InFo-Cyber. Journal of Cybersecurity and Digital Forensics.
Volumen 1. Número 1 Año 2026. ISSN: en trámite.
https://revistas.ufasta.edu.ar/index.php/InFoCyber/index

INFO-CYBER CYBERSECURITY AND DIGITAL FORENSICS JOURNAL

La informática forense en el proceso penal santafesino. Cuestionamientos éticos y legales ante la inobservancia de su aplicación. Casos de estudio

Digital forensics in the criminal justice system of Santa Fe. Ethical and legal questions arising from its non-application. Case studies

Javier Esteban Bura Peralta

Instituto Argentino de Derecho Procesal Informático (Argentina)

javierburaperalta@hotmail.com

https://orcid.org/0009-0007-7966-625X

Artículo de reflexión

Recibido: 28-08-2024. Aceptado: 02-10-2025
Publicado: 03-03-2026

Universidad FASTA. Facultad de ingeniería; Mar del Plata, Argentina

Resumen

Se analizarán los aspectos más relevantes de la falta de criterio judicial en la aplicación de la informática forense dentro del proceso penal en la provincia de Santa Fe. Más precisamente, se efectuará una apreciación acerca de la inobservancia de los protocolos existentes en el levantamiento de la cadena de custodia digital, la paupérrima capacitación en el personal policial actuante y las consecuencias legales que esto conlleva cuando se debe endilgar responsabilidad penal al imputado.

Palabras clave

cibercrimen, evidencia digital, informática forense, proceso penal

Abstract

The most relevant aspects of the lack of judicial criteria in the application of computer forensics within the criminal process in the province of Santa Fe will be analyzed. More precisely, an assessment will be made about the non-observance of the existing protocols in the lifting of the digital chain of custody, the very poor training of the police personnel involved and the legal consequences that this entails when criminal responsibility must be placed on the accused.

Keywords

cybercrime, digital evidence, digital forensics, criminal process.

JAVIER ESTEBAN BURA PERALTA. Abogado (F.C.J.S. - U.N.L.), Diplomado en Cibercrimen (U.C.A. Rosario), Diplomado Investigación Ciberdelitos (U.N.L.Z.), Director Área Investigación Forense (I.A.D.P.I.), docente universitario Práctica Profesional Final (Abogacía, F.C.J.S. – U.N.L.), miembro A.A.L.C.C.

I. INTROITO

Quiero aclarar que el presente artículo es una variante (adecuadamente reformada, conforme a la temática requerida) de su original, publicado allá por el año 2022 [1].

Desde que me inicié en las prácticas del cibercrimen y la informática forense, muchísima agua ha corrido por el puente. A medida que me iba capacitando en la materia, aprovechando las oportunidades que me brindaban ciertas editoriales para publicar artículos sobre la temática específica, tuve que enfrentar continuos desafíos resolviendo casos prácticos: es así que tuve que lograr imbuirme en los aspectos técnicos específicos, que se actualizaban y cambiaban día a día.

Esto no es nada nuevo: a más de un profesional del derecho se le genera un torrente de ideas y reflexiones a medida que va avanzando en las distintas especializaciones en probática electrónica. La primera reflexión que me surge es la innegable sincronicidad que debe existir entre la informática forense y el derecho. Tal como organismos simbiontes, uno no puede coexistir sin la subsistencia del otro. Esta relación, por otro lado, jamás debe ser dejada de lado por los operadores judiciales. En segundo término —no menos importante—, la incidencia que trasunta la normativa para brindar un adecuado marco legal a la recolección (congruente o no) de la evidencia digital, dentro del marco de una investigación penal preparatoria, bajo el ámbito del sistema acusatorio adversarial.

Fruto de aplicar al campo práctico las distintas capacitaciones específicas mencionadas precedentemente, surge un interrogante que trataré de resolver a través del presente trabajo: ¿la falta de observancia de los acertados protocolos que regulan el tratamiento de evidencia digital como un todo, por parte de autoridades policiales y judiciales debería generar una reacción legal? ¿Es ético que un funcionario público, sujeto innegablemente al respeto de la ley y de las instituciones en razón de su investidura, desoiga los parámetros normativos que estructuran la recolección de prueba electrónica? La falta de regulación específica en los distintos códigos de forma —según argumenta en numerosas oportunidades el organismo investigador/acusador para justificar imputaciones viciadas de nulidad—, ¿coadyuva a resultados disvaliosos, en franca violación a las garantías constitucionales más fundamentales? Indudablemente, sí.

