altamente manipulable de la evidencia digital. Las partes, en todo caso, siempre tendrán la posibilidad de cuestionar la razonabilidad y proporcionalidad de la búsqueda a posteriori.

1.- Introducción

Hoy no podemos negar que la evidencia física, en cualquier tipo de investigación, está siendo reemplazada (en algunos casos totalmente) por la digital. Esto viene ocurriendo desde hace ya mucho tiempo, siendo un fenómeno que se acrecienta de manera exponencial. Sin duda alguna estamos en presencia de un *cambio de paradigma*. Y tomo esta última palabra como lo que significa, es decir el *". . . conjunto de teorías cuyo núcleo central se acepta sin cuestionar y suministra la base y el modelo para resolver problemas y avanzar en el conocimiento"*[1].

Ya lo predecía Nicholas Negroponte, cuando en su libro "*Ser digital*", publicado en el año 1995, sostenía que el mundo se inclinaba hacia la *"digitalización"*, trasladándose de los *átomos* hacia los *bits*.

No es un secreto que la tecnología cambia a pasos *agigantados*, no solo aquella de la que hacemos uso cada día, sino también la que utilizamos en la investigación criminal[2].

Lo expuesto es también sostenido por otros destacados autores, como es el caso de María Florencia Suarez[3], cuando nos indica que *". . . a corto plazo, la evidencia en cualquier causa penal, ya no va a ser física, sino solo evidencia digital. . ."*.

Un ejemplo claro de ello está dado por las *cámaras de seguridad*. Los operadores jurídicos siempre lidiamos contra las fallas de percepción de los testigos, su falta de memoria o hasta incluso sus miedos a la hora de prestar declaraciones, mientras que los registros contenidos en las cámaras *(que hoy presentan una gran proliferación en la vía pública y en espacios privados)* muestran la realidad tal cual ocurrió, cualquiera sea el tiempo transcurrido y sin ningún sentimiento ni sesgo cognitivo que las altere.

Con esta reflexión no pretendo sostener que se terminará la prueba de testigos en los debates orales, pero sí que la evidencia digital aportará mayor credibilidad a sus dichos. Incluso, los testigos seguirán siendo necesarios durante el debate, de modo de posibilitar la incorporación de ese tipo de evidencia al juicio oral.

En nuestros días no hay investigación criminal que no tenga, como potencial prueba, información contenida en dispositivos que almacenan evidencia digital *(computadoras, celulares inteligentes, memorias, discos rígidos, etc.)*. Este cambio rotundo de las evidencias que se recolectan en las investigaciones penales y que eventualmente luego llegan a los juicios orales, exige que deban repensarse algunos institutos que se vienen aplicando al mundo material, sobre todo en lo que tiene que ver con las invalidaciones, la aprovechabilidad de la evidencia, con su análisis y con su

utilización concreta en audiencias y debates.

En este contexto, se hace *necesaria una reforma en el Código Procesal Penal de la Provincia de Santa Fe*, que aborde todos los métodos de investigación disruptivos. Si bien, la *libertad probatoria*, regulada por el artículo 159[4], del citado cuerpo normativo, permite la aplicación de este tipo de medidas investigativas, no es suficiente a los fines de regular su correcta aplicación en casos concretos.

En efecto, se trata de enormes volúmenes de información, mucha de la cual excede el *objeto* de la investigación, lo que genera un inconveniente en tanto que en numerosos casos versa sobre datos que se encuentran cubiertos, en mayor o menor medida, por la *expectativa razonable de privacidad*.

La pretensión del presente artículo es indagar sobre las premisas jurídicas que deben guiar nuestro accionar al momento de analizar esa información. En algunos países la legislación, la doctrina y la jurisprudencia en la materia están muy desarrolladas, mientras que, en otros, no tanto.

Para cumplir con este objetivo, me propongo *bucear* a través de las diferentes respuestas que se fueron dando en algunos de los sistemas jurídicos del mundo, para luego llegar a conclusiones que nos orienten en la tarea investigativa basada en evidencia digital, que de estar siempre enmarcada en el respeto de la privacidad. De ese modo, pretendo brindar soluciones que sean de utilidad en la labor diaria de los operadores de los sistemas penales, con independencia de la jurisdicción en la que se desempeñen.

Este camino estará signado por muchas preguntas, las que no pretendo agotar en este ensayo, aunque si sumergirme en la siguiente: *¿Pueden imponerse límites a la hora de introducirnos en el análisis de información contenida en dispositivos de almacenamiento masivo de evidencia digital?*

En esa dirección, primeramente es necesario recurrir a las *fuentes* de derecho, y en ese sentido, resultan útiles los principios generales, y también a la doctrina y jurisprudencia comparada, que mucho tienen para enseñarnos. Cabrá también valerse de las *transpolaciones* que puedan realizarse de las normas que rigen la recolección de evidencias en el mundo físico (tal el caso de allanamientos, requisas y secuestros, entre otras); pero siempre teniendo en consideración la permanente tensión que existe entre *la necesidad de una investigación penal eficaz, y el resguardo de las garantías constitucionales y supra constitucionales*, y en este caso en lo que refiere, principalmente, a la *expectativa razonable de privacidad.*

Sentado lo expuesto, no podemos negar la realidad en cuanto a que los dispositivos de almacenamiento digital (y principalmente los teléfonos celulares inteligentes) contienen, hoy en día, una gran cantidad de información personal, constituyéndose en verdaderas *"cajas negras"* de nuestras vidas. Se resguardan allí conversaciones con familiares, amigos o parientes, hobbies, intereses literarios, intereses deportivos, viajes, problemas de salud, traiciones, infidelidades, etc.