El horizonte primigenio del presente trabajo es, entonces, efectuar una minuciosa consideración acerca de las consecuencias legales que conlleva la falta de observación de protocolos específicos en la recolección y tratamiento de evidencia digital, considerada en sí misma como un acto procesal válido, definitivo e irreproducible. Bajo esta línea argumental, efectuaré un análisis de los efectos desfavorables que castigan al ciudadano común —a la sazón inocente por designio constitucional— en razón de una incorrecta apreciación de los vacíos normativos. Se justifica, de este modo, la errónea imputación de un delito (debatible en las audiencias del juicio, a criterio fiscal) y el ataque desmedido a principios fundamentales como la garantía de defensa y el principio de inocencia (debatible del mismo modo), lo cual en numerosas oportunidades —inclusive— genera una desacertada condena. Todo ello en base al menosprecio que los judicandos poseen respecto de la evidencia digital, como un verdadero indicio del cometimiento (o no) de un ilícito penal.

II. LA EVIDENCIA DIGITAL

A. Breves conceptos básicos

No podemos proseguir con la línea argumentativa iniciada sin focalizarnos un poco en los aspectos relacionados con aquella, su calidad como tal dentro del proceso, y los específicos hechos (ciberdelitos e incidentes informáticos también, si se quiere) que se intentan demostrar. Con el objetivo de no ser reiterativo en expresiones terminológicas, me referiré tanto a "prueba electrónica" como a "evidencia digital" como sinónimos (a pesar de que muchos autores las distinguen). En este sentido, el InFoLab los ha definido como información o datos, almacenado o transmitido en un medio informático, que puede ser utilizado en una investigación [2, p. 76].

Ampliando un poco más estos conceptos, también se puede mencionar que son *"*cualquier información que, sujeta a una intervención humana, electrónica, y/o informática, ha sido extraída de cualquier clase de medio tecnológico informático —computadoras, etc. Técnicamente, es un tipo de evidencia física que está constituida por campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas técnicas especiales*"* [3, p. 15].

Molina Quiroga prefiere hablar de "documento digital", definiéndolo como

> aquel que es conservado en formato digital en la memoria central del ordenador o en las memorias de masa y que no puede ser leído o conocido por el hombre sino como consecuencia de un proceso de traducción que hace perceptible y comprensible el código de señales digitales. Técnicamente, el documento digital es un conjunto de impulsos eléctricos que recaen en un soporte de computadora que, sometidos a un proceso, permiten su traducción al lenguaje natural a través de una pantalla, una impresora u otro periférico que genere un resultado equivalente [4].

Esta última enunciación es la que me resulta más adecuada, dado que explica acertadamente y en pocas palabras un proceso harto complejo, en términos de la informática forense.

B. Su trascendentalidad

Indudablemente, la diferencia que la prueba electrónica tiene con su par *física* —además de lo evidente— es su *especificidad*. ¿A qué nos referimos con ello? Alineándonos a la ciencia criminalística aplicada en este campo [5], la mencionada característica se encuentra determinada, a título ejemplificativo, en el principio de transferencia de Edmond Locard ("es imposible que un criminal actúe, especialmente en la tensión de la acción criminal, sin dejar rastros de su presencia" [5, p. 54]).

Si trasladamos esta premisa a la perspectiva de la informática forense, descubriremos "pistas o huellas" tecnológicas que identifican el obrar ilícito por parte de un ciberdelincuente (el rastro digital del delito, tal como reza el título de una obra imprescindible para el estudio de esta temática [5]). La especificidad también ocurre por la circunstancia de que *no hay ciberdelito si no se ha utilizado una herramienta tecnológica para su comisión*: tal el es el caso de un *groomer* que contacta a la víctima menor de edad a través de redes sociales, inevitablemente bajo la utilización probable de *smartphones*. De similar forma, en una ciberestafa realizada bajo la metodología de *phishing,* necesariamente se tiene que haber utilizado una computadora para lograr un acceso no autorizado o fraudulento a una base de datos informática en la que se alojan los datos de una cuenta bancaria de la víctima. Es así, entonces, que a nivel tecnológico también deducimos la existencia de un agente, de una acción y de un objeto sobre el cual aquella recae, como los metadatos dejados por un pedófilo al *loguearse* en un sitio web con contenido de imágenes de abuso sexual infantil.

C. Particularidades

De aquella originaria idea de especificidad es que surgen ciertos parámetros —absolutamente insoslayables— que, al recolectar la evidencia digital, la definen unívocamente:

1) El dato informático solo es accesible para las personas con una formación técnica especial: los *peritos*. El análisis que efectúan solo es asequible a sus sentidos y apreciaciones, conforme a la *expertise* que solo ellos poseen.

2) La prueba electrónica es *en exceso* volátil: cualquier manipulación errónea puede alterar su estado o hacerla desaparecer; es por ello que se necesita la habilidad necesaria, secundada ineludiblemente con software y hardware adecuados, para asegurar la inalterabilidad de los datos.