De ese modo, resulta necesario observar cómo debe realizarse el análisis de los datos existentes en dichos dispositivos, ya sea que fueran secuestrados o bien extraída su información *(copia forense bit a bit)* en el lugar donde se encuentren, en el marco de lo que hoy se denomina como *"Derecho a la protección del entorno digital"*, concebida como una nueva categoría constitucional, tal como lo grafica la Sentencia de la Sala de lo Penal del Tribunal Supremo Español[5].

Así, teniendo en miras los inconvenientes que lo trazado genera, y el debido respeto de las garantías constitucionales, me adentraré en los parámetros y criterios que pueden marcar un camino, acudiendo para ello a la legislación, la jurisprudencia y la doctrina desarrollada en los países que más adelantos han tenido al respecto. Por lo demás, y considerando el alcance transnacional que tienen las investigaciones de ciberdelitos y que involucran evidencia digital, debemos alentar a aunar criterios, que permitan investigaciones más rápidas y eficaces.

2.- Distinciones entre el espacio físico y el espacio digital.

Para empezar a delimitar la cuestión, conviene entender las grandes diferencias que existen para la recolección de la evidencia en el mundo físico y en el mundo digital.

2.1.- El *espacio físico* vs. el *espacio digital*.

Registrar un dispositivo de almacenamiento masivo presenta una dinámica muy diferente a la de un allanamiento de morada. En efecto, para el registro de un domicilio o una finca se requiere que el personal policial ingrese en ella. Lo mismo ocurre con un objeto que se encuentra dentro de un contenedor, que es registrado cuando este se abre. Una casa es registrada cuando un agente del gobierno entra en ella, un *paquete* es registrado cuando un agente del gobierno lo abre[6].

Por otra parte, un dispositivo de almacenamiento masivo se diferencia de un inmueble en tanto que guarda una gran cantidad de información que, a veces, es incluso *desconocida para su dueño*. Un ejemplo claro son aquellos *softwares* que almacenan *metadatos* sin que los usuarios lo sepan, estando programados por defecto para hacerlo de esa manera (sitios *webs* visitados, motores de búsqueda, favoritos, claves de acceso, etc.). Normalmente una persona tiene un mayor control de los objetos que tiene en su hogar, dentro de un limitado espacio físico, mientras que no ocurre lo mismo con un dispositivo, que se convierte, como decía más arriba, en una verdadera *caja negra* de la vida de las personas.

Frente a estas realidades, es fácil advertir que la recolección y el análisis de información difiere sustancialmente ya sea que se trate del espacio físico o del espacio digital. Por lo tanto, el desafío radica en *determinar qué posibilidades de selección de la recolección y el análisis nos permite cada espacio*, y de esa manera determinar *qué límites nos podrá enfrente el respeto de la privacidad.*

2.2.- Los diferentes modos de almacenamiento. La copia *bit a bit*.

Cuando refiero a una copia *bit a bit*, estoy haciendo alusión a aquella que se realiza en relación a todas y cada una de las secciones de un dispositivo de almacenamiento digital, y que replica todos los sectores, incluso los que están vacíos o son lógicamente defectuosos (por ello también se la conoce como *clonación sector por sector*).

Luego de realizada la copia *bit a bit*, nos vamos a encontrar, en una primera etapa de identificación y preservación de la evidencia, con algo que podría compararse con un sistema de *celdas*, donde cada una contiene un *uno (1)* o un *cero (0)*. Estos son los llamados *bits*, y lo que se observa en esta primera instancia son los estados lógicos de los espacios de

almacenamiento, y solo eso. Si ellos no se reúnen, si no se combinan, no podemos saber de qué se trata, que es *lo que forman* (una imagen, un video, un texto, etc.). El objetivo de esta primera etapa de análisis es realizar esa imagen forense *("copia bit a bit")*. El *bit* es la unidad mínima de almacenamiento en un sistema de archivos. No es la pretensión de este ensayo ahondar sobre esta cuestión, pero si es importante saber que las unidades mínimas de almacenamiento pueden ser *bits, bytes (ocho bits)* o *clusters (cuatro mil bytes, el más común de ellos)*, y que con su sola observación a ninguna conclusión se puede arribar, ni se puede saber frente a que *objeto* nos encontramos. Mirando las *unidades mínimas de almacenamiento* en forma conjunta no podemos determinar si nos encontramos frente a una foto, a un archivo de word, a un archivo .pdf, etc. Las herramientas forenses que nos permiten realizar extracciones *bit a bit* (como Encase, FTKimager, Axion Magnet, etc.) no nos mostrarán más que *unos y ceros*. Incluso un determinado archivo puede estar en distintas partes del dispositivo de almacenamiento, y es necesario juntar esas partes para que el objeto pueda ser representado en un monitor. Esto se logra a través de la *tabla de partición*. Esos unos y ceros pueden ser convertidos por una computadora en una letra, un número, un símbolo, un pixel, etc. Por ejemplo, la letra *"m"* sería almacenada por una computadora como *01001101* y el número *"6"* como *00110110*[7]. No se ingresa físicamente a una computadora (como a un inmueble), no se mueven objetos dentro de ella, solo se observan unos y ceros, que se copian, para luego ser procesados.

Además, y para marcar mayores diferencias, la copia que se haga de la información contenida en el dispositivo puede ser *física* o *lógica*. La primera es *bit a bit*, mientras que en la segunda se copian carpetas y archivos, y permite recuperar archivos *borrados* (suprimidos de forma no segura), o información de partes del dispositivo que no estén formateados o asignados.