3) Esta idea de volatilidad suele ser reforzada, en muchas ocasiones, dado que los metadatos, en forma inconveniente y casual, también pueden ser alterados o eliminados por la utilización normal y habitual del dispositivo electrónico: la simple acción de decidir por la opción *guardar los cambios antes de cerrar* o permitir la ejecución automática de un programa determinado que efectúe una limpieza de memoria RAM, archivos de registro o *cookies* en un navegador.

4) No es menos importante destacar que la información digital contenida en numerosos dispositivos puede clonarse sin límites. Este atributo único permite realizar múltiples copias exactas al contenido original, para ser distribuidas y analizadas por diversos especialistas, al mismo tiempo: puede entregarse una copia bit a bit de un volcado forense de memoria a la defensa o a la querella para que lleven a cabo sus propias pericias, inclusive con software distinto al utilizado por los peritos oficiales. De esta manera, una correcta obtención de la prueba digital permite que todos los actos investigativos sean siempre actos de prueba reproducibles, en términos procesales [6]. Justamente se habla de clonación (copia bit a bit) de metadatos *y no de la entrega de los resultados de una pericia*, algo que tanto la defensa como la querella *no pueden llegar a analizar con sus propios expertos.* Si así se procediera, se violaría el principio contradictorio que caracteriza unívocamente al sistema adversarial.

Al sistema le interesa enormemente, entonces, que las partes tengan amplias posibilidades de contraexaminar la prueba presentada por la otra, y aunque el derecho a defensa presiona todavía un poco más la lógica de la contradictoriedad en favor de la defensa, lo cierto es que al sistema le interesa crucialmente que ambas partes —tanto la fiscalía como la defensa— tengan amplias posibilidades de controvertir la prueba en condiciones de juego justo. Tanto si el testigo del fiscal está mintiendo, falseando, tergiversando, exagerando u omitiendo, como si lo está haciendo el testigo de coartada de la defensa; de ambas cosas es valioso que el sistema se entere. [7, p. 96]

III. El rol de la evidencia digital dentro del sistema adversarial

A. Lo público versus lo privado (en un marco de administración de justicia pública)

El anterior cúmulo reflexivo me traslada al siguiente cuestionamiento: ¿qué ocurre cuando nos encontramos, como querella o defensa técnica, ante la imposibilidad de analizar adecuadamente los metadatos contenidos en determinada prueba electrónica, ya colectada? En la práctica, es tristemente reiterativo que el organismo acusador (abusando descaradamente de las atribuciones conferidas por ley para dirigir la investigación penal preparatoria) ofrezca como indicio de imputación los resultados de una pericia efectuada por profesionales propios.

Es en esta situación que indudablemente el principio procesal de contradicción se quiebra: la necesariedad de acceder imperativamente a los metadatos *sin mayor tratamiento que los sometidos a la preservación y recolección* por parte de los otros

actores del proceso penal, para que sean sometidos a análisis por parte de sus propios expertos.

Ahora bien, Baclini y Shiappa Pietra, en su análisis al Código Procesal Penal de la provincia de Santa Fe (ley n.º 12.734 y modificatorias), exponen que lo que se debe demostrar —a través de ciertas y determinadas probanzas— es un hecho humano que indefectiblemente argumente, a nivel probático, una acusación para una posterior condena:

> Es que en el juicio oral se prueban discursos que versan sobre los hechos pasados (...). La prueba de los hechos de este acto es un problema que debe regirse por la teoría general de la prueba y nada tiene que hacer este concepto de irreproducible en este aspecto, y es por ello que no agrega absolutamente nada de claridad la construcción teórica que se ha hecho de estos actos[8].

A criterio de estos autores, entonces, el hecho demostrado a través de sucesos humanos voluntarios —definitivos e irreproducibles— debe someterse a la teoría general probatoria. Criterio coherente, a la sazón, dado que mucho se ha opinado respecto de la caracterización y los efectos de aquellos actos, aunque poco se ha concluido respecto de ello.

B. Un poco de pragmatismo no viene mal

Es necesario que le brindemos a este marco teórico un enfoque verdaderamente práctico, partiendo de la siguiente premisa: se debe involucrar a la evidencia digital dentro de un acto procesal que tenga, *per se*, carácter definitivo e irrepetible. Supongamos, de este modo, que el perito policial ha efectuado una extracción forense de toda la información contenida en el disco rígido de una notebook, en ocasión de allanar la vivienda de una persona aparentemente investigada por tráfico de imágenes de abuso sexual infantil. Se lo encuentra *in fraganti*, con su computadora encendida, al momento de la irrupción de las fuerzas de seguridad. El informático (queremos suponer que posee entrenamiento DEFR [9]) logra impedir que el sospechoso cierre su laptop para que su sesión de usuario de Windows no se bloquee, logrando acceso, así, al dispositivo encendido, funcionando y con *software* "corriendo". El perito nota que eMule [10][1] estaba conectado a la red e intercambiando archivos, por lo que inmediatamente pone manos a la obra e inicia la preservación de metadatos contenidos en esa computadora.

Concretamente, la extracción forense que se efectúe en el disco rígido de los archivos enviados y/o recibidos a través de este *software* (como todos los otros que sean de interés a la causa, que existieran en dicha *notebook*, archivos de registro, *logueo*, imágenes o videos descargados, historiales de navegación, intercambio de *e-mails,* y un muy vasto etcétera) es un ejemplo específico de la realización de un acto definitivo e irreproducible en materia de recolección digital de material probático electrónico: se efectúa en el momento exacto a riesgo de generar pérdida o adulteración: es necesario hacerlo de este modo, no puede volver a repetirse por el carácter frágil y volátil de la evidencia a preservar y recolectar.

C. De la génesis técnica a un marco jurídico.

Numerosos autores han explicado, a través del análisis de estándares internacionales, cuáles son los parámetros de tratamiento de la evidencia digital, con miras a poder ser utilizada e incorporada como prueba útil en un proceso penal. La admisibilidad en sí refiere al cumplimiento de ciertos requisitos legales a fin de ingresar —ya convertida en prueba— a las audiencias de debate. Así, para el caso de la prueba electrónica, los principios específicos que la gobiernan se resumen en los siguientes:

1) Relevancia

Este requisito es una condición técnicamente jurídica, que habla sobre aquellos elementos que son pertinentes a la

[1] eMule es un programa informático cuya funcionalidad es la de compartir archivos informáticos con otros ordenadores repartidos por el mundo. Es un programa informático gratuito. En esta red de ordenadores no existe un ordenador central donde se almacenan los archivos y al que se accede. Es una plataforma donde cada usuario del ordenador comparte o no sus archivos con el resto de ordenadores del mundo. Por ejemplo, un ordenador central con archivos almacenados y al que se debe acceder para obtenerlos, es el ordenador del Fondo Documental del Consejo General del Poder Judicial (http://www.poderjudicial.es). Quién desee acceder al Fondo Documental y buscar jurisprudencia debe acceder a ese ordenador. En la plataforma que se detalla, no existen ordenadores centrales que almacenen archivos. Cada usuario de un ordenador puede obtener archivos de los restantes usuarios de ordenadores. Luego compartir o no los archivos que tenga en su ordenador con el resto de usuarios. Los archivos se dividen en fragmentos de archivo y esos fragmentos de archivo es lo que se intercambia. La forma de compartir archivos en eMule es por fragmentos. No todos los ordenadores disponen al mismo tiempo del 100% de los fragmentos del archivo; sino que uno puede tener un 40% de los fragmentos, otro un 30% y otro el 100%. Para poder visualizar el contenido completo de un archivo es preciso haber obtenido todos los fragmentos de un archivo. Es preciso haber obtenido el archivo por completo. Para poder visualizar parte del contenido del archivo, o poder saber qué se está obteniendo, es preciso haber obtenido siempre el primer y último fragmento del archivo, así como una parte sustancial del archivo. Lo cual en la práctica es normalmente equivalente a tener descargado el archivo completo. La obtención de todos los fragmentos de un archivo de otros ordenadores puede tardar minutos, horas, días o semanas. Todo dependiendo del tamaño del archivo, del número de archivos que se descargan de modo simultáneo y del ancho de banda de la conexión contratada para acceder a Internet (cantidad de información que puede transmitirse a través de una conexión por unidad de tiempo).

situación que se analiza o investiga, con el fin de probar o no una hipótesis que se ha planteado alrededor de los hechos [11].

2) Suficiencia

Con las evidencias recolectadas y analizadas, tenemos elementos suficientes para sustentar los hallazgos y verificar las afirmaciones efectuadas sobre la situación investigada [11].

3) Confiabilidad

Relacionado con la necesaria validación de la reproducibilidad y auditabilidad de un proceso aplicado para obtener prueba electrónica: si un tercero sigue el mismo proceso respetando los estándares, deberá obtener resultados similares, verificables y comprobables [11].

4) Auditabilidad y reproducibilidad

A través de la aplicación de la norma ISO 27037, los procedimientos seguidos deben haber sido validados y contrastados por las buenas prácticas profesionales. La trazabilidad de los resultados debe ser incuestionable. Los métodos aplicados podrán ser reproducibles, verificables y argumentables al nivel de comprensión de los entendidos en la materia, quienes puedan dar el respaldo necesario a las actuaciones realizadas [12].