En mundo digital está conformado por ceros y unos, en el sentido que todo en él es información, y tampoco hay fronteras materiales para limitar y dar forma a los espacios.

2.3.- Los procesos de búsqueda en ambos espacios.

Las viviendas ofrecen regiones físicas predecibles y específicas para las búsquedas en esos lugares. El personal policial puede ingresar a través de la puerta o ventana, y caminar de habitación a habitación, registrando cada una, primero observándola visualmente, y luego abriendo placares y cajones. El mecanismo básico es recorrer el espacio físico, mirando y moviendo elementos materiales de modo de exponer pertenencias adicionales a la observación visual. Ingresar, observar y mover[8]. En este tipo de registros el personal actuante sólo registra los espacios donde aquellos objetos buscados pueden ser hallados y luego se retira del lugar. De ese modo, en este tipo de búsquedas no se podría abrir un cajón si lo que se está buscando es un automóvil.

Por el contrario, el análisis en el entorno digital, salvo contadas excepciones, se realiza en un laboratorio, y el objeto es buscado entre una gran cantidad de datos almacenados, que pueden estar "*escondidos*" o *encriptados*. Así, se advierte que la cuestión acerca de *donde efectuar el registro* es mucho más fácil de resolver en el espacio físico que en el digital.

En tal sentido, una orden de allanamiento sobre un espacio físico puede limitar las búsquedas mediante el señalamiento del objeto que se pretende encontrar. Sin embargo, registrar un dispositivo de almacenamiento digital en busca de datos trastorna ese supuesto.

Teniendo en cuenta las posibilidades de guardado de información, por ejemplo, en un disco duro, esa individualización del objeto ya no es útil a los fines de poner límites, ya que la evidencia buscada puede encontrarse en cualquier espacio del dispositivo analizado.

3.- Limites al análisis de información contenida en dispositivos de almacenamiento digital. Pautas para el establecimiento de sus justos límites. *La expectativa razonable de privacidad* como *faro*.

Continuando con en el objetivo del presente trabajo, es importante determinar el faro que debe guiar nuestras decisiones en cuanto a *cómo* realizar el análisis de información contendida en dispositivos de almacenamiento masivo.

Ese *norte* al que nos referimos está dado por la *expectativa razonable de privacidad*. Es a partir de allí que debemos dar cuenta de los límites constitucionales que encontramos al adentrarnos en la tarea de analizar evidencia digital.

Dicho concepto fue desarrollado en el Fallo "*Katz*", de la Corte Suprema de los Estados Unidos[9] , y se encuentra consagrado como garantía en casi todas las constituciones del mundo civilizado, siendo de igual manera receptado ampliamente por abundante doctrina y jurisprudencia.

En *Katz* la Corte Suprema de EEUU delimitó este concepto. En cuanto a los hechos del caso, el acusado estaba siendo investigado por transmitir, telefónicamente, información sobre apuestas. Las llamadas se realizaban, normalmente, de una *cabina telefónica pública*. Entonces, *agentes estatales* (los encargados de las investigaciones en EE.UU.) colocaron, en ese recinto, un dispositivo para grabar esas conversaciones. La particularidad, y con ella se defendieron, es que el micrófono estaba ubicado *fuera de la cabina*. Pero la Corte Suprema considero que la 4ta. Enmienda[10] protegía *a las personas y no a los lugares*, por lo que se consideró que dicha medida debió contar con la autorización judicial. El Juez Harlan (primer voto) entendió que lo que se protege es *la razonable expectativa de privacidad de las personas*. Además, estableció que debía realizarse un doble juicio. El primero de ellos *subjetivo*, considerando si el individuo en particular tenía esa expectativa. Y si ese juicio se confirmaba, debe pasarse al juicio *objetivo* en cuanto a determinar si la sociedad reconoce en el caso esa razonable expectativa. Entonces, en este caso, *lo determinante fue la cabina, con puerta, que el imputado cerraba cada vez que hablaba.*

Algunos de los instrumentos internacionales de Derechos Humanos que consagran la mencionada garantía son: *(i) La Declaración Universal de Derechos Humanos en su artículo 12*[11]*; (ii) El Pacto Internacional de Derechos Civiles y Políticos en su artículo 17.1*[12]*; y (iii) La Convención Americana sobre Derechos Humanos en su artículo 11.2*[13]. De allí pueden extraerse cuales son los límites que se imponen al Estado al momento de llevar adelante investigaciones penales, siendo que todos los instrumentos que se mencionan tienen rango constitucional, como es el caso de la República Argentina, conforme lo dispuesto por el art. 75, inciso 22, de la Constitución Nacional.

Es importante tener en cuenta, entonces que está vedada cualquier tipo de *injerencia arbitraria* en la vida de las personas. Y - en lo que hace a la materia en estudio - éstas lo serán en tanto y en cuanto no exista una causa probable (plausible) para entrometernos en

esa privacidad, enmarcada en la expectativa razonable de respeto que se tiene sobre ella. Y ello conlleva a la obvia conclusión de que cualquier intromisión debe realizarse con autorización judicial.

Sin embargo, la discusión pasa por la validez de las *limitaciones* que esos permisos puedan imponer cuando se trata de *búsquedas que deben realizarse en el particular entorno digita*l de los dispositivos que almacenan este tipo de evidencia.

3.1.- Protocolos de búsqueda. Limites *ex ante* y controles *ex post*.

Hay dos formas de regular la búsqueda de la información almacenada en dispositivos, las que se caracterizan por el establecimiento de restricciones *ex ante* o bien, de controles *ex post*.

La estrategia *ex ante* tiene por objeto fijar protocolos para regular registros informáticos, determinando los pasos precisos que los analistas forenses pueden realizar cuando llevan a cabo el proceso de búsqueda. En tal sentido, las órdenes podrían indicar *dónde, cómo* y respecto de *qué elementos* puede realizarse la búsqueda. La limitación *ex post* se basa, en cambio, en las normas de revisión del proceso de búsqueda una vez encontradas las evidencias. Bajo este enfoque, los tribunales revisarían el proceso de búsqueda en la fase posterior a que la evidencia ha sido hallada.

Para analizar dichos procesos y entender si es posible su aplicación, deberemos adentrarnos en algunos conocimientos que pertenecen al área de las ciencias informáticas. No olvidemos que estamos intentando fijar los límites para el análisis de información contenida en un entorno digital, y ya pudimos ver las diferencias que se presentan en cuanto al espacio físico. De lo que se trata, en definitiva, es de determinar si estos protocolos de búsqueda o limitaciones *ex ante* pueden ser legítimamente ordenados.

En esa dirección, es importante tener en cuenta que en el entorno digital la información puede ser *"escondida"* de muy diversas maneras, y con mayor facilidad que en el espacio físico. Esto provoca que el proceso de análisis forense presente una naturaleza *altamente contingente e impredecible.*

Para graficar lo expuesto podemos analizar algunos ejemplos. Uno de ellos es la *fecha de creación de un archivo*, la que es fácilmente modificable, ya sea porque la persona investigada lo haga con el propósito de esconder una evidencia, o bien por el simple hecho de que el dispositivo tenga la fecha modificada (lo cual incluso podría ocurrir sin intención alguna de su dueño, como en el caso de agotamiento de la batería que sostiene ese sistema). Otra característica fácilmente modificable de un archivo es su *extensión* (después del punto), y por ende la posibilidad de que el mismo se pueda visualizar. La extensión del archivo le *indica* al sistema operativo el tipo de contenido y con qué *software* debe ser abierto. Si se cambia la extensión, el sistema operativo va a continuar los intentos de abrirlo con el programa que "entiende" adecuado, sin analizar su contenido. Relacionado con ello, también se puede ocultar evidencia *escondiendo determinados tipos de archivos* (con una extensión determinada) *en otros con una extensión diferente.* Esto ocurriría en un caso en el que dejemos imágenes adheridas a un archivo cuya extensión sea *.doc* o *.pdf*.

Este problema podría solucionarse, en alguna medida, con una herramienta forense que encuentre la característica de los *encabezados* que contienen datos que dan información al sistema operativo sobre el tipo archivo asociado. El encabezado no se altera, aunque

se cambie la extensión que el usuario le dé, y por lo tanto una búsqueda física sobre dichos elementos podría descubrir archivos de imágenes que una búsqueda a nivel lógico no lograría. No obstante, registrar un disco rígido en función de los encabezados podría tomar semanas y por ende consumir mucho tiempo, siendo además muy fácil que un analista pase por alto elementos relevantes.

Lo expuesto nos muestra que es verdaderamente difícil predecir cómo serán las búsquedas de evidencia digital, lo que provoca que las limitaciones *ex ante* no sean adecuadas.

Esta problemática ha sido abordada por diferentes autores. Uno de ellos es Jonathan Polansky[14], quien entiende que no sería posible, de manera previa a la apertura del dispositivo, conocer a ciencia cierta la *cantidad y la calidad* de la información que se pueda llegar a encontrar allí. Incluso es imposible saber, al momento de los secuestros, en cual o cuales de los dispositivos se encuentra la evidencia relevante para la investigación. Por lo tanto la confección de protocolos de búsqueda *ex ante*, a través de cualquier filtro como ser *palabras clave, fechas, tipos de archivos,* etc., afectaría gravemente la labor de investigación de la Fiscalía, ya que bastaría con que la persona sospechada (normalmente avezada en conocimientos informáticos, sobre todo en determinados tipos de conductas delictivas) almacene la información con palabras clave que no tengan que ver con el *objeto* de la investigación, o adultere la fecha de creación o modificación de los archivos, o guarde los tipos de archivos buscados dentro de otros, o con distinta extensión. En ese sentido, la jurisprudencia extranjera ha sostenido que equivaldría a decirle a la policía que no secuestre una bolsa de plástico que contiene una sustancia blanca, si en su etiqueta se lee: *"harina"* o *"talco"*[15] , en el marco de una investigación en la que se busca cocaína.

No obstante, la cuestión no resulta pacífica. En efecto, el jurista Lanzón, se pronuncia en favor del establecimiento de limitaciones ex ante. Concretamente tiene dicho: *"... el apresurado análisis expuesto pierde de vista, en primer lugar, que no siempre es necesario y está debidamente justificado analizar todo el contenido del componente en cuestión. Es preciso tener presente qué delito se está investigando y, concretamente, qué evidencia es la que se pretende hallar al llevar a cabo la medida solicitada por la fiscalía y autorizada por el tribunal. En ese sentido, por ejemplo, si lo que se investiga es una maniobra defraudatoria sobre la cual se tiene evidencia de que fue pergeñada durante el año en curso, no sería razonable explorar la información contenida en el dispositivo anterior a esa fecha determinada ..."*[16] .