Quiero compartirles algunos cuestionamientos. Un especialista en informática forense puede efectuar una extracción forense de evidencia digital en un dispositivo o desde la nube, en una sola oportunidad o en varias. La pregunta es: ¿su contenido, datos y metadatos serán similares? Siguiendo los protocolos establecidos y ateniéndonos a las buenas prácticas, seguro que sí. Ahora bien, si se realiza la extracción con los dispositivos forenses idóneos, al finalizar el proceso informático se va a generar un archivo de formato forense (.raw, .dd, .001, .e01 o .ad1, por ejemplo) con su consecuente huella *hash*, fruto de aquella recolección. Esta función criptográfica siempre va a ser distinta si se efectúa una posterior extracción similar, siguiendo la misma metodología forense y sobre el mismo dispositivo. *Lo que no va a variar son los metadatos de dichas extracciones*. Por lo tanto, el acto técnico de extracción de evidencia forense *también es*, a los fines procesales, "un acto definitivo e irreproducible" (de lo cual me explayaré luego), aunque tantas veces repetible como queramos, en caso de que la evidencia digital recolectada se mantenga incólume.

Mantengámonos en esta línea de tiempo argumental. Surge un segundo cuestionamiento: ¿y si la pericia informática es anulada, ya sea por haberse violado la cadena de custodia, por tener el software forense utilizado licencia caduca o por haberse vencido la matrícula del perito? En todo caso, ¿qué ocurre si el perito es recusado? Estos actos, definitivos e irreproducibles, ¿mantienen su validez legal?

No dejo de insistir, en base a aquello, en que las partes deben ser notificadas antes de la realización de estos actos técnicos, para que efectivamente cada uno de los actores involucrados —con sus propios expertos— logre realizar un adecuado control de los procedimientos técnicos de detección, aseguramiento y preservación de la prueba electrónica. Este es uno de los fundamentales pilares a través del cual se basamenta el principio contradictorio, dentro del sistema acusatorio adversarial: la oportunidad del acceso y control por igual a todas las pruebas y a la producción de las mismas.

Si alguno de estos procedimientos falla, si no se aplica el método adecuado, si quien lleva adelante el protocolo no está capacitado, si no nos aseguramos que el dispositivo es efectivamente el continente de la información que necesitamos, si de alguna manera se alteraron los datos originales, si la copia bit a bit difiere de la extracción original, el proceso de obtención de la evidencia se tornaría —*fruto del error humano*— irrepetible (paradójicamente sería la contracara forense de su par procesal), y la consecuencia inevitable sería la inutilidad de esa información, por carecer del requisito de confiabilidad. Esta evidencia, en consecuencia, sería inadmisible en las audiencias de debate.

He aquí en donde surge la llamada regla de la exclusión probatoria: las pruebas que provengan de un acto producido bajo las características antedichas, u obtenido o incorporado mediante violación de garantías constitucionales, no pueden ser admitidas como tales en un proceso:

> La obtención ilegítima de un medio probatorio, da lugar al rechazo, no utilización, ni valoración alguna, en la actuación procesal. Es decir, que la prueba que amerita ser excluida no puede ser considerada, de ninguna manera, por el juez que va a decidir acerca de la responsabilidad del acusado [13].

La mentada regla se encuentra regulada en el Código Procesal Penal de la provincia de Santa Fe [14], que en su artículo Nº 162 reza: "carecerá de toda eficacia la actividad probatoria cumplida vulnerando garantías constitucionales. La ineficacia se extenderá a todas aquellas pruebas que, con arreglo a las circunstancias del caso, no hubieran podido ser obtenidas sin su violación y fueran consecuencia necesaria de ella". Siguiendo este orden de ideas, el artículo Nº 246 del mismo cuerpo normativo refuerza esta idea de legalidad, haciendo hincapié en el anterior, que fija una regla inobjetable para los judicandos: (...) no podrán ser valorados para fundar una decisión judicial, ni utilizados como presupuestos de ella, los actos cumplidos con inobservancia de las formas y condiciones previstas en este Código, salvo que el defecto haya sido subsanado o no se hubiera protestado oportunamente por él".

Concluimos entonces que, si se logra nulificar el contenido de la prueba de cargo, *no hay teoría del caso.* Es por ello que la evidencia electrónica, posicionada bajo el análisis de una adecuada valoración judicial, demuestra su complejidad

(comparativamente hablando) con el resto de los medios de prueba tradicionales. Su ofrecimiento, producción, resguardo, valoración e impugnación se llevan a cabo según parámetros y conocimientos técnicos especiales. Y en extremo específicos.