Ha quedado claro que no comparto el establecimiento de este tipo de restricciones, veamos algunas de las que, eventualmente, podrían imponerse. Para ello es útil tomar algunos ejemplos de la jurisprudencia estadounidense, que ha desarrollado limitaciones *ex ante*, y que pueden dividirse en las siguientes categorías:

a) El *hardware* que se puede secuestrar;

b) El *tiempo* durante el cual se puede analizar la información;

c) La *forma* (el establecimiento de un "*protocolo*") en que se deben desarrollar las búsquedas, a fin de encontrar los elementos relacionados a la investigación y que son *objeto* de la medida investigativa, en el sentido de imponer limitaciones relacionadas con palabras claves, temporales, relacionadas con tipos de archivos, etc.;

d) La condición de *devolver los elementos secuestrados* dentro de un plazo[17].

Estos límites fueron impuestos en distintos fallos. Sin embargo, desde la doctrina y la jurisprudencia de los Estados Unidos se han realizado duras críticas a la imposición de estas restricciones *ex ante*, por *cuestionar las facultades que tienen los jueces para imponer al órgano acusador como debe desarrollar la investigación* y, además, por considerarlas *poco efectivas*. En este camino es importante analizar qué respuesta debe darse a la legitimidad de cada una de las limitaciones previamente mencionadas, incluso en cuanto a la viabilidad de su aplicación práctica.

En cuanto a la *primera* de las restricciones, esto es, qué *hardware* es dable incautar, es importante dejar sentado que debe permitirse el secuestro de aquellos dispositivos sobre los cuales exista *causa probable* en cuanto a que puedan contener información relacionada con el objeto de la investigación.

Eso fue lo dicho en el fallo de la Jurisprudencia Estadounidense conocido como *"United States v. Hill"*[18], del año 2006. En dicha causa un imputado había enviado su computadora a reparar, y quien se avocó a esa tarea encontró imágenes que contenían Material de Abuso Sexual Infantil (M.A.S.I.), razón por la cual formuló la denuncia. Por ello se obtuvo orden de allanamiento para el secuestro de la computadora, pero cuando llegaron al comercio de reparaciones, el dispositivo ya había sido retirado por su dueño, el Sr. Hill. Posteriormente lograron una orden de allanamiento sobre el domicilio del imputado y cuando efectivizaron la medida, si bien ya no estaba la computadora, secuestraron otros dispositivos en los que había M.A.S.I. Los jueces intervinientes decidieron que no debía excluirse la evidencia ya que los agentes policiales habían actuado pragmáticamente, y no motivados por el afán de ir a la "*pesca*".

Compartimos tal solución ya que, en el caso bajo análisis, el secuestro de otros dispositivos distintos al *incriminado*, tuvo origen precisamente en el hallazgo en este último de elementos que daban cuenta de la plausible existencia de más evidencia relacionada con la investigación, contenidas en las restantes unidades de almacenamiento, pertenecientes al mismo dueño, y habidos en el interior del domicilio donde residía el acusado.

Sobre este punto es importante dejar en claro que muchas veces, cuando se acude a realizar el secuestro de dispositivos, no es factible determinar ni de antemano, ni tampoco en el mismo lugar del secuestro, cuáles de ellos contendrán evidencia. En dichas circunstancias deberá recabarse autorización para el secuestro de todos aquellos en relación a los cuales pueda, razonablemente, inferirse que puedan estar relacionados con el *objeto* de la investigación. Y en ese cauce, si como producto de la medida se incautan innumerables dispositivos de almacenamiento digital *¿Cómo determinaremos cuál o cuáles de ellos contienen la información que buscamos?* Pues, habrá que hacer un análisis, ya sea en el mismo lugar o bien en el laboratorio, de la totalidad de los dispositivos que encontremos.

En lo atinente a la *segunda* de las limitaciones, es decir lapso de *tiempo* dentro del cual debe efectuarse el análisis de la información obtenida de los dispositivos, hubo fallos en donde se limitó el periodo para llevar a cabo la medida. Así, en el Fallo *"United States v. Brunette"*[19], del año 1999, se circunscribió a treinta días el plazo para efectuar el análisis. En el Fallo *"People v. Strauss"*[20] se había establecido un período de noventa días para el examen de los datos. Posteriormente, luego de haberse fugado Strauss, la medida perdió trascendencia, motivo por el cual transcurrió el plazo sin que se hubiera realizado. Tiempo después, el imputado fue detenido y se solicitó una nueva autorización para el análisis de la información. La defensa del imputado solicitó la exclusión probatoria por el vencimiento del

plazo, no obstante, lo cual la Corte Suprema de Justicia del Estado de Colorado, en el año 2008, la convalidó, en razón de la nueva autorización solicitada.

Es importante dejar establecido, en relación a las limitaciones atinentes al *tiempo*, que no son pocas las veces en que la determinación de un plazo para su realización resulta irrazonable, toda vez que ello dependerá de incontables factores, tales como la cantidad de información que se encuentre, el tipo de información a procesar, como se encuentre almacenada la misma, entre otros. De esa manera, el lapso para la concreción del examen deberá atender lo que se estime razonable en cada caso. En definitiva, siempre existe la posibilidad de que la Defensa haga valer la garantía del *plazo razonable*, largamente reconocida en el ámbito jurídico.

Sin perjuicio de lo antes dicho, algunos de los inconvenientes reseñados precedentemente encuentran solución a través de la llamada *"imagen forense" (copia bit a bit)* que puede realizarse sobre los elementos a examinar, para proceder luego al análisis del contenido de los mismos en el laboratorio, sin que sea necesario secuestrar el dispositivo, o bien devolviendo el mismo en un corto plazo.