IV. PRUEBA ELECTRÓNICA Y PROCESO PENAL

A. Los actos definitivos e irreproducibles

Volvamos ahora a la caracterización de estos actos en particular. Es claro que ambos términos no son sinónimos, ni mucho menos. "Definitivo" es aquel que, *para servir de prueba en el juicio, no es necesario repetirlo y mejorarlo procesalmente [15]*; en tanto que "irreproducible" *será aquel acto que no puede volver a repetirse en las mismas condiciones [16]*, es decir aquellas actividades que pueden resultar de imposible realización ulterior durante el proceso. La legislación requiere expresamente que el acto tenga *ambas características*, es decir, que deba ser *definitivo e irreproducible*. En realidad, todo acto procesal, sea de recolección de prueba o decisorio, es siempre definitivo, porque ese acto, como tal, una vez realizado ya no se puede modificar. Del mismo modo, es también irreproducible, ya que si se vuelve a realizar, será otro acto diferente, realizado en otro momento histórico y bajo otras circunstancias.

Las características propias de la investigación penal preparatoria hacen que muchos de los actos realizados sean definitivos, a menos que haya oposición procesal oportuna por parte de alguno de los otros actores relacionados: si bien *per se* pueden ser incorporados a las audiencias de debate, necesariamente se debe discutir su validez como tales, respetando las garantías constitucionales, en forma previa.

B. La cuestión de la normativa de forma local

El Código Procesal Penal de la provincia de Santa Fe (Ley n.º 12.734 y sus modificatorias) en su artículo 260 determina:

> deberán constar en actas debidamente formalizadas, con expresa mención de la fecha, hora, intervinientes, firmas de los funcionarios actuantes y mención de cualquier otro dato útil a la eficiencia y acreditación de la autenticidad del documento, (...). Las restantes diligencias de la investigación no guardarán otras formalidades que las exigidas por la reglamentación y por las instrucciones generales y especiales expedidas por el Ministerio Público Fiscal, salvo las que tuvieran una formalidad expresamente prevista en este Código [14, p. 73]

Sin lugar a dudas, el legislador santafesino fue muy poco referencial en términos de tratamiento de prueba electrónica. Por lo tanto, al no encontrarse específicamente regulado en la ley de forma, *deberíamos* remitirnos *por analogía* (algo que produce cierto resquemor dentro del fuero penal) a lo dispuesto por el Convenio de Cibercriminalidad de Budapest. En su defecto, a la aplicación —para el caso del organismo acusador— del Protocolo Unificado de los Ministerios Públicos de la República Argentina, o a las guías PAIF PURI del InFoLab. Las fuerzas de seguridad, por otro lado, deberían sujetar su actuación conforme a lo regulado por el Convenio n.º 088 del Ministerio de Seguridad de la Nación (al cual la provincia de Santa Fe ha adherido oportunamente). Además de otras numerosas opciones a considerar por parte de la defensa técnica o la querella (como la observancia de las normas ISO/IEC), en ocasión de tener que producir prueba. Lo cierto es que en la provincia de Santa Fe, todo ello se desoye, y con resultados muy dispares, esto hay que decirlo. Ya ahondaré con mayor profundidad acerca de ello al ejemplificar la problemática.

En numerosas oportunidades, los vacíos legales permiten que la doctrina santafesina analice la cuestión sin demasiado rigor técnico, confundiendo cuestiones relacionadas con la afectación de garantías con otras referentes a la prueba:

> La dificultad del abordaje teórico del problema (más asociado a nuestra tradición jurídica inquisitiva) es que al no existir una práctica y teoría de las formas de registro y documentación de actos procesales para el sistema acusatorio (funcional a los valores de la oralidad, inmediación, etc.), se recurre –intuitivamente- a pensar esos problemas con el bagaje de conceptos del sistema inquisitivo [8].

A pesar de ello y ante las innegables argumentaciones nulificatorias:

> la doctrina desde siempre acuerda que los registros de estos actos son suficiente prueba de los mismos en el juicio oral, sin perjuicio de que puedan además traer testigos que den cuenta de ellos para garantizar algunos otros valores asociados al proceso probatorio (contradicción, entre otros). En palabras de Cafferata Nores: 'la exigencia de un acta circunstanciada se refiere, sobre todo, al reconocimiento practicado en la etapa instructoria, pues éste podrá ser incorporado al debate mediante la lectura de aquélla y ser, así, de base a la sentencia. [8].

Así y todo, nuestra normativa de forma es sensible a la afectación de garantías constitucionales durante la producción de estos actos, aunque esto no implique su obligatoria observancia por parte de funcionarios judiciales o autoridades policiales. El artículo 282 estatuye:

> Toda medida probatoria que por su naturaleza o características debiera considerarse definitiva o irreproducible, para ser válida, será ordenada por el Fiscal y notificada a la defensa y al querellante si lo hubiera, a fin de que ejerciten sus facultades. En caso de divergencia respecto al modo de realización del acto, se requerirá verbalmente la intervención del Tribunal de la Investigación, el que adoptará las medidas que considere pertinente para la realización garantizadora del mismo. [14, p. 81]

Si bien el articulado es específico, no existe impedimento a

que dicha regla general pueda ser aplicada a la preservación y producción de evidencia digital.

C. Lo que funciona a nivel técnico no lo hace a nivel normativo

Es opinión de la doctrina mayoritaria afirmar que —en un sistema acusatorio adversarial— el control de los judicandos no debe ser exhaustivo, excepto que se encuentren en juego premisas constitucionales, porque *desvirtuaría la naturaleza misma de esta clase de procesos*. Humildemente entiendo que también deberíamos incorporar al debate la idea de *especificidad* como característica primordial de la evidencia digital, siempre teniendo en cuenta el rol preponderante que ocuparía dentro de un proceso. De este modo lograremos fusionar esta concepción con los preceptos inicialmente descritos, logrando así *relacionar un acto irreproducible —a nivel técnico— con la teoría de los actos definitivos e irreproducibles, dentro del sistema acusatorio*.

Yendo un paso más allá en el desarrollo de este ideario, según la postura doctrinaria referida, la prueba de cargo colectada es *indiciaria*: no se identifica directamente con el objeto fundamental del proceso, sino que se relaciona con otros hechos secundarios que, a su vez, sirven para inferir la existencia del hecho principal. Se la considera también una *prueba indirecta* porque tiene por objeto no al hecho inmediato, sino a otros que sirven para demostrar su existencia. De todos modos, incorporadas al proceso, recién adquieren su verdadero carácter probático al culminar el procedimiento intermedio, previo a las instancias propias del juicio oral.

En el ejercicio de la profesión me he dado cuenta de que en todas las ocasiones en las que he tenido oportunidad de debatir —audiencia mediante— sobre la calidad del medio probático de origen digital, los judicandos han sido variables en su interpretación:

> La eficacia probatoria de esta prueba dependerá, en primer lugar, de que el hecho constitutivo del indicio esté fehacientemente acreditado; en segundo término, del grado de veracidad, objetivamente comprobable, de la enunciación general con la cual se lo relaciona con aquél; y, por último, de la corrección lógica del enlace entre ambos términos [17, p. 193].

Si nos mantenemos dentro de las variables que exige la observancia de la aplicación de las reglas de la prueba general, aplicada a los parámetros de su similar electrónica, nada cambia: como paso previo al estudio de la interpretación de los indicios, será preciso determinar la validez de los mismos, es decir, que no hayan sido obtenidos en violación a determinada pauta procesal o que no hayan sido producto de una vulneración a alguna garantía constitucional. Luego de ello, es necesario esforzarse para determinar adecuadamente la relación que une al medio probático entre el hecho dado con el hecho investigado.

De todos modos, en la práctica forense el tinte de informalismo que cubre a la investigación penal preparatoria *no tiene nada de informal* (se priva de la libertad a un ciudadano, se disponen medidas de índole personal como la prohibición de acercamiento o de índole patrimonial como la caución de bienes, esto ya se dijo), y el carácter indiciario de la prueba de cargo *sí posee* el carácter de definitivo e irreproducible, dado que impulsa a aquellas medidas.

Algunos componentes de doctrina especializada —Navarro y Daray, entre otros— entienden que en los allanamientos en los que se realiza el examen de dispositivos informáticos en el lugar, no debe darse intervención a la defensa técnica en razón de ser un simple registro domiciliario, y porque asimismo *es un relevamiento de los datos informáticos* almacenados en los dispositivos que pudieran encontrarse allí, y no un verdadero análisis. Aseveran asimismo que, en el caso de hallarse información que pudiera involucrar penalmente al investigado, se procede al secuestro del dispositivo para posteriormente efectuar un análisis a fondo en un laboratorio pericial:

> Finalmente, el relevamiento de datos que se realice en oportunidad del registro domiciliario no constituye un acto definitivo ni irreproducible; la defensa del encausado tendrá la posibilidad de hacerse de una copia forense de toda la información que contengan los dispositivos, oportunidad donde podrán controlar la legitimidad del secuestro oportunamente realizado [18].

Quizá estas ideas prosperen en un mundo ideal, en donde los operadores forenses (adecuadamente capacitados) cuenten con las herramientas necesarias para lograr la adecuada asepsia y esterilización digital del lugar a examinar y de los dispositivos a encontrar en dicho sitio. ¿En CABA? Indudablemente. ¿En la Provincia de Buenos Aires? También. Lo mismo que en Neuquén y Córdoba, quizá. ¿En el resto del país? Difícilmente. La provincia de Santa Fe no es ajena a ello, por los motivos ya descriptos.