La *tercera* limitación que trataremos consiste en el establecimiento de un "*protocolo*" conforme al cual deberían desarrollarse las búsquedas objeto de la medida judicial, en el sentido de imponer *restricciones relacionadas con palabras claves, limitaciones temporales, en cuanto al tipos de archivos*, etc. Cabe aquí realizar un pormenorizado estudio de la cuestión toda vez que la admisión sin más de este tipo de limitaciones *podría traer aparejada la frustración injustificada de muchas investigaciones penales.*

Ya vimos, al principio de este apartado, todo lo que posibilita la informática en cuanto a llevar adelante acciones que *oculten* la evidencia digital que se busca. Por ese motivo es necesario dejar sentado que, las limitaciones atinentes a la forma de realizar el análisis, en modo alguno deberían entorpecer la investigación en curso, teniendo -para ello- siempre en miras cual es el *objeto* de la pesquisa. Así, habrá que verificar en *cada caso concreto* si se están imponiendo restricciones que podrían echar por tierra la obtención de la información que se busca, o por el contrario si se trata de limitaciones inocuas en ese sentido.

Un primer punto importante para considerar es aquel relacionado con las herramientas informáticas con las que se cuenta, y de qué manera éstas permiten filtrar la información que se busca, para asegurarnos que tenga que ver con el *objeto* de la investigación. Esto debe hacerse no sólo para respetar la *expectativa razonable de privacidad*, sino también para poder abarcar efectivamente ese análisis, que en muchos casos incluirá una gran cantidad de información. No obstante, debe tenerse en cuenta que la herramienta forense perfecta no existe hoy en día, y de existir en el futuro, seguramente aparecerían luego *"contra-tecnologías"* suficientes para neutralizarla.

Otra opción es la utilización de *filtros*, ya sea autoimpuestos por parte del órgano acusador, o bien ordenados judicialmente. En este punto volvemos a recalcar que deberá analizarse cada caso en concreto. Si las limitaciones se realizan a través de palabras claves puede ocurrir que se pierda evidencia relevante para la investigación. Consideremos una investigación en la que se está buscando Material de Abuso Sexual Infantil. Deberíamos empezar preguntándonos: *¿Cuáles serían las palabras claves para limitar esa búsqueda?* o *¿Su aplicación permitiría una búsqueda efectiva?* Veamos algunos ejemplos de ellas: *"MASI", "M.A.S.I.", "Material de abuso sexual infantil", "Pornografía infantil", "Niños y niñas desnudos"*, etc. Es muy fácil burlar las palabras

clave ya que resulta muy poco probable que a través de dichos términos se nombren carpetas o archivos que contengan la evidencia buscada en un caso como el planteado. Ello así, sin perjuicio de las herramientas forenses que permiten localizar este tipo de archivos a través de sus *hashes*, que también pueden ser burladas con manipulaciones informáticas.

En este punto, cabe recordar un ejemplo al cual se hizo alusión al inicio del presente trabajo citado por Jonathan Polansky[21], quien toma el fallo *"United States v. Hill"* en el cual se sintetizó este tipo de restricciones asimilándolas al supuesto de instruir a la policía que no secuestre una bolsa con una sustancia blanca si su etiqueta reza *"harina"* o *"talco"*. En los casos bajo análisis, el uso de ciertas palabras tampoco serviría cuando aquello que se buscan son imágenes o determinados contenidos que se encuentran *"escondidos"* en archivos de *Word (.doc)*.

Por su parte, en los casos de limitaciones impuestas a través *fechas*, podría suceder que el momento de creación o modificación de un determinado archivo haya sido manipulado, siendo éste un procedimiento relativamente fácil, en tanto bastará para ello con valerse de la información accesible públicamente en la *web*, donde se indican sencillamente los pasos a seguir. La alteración de la fecha también puede ocurrir en razón de que el dispositivo que se esté utilizando tenga un calendario modificado, y por lo tanto esa cuestión quede plasmada en el archivo o evidencia en cuestión.

Para el caso en que la búsqueda se pretenda limitar por *tipo de archivo* (extensiones *.doc, .xlsx, .pdf, .jpeg,* etc.) puede ocurrir que el que estemos buscando este cargado con una extensión distinta o bien este escondido en un archivo de otro tipo.

Además, hasta no abrir una computadora no se puede saber cuánta información tiene, cuál es el sistema operativo, como está distribuida, cuanto espacio ocupa, cuáles son los motores de búsqueda, si la información está encriptada o no, etc. De lo expuesto se desprende que, al tratarse de evidencia digital, no se puede plantear *ex ante* una estructura o protocolo de búsqueda.

En el caso conocido como *"Silk Road"*[22], frente al planteo del imputado en ese sentido, la Corte de Apelaciones dictaminó que resulta imposible determinar previamente los términos o frases para realizar una búsqueda, en tanto no se puede saber de antemano el criterio conforme al cual se ha almacenado la información. En efecto, los archivos, carpetas y/o documentos pueden presentar nombres que nada tengan que ver con aquello que se busca, o bien un código insertado mediante el cual se logre evitar que la búsqueda por filtros tenga éxito.

Estos ejemplos nos muestran que las limitaciones *ex ante* pueden ocasionar, injustificadamente, que no se llegue a buen puerto en la investigación penal, entendiendo que la posibilidad de esconder evidencia digital en un dispositivo de almacenamiento es mucho más amplia que la de esconder un objeto material en un espacio físico.

Lo que pretendo explicar es que la *razonabilidad* acerca cómo se llevó adelante la medida surgirá a posteriori de su realización (la cual efectivamente deberá controlar un juez de garantías), y en todo caso existirá siempre el control de las partes (la Defensa en este caso), quienes podrán plantear –a todo evento- que la búsqueda se llevó a cabo de manera arbitraria, desproporcionada o irrazonable. Sera entonces el magistrado quien, en definitiva, decidirá acerca de la exclusión de la evidencia hallada, o su convalidación. Un importante autor como Orin Kerr [23]pone la cuestión

en sus justos términos. Sostiene que puede apreciarse un *encanto inicial* claro en relación a que las órdenes de registros informáticos merecen un *"enfoque especial"*[24], que exija al gobierno articular un protocolo que los especialistas forenses deberían seguir. Sin embargo, postula que, de articularse un protocolo de registro, éste podría ser tan limitado, que termine resultando demasiado estrecho. Entiende que la estrategia de análisis *ex ante* es profundamente defectuosa, ya que asume, erróneamente, que los acusadores y los jueces tienen el conocimiento necesario para articular protocolos de registro antes de que éste comience. Indica que el proceso forense es demasiado fluctuante e impredecible para permitir reglas *ex ante*, y que, a diferencia de lo que ocurre en las búsquedas en los espacios físicos, el control de los registros informáticos solo debe ser realizada *ex post*. Antes de iniciar el proceso forense informático se tendrá poca idea de una importante cantidad de información que será determinante para su realización *(sistema operativo, softwares instalados, cómo funcionan los mismos, si hubo medidas para ocultar la información incriminante, si se encriptó la información, si se cambiaron las extensiones, si hubo cambio de cabeceras, etc.*[25]*)*. Entonces, lo que tampoco puede establecerse de antemano, es qué herramienta forense conviene utilizar, ya que tienen muy diferentes características. El citado autor [26]lo compara *con una cirugía*, en la que el médico no puede saber la mejor forma de proceder hasta que finalmente *"abre"* al paciente y lo observa. Existen en una cirugía, como en un análisis de evidencia digital, factores que son imposibles de predecir antes del inicio.

Imaginemos una investigación por una defraudación, en la que el analista trabaja con la copia forense *(bit a bit)*, en procura de hallar documentos digitales que constituyan evidencia para la investigación que llevó a secuestrar el dispositivo. A mi parecer, el investigador deberá ingresar en la totalidad de las carpetas y archivos hallados, cualquiera sea el nombre bajo el cual se hubiesen guardado, en razón la altísima probabilidad de que la documental incriminante (digital en este caso) no haya sido almacenada bajo rótulos que grafiquen su contenido, tal como por ejemplo *"CONTRADOCUMENTOS", "GASTOS SIN JUSTIFICAR",* o *"FACTURAS APROCRIFAS"*. Por el contrario, resulta obvio pensar que las pruebas de cargo se encontrarán guardadas en carpetas y subcarpetas llamadas, por ejemplo, *"FOTOS CUMPLEAÑOS"*, o *"VIAJE VACACIONES VERANO"*. Sostengo que, siempre dentro del margen de la razonabilidad trazado dentro del objeto de la investigación, el agente debería contar con la facultad para ingresar a estas últimas carpetas, interpretándose que son equiparables a los *"cajones de una mesa de luz"* (del espacio digital) que pueden contener la evidencia relacionada con el objeto de la investigación que se está desarrollando.

Si un informático forense experto no puede predecir que técnicas van a ser necesarias para encontrar la información que se busca, mucho menos lo podrá hacer un juez que desconoce la investigación (más aún si nos encontramos frente a un *sistema acusatorio adversarial*).

Se trata entonces del debate de las *reglas* versus los *estándares*. Estos últimos son juzgados *ex post*, pero basados en hechos específicos y ocurridos; mientras que las reglas se aplican *ex ante*, pero con muchísima menos información de la que se tiene frente a lo ya ocurrido[27].

De allí que el proceso de análisis de información contenida en dispositivos de almacenamiento masivo requiere estándares *ex post*, y no reglas *ex ante*.

Sin perjuicio de lo sostenido hasta aquí, habrá supuestos en los que este tipo de limitaciones cobren sentido y puedan aplicarse, estableciendo un *protocolo* de búsqueda que no resienta las posibilidades de los analis-

tas de llevar adelante una investigación eficaz. Tal sería el caso, por ejemplo, de una amenaza proferida a través de la red social *WhatsApp*, desde la cuenta de una persona hacia otra. No tendría sentido en este supuesto autorizar una búsqueda que supere ese específico *chat*.

En cuanto a la *cuarta* limitación, esto es la fijación de antemano de un plazo para la *devolución* de los elementos a analizar, resultan de aplicación los mismos argumentos y soluciones propuestas al abordar la *segunda* restricción, inherente al tiempo para la realización del análisis de la evidencia digital. ■

Referencias

1 Diccionario de la Lengua Española. Real Academia Española.
2 "Los próximos paradigmas de las pruebas digitales". Andrés Velázquez. Cibercrimen II. Editorial B de f. Año 2021. Página 313.
3 "Vulneración de las Garantías Constitucionales en la Investigación en entornos digitales". María Florencia Suarez. Revista Pensamiento Penal. Penal (ISNN 1853-4554). Página 3.
4 ARTÍCULO 159°.- "Libertad probatoria.- Todos los hechos y circunstancias relacionados con el objeto del proceso podrán ser acreditados por cualquier medio de prueba, salvo las excepciones previstas por las leyes. . ."
5 Sentencia de la Sala de lo Penal del Tribunal Supremo Español, del 10 de marzo de 2016, N° 204/2016, en http://www.poderjudicial.es/search/index.jsp. En la misma se la sostenido que ". . . La ponderación judicial de las razones que justifican, en el marco de una investigación penal, el sacrificio de los derechos de los que es titular el usuario del ordenador, ha de hacerse sin perder de vista la multifuncionalidad de los datos que se almacenan en aquel dispositivo. Incluso su tratamiento jurídico puede llegar a ser más adecuado si los mensajes, las imágenes, los documentos y, en general, todos los datos reveladores del perfil personal, reservado o íntimo de cualquier encausado, se contemplan de forma unitaria. Y es que, más allá del tratamiento constitucional fragmentado de todos y cada uno de los derechos que convergen en el momento del sacrificio, existe un derecho al propio entorno virtual. En él se integraría, sin perder su genuina sustantividad como manifestación de derechos constitucionales de nomen iuris propio, toda la información en formato electrónico que, a través del uso de las nuevas tecnologías, ya sea de forma consciente o inconsciente, con voluntariedad o sin ella, va generando el usuario, hasta el punto de dejar un rastro susceptible de seguimiento por los poderes públicos. Surge entonces la necesidad de dispensar una protección jurisdiccional frente a la necesidad del Estado de invadir, en las tareas de investigación y castigo de los delitos, ese entorno digital. . .".
6 Wilson v. Layne, 526 U.S. 603, 610 (1999) (registro domiciliario); United States v. Ross, 456 U.S. 798 (1982) (registro de un paquete).
7 "Searches and Seizures in a digital world". Autor: Kerr, Orin S. The George Washington University Law School. Public Law and legal Theory Working Paper Nº 135. 119 Harvard Law Review. Año 2005. Página 8.
8 Cfr. Kerr, Orin S. Ob. Cit. Página 8.
9 389 U.S. 347 (1967) - "Charles Katz v United States" – Suprema Corte de los Estados Unidos – 18/12/1967.
10 La Enmienda trata sobre la protección a pesquisas y aprehensiones arbitrarias. Fue establecida como respuesta a la controvertida writ of assistance (una especie de orden general de registro), la cual jugó un papel importante tras la Guerra de Independencia de los Estados Unidos. La misma establece lo siguiente: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized", y cuya traducción sería la siguiente: "El derecho de los habitantes de que sus personas, domicilios, papeles y efectos se hallen a salvo de pesquisas y aprehen-

siones arbitrarias, será inviolable, y no se expedirán al efecto órdenes que no se apoyen en un motivo verosímil, estén corroborados mediante juramento o protesta y describan con particularidad el lugar que deba ser registrado y las personas o cosas que han de ser detenidas o embargadas"

11 389 U.S. 347 (1967) - "Charles Katz v United States" – Suprema Corte de los Estados Unidos – 18/12/1967.

12 La Enmienda trata sobre la protección a pesquisas y aprehensiones arbitrarias. Fue establecida como respuesta a la controvertida writ of assistance (una especie de orden general de registro), la cual jugó un papel importante tras la Guerra de Independencia de los Estados Unidos. La misma establece lo siguiente: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized", y cuya traducción sería la siguiente: "El derecho de los habitantes de que sus personas, domicilios, papeles y efectos se hallen a salvo de pesquisas y aprehensiones arbitrarias, será inviolable, y no se expedirán al efecto órdenes que no se apoyen en un motivo verosímil, estén corroborados mediante juramento o protesta y describan con particularidad el lugar que deba ser registrado y las personas o cosas que han de ser detenidas o embargadas"

13 "Garantías constitucionales del procedimiento penal en el entorno digital". Jonathan Polansky. Editorial Hammurabi. Buenos Aires. Año 2022. Páginas 171 y siguientes.

14 https://caselaw.findlaw.com/court/us-9th-circuit/1256638.html. "United States v. Hill". Del voto del Juez Kazinski.

15 "La búsqueda de evidencias en los dispositivos de almacenamiento digital. Alcances y límites al análisis forense en el marco del procedimiento penal". Román P. Lanzón. DPyC. Derecho Informático (Doctrina). Año XIII. Número 2. Marzo 2023. Página 120.

16 Orin S. Kerr. "Exante Regulation or computer search and seizure". Artículo publicado en la Virginia Law Review, año 2010, Página 1245.

17 Orin S. Kerr. "Exante Regulation or computer search and seizure". Artículo publicado en la Virginia Law Review, año 2010, Página 1245.

18 https://caselaw.findlaw.com/court/us-9th-circuit/1256638.html

19 https://law.justia.com/cases/federal/district-courts/FSupp2/76/30/2370086/

20 https://case-law.vlex.com/vid/people-v-strauss-no-895701688

21 Garantías constitucionales del procedimiento penal en el entorno digital". Autor: Jonathan A. Polansky. Editorial Hammurabi. 1era. Reimpresión. Buenos Aires. Año 2022. Página 187.

22 Caso Silk Road, en https://www.wired.com/2015/04/silk-road-1/ y https://www.wired.com/2015/05/silk-road-2/

23 Crf. Kerr, Orin S. Ob. Cit. Página 45.

24 United States v. Carey, 172 F.3d 1268, 1275 n. 7 (10th Cir. 1999).

25 United States v. Gray, 78 F. Supp. 2d 524, 529 (E.D. Va. 1999).

26 Crf. Kerr, Orin S. Ob. Cit. Página 49.

27 Pierre J. Schlag. "Rules and Standards". 33 UCLA L. Rev. Página 379.