Es por ello que el enfoque de la doctrina mayoritaria me parece erróneo. Si consideramos que el rol del juez dentro de la investigación penal preparatoria —propia de un sistema acusatorio adversarial— no es controlar el accionar de la policía o de la fiscalía, entonces mayor motivo para que se le permita a la defensa o la querella poder intervenir en esta clase de actos a los fines de verificar el accionar de aquéllos, o en todo caso, participar en los actos procesales llevados a cabo.

Asimismo, he leído algún que otro fallo [19] a través del cual los judicandos consideraron que una extracción forense no era pericia (indudablemente no lo era), y que por lo tanto las autoridades no se encontraban obligadas a notificar a la defensa de dicho acto procedimental, por no considerarla un acto definitivo e irreproducible. Si bien la doctrina santafesina considera a *todos los actos realizados dentro de la investigación*

penal preparatoria como definitivos e irreproducibles que puedan conducir a un juicio o al archivo de aquella, considero personalmente que la extracción forense de evidencia digital, desde un dispositivo o desde la nube —a través de *hardware* acorde— es, innegablemente, uno de los *mayores* actos definitivos e irreproducibles. Por la absolutamente inherente característica de especificidad de la prueba electrónica a extraer y preservar, algo de lo que ya me vine explayando regularmente.

Vuelvo a reformularme la pregunta de siempre: ¿el resultado de la pericia informática en sí, presentado en las instancias primigenias del proceso penal como un acto definitivo (la repetibilidad a la que nos referimos es una *repetibilidad técnica*, que no tiene absolutamente nada que ver con el carácter de irrepetible que un acto procesal urgente pueda tener), logrado sin importar la observancia de las buenas prácticas, es *válido*? ¿Sigue manteniendo tal carácter aún por la circunstancia de haberse producido, en razón de su urgencia, sin haber notificado al resto de los actores del proceso, a los fines de su control? Estará en cabeza de la defensa técnica demostrar las violaciones a las garantías constitucionales que pudieran existir. El grado de certeza que exige la ley, en la práctica, no existe.

V. Casos prácticos ocurridos en el foro santafesino.

A. "T.O.O. s/delito contra la integridad sexual"

En los autos caratulados "T.O.O. s/delito contra la integridad sexual" (C.U.I.J N° 21-08164141), la denunciante concurrió ante la autoridad policial con el objetivo de poner en conocimiento que, a través de la aplicación del servicio de mensajería instantánea WhatsApp, su hijastra menor de edad le había dicho que había sido víctima del delito de abuso sexual por parte de un familiar cercano. El personal policial recibió la denuncia y realizó *capturas de pantalla* de la conversación almacenada en el teléfono celular de la denunciante para su incorporación a la investigación policial, que luego pasó a conformar el legajo fiscal.

Comenzada la etapa intermedia, la fiscalía intentó incorporar al debate aquellas capturas de pantalla como prueba documental, situación a la cual la defensa se opuso, en razón de que, siendo una conversación de WhatsApp, información almacenada y transmitida *a través de* un dispositivo electrónico, la misma debía ser considerada como evidencia digital. Fue obtenida por personal policial que no tenía los conocimientos técnicos requeridos para extraer información de un *smartphone* electrónico, con riesgo de alterar su estado originario. Asimismo, no se secuestró aquel teléfono para preservar y analizar los metadatos contenidos en el mismo. Tampoco se pudo acreditar que la prueba que se pretendía incorporar haya provenido de ese artefacto, y que date de la fecha que se alega, máxime por no haberse requerido la información de la línea telefónica de la que se emitieron dichos mensajes (numeración y titularidad), por lo que menos aún se pudo corroborar si ellos realmente existieron.

Este accionar por parte del personal policial ha provocado la disrupción entre los factores de repetibilidad y auditabilidad que generalmente tiñen de certeza el procedimiento aplicado para obtener dicha evidencia digital, provocando su nulidad. Al convertirlo en un acto irreproducible, *tornó exigible la presencia de la defensa del imputado,* a los fines de ejercer el control de dicho accionar, conforme lo regulan los artículos 2 y 8 del Código Procesal Penal de la provincia de Santa Fe, en consonancia con el resto de la normativa específica ya precitada (artículo 282). El planteo defensista fue rechazado en primera instancia; habiendo sido apelado, la alzada confirmó la resolución del *a quo*, por los siguientes argumentos:

a) El tribunal admitió la incorporación de *ocho hojas impresas* de mensajes de WhatsApp que en teoría involucraban al acusado, lo cual indudablemente no es una pericial informática, en el sentido que la defensa quiso resaltar.

b) En este sentido, los magistrados confundieron los argumentos defensistas, considerando erróneamente que no era necesario exigir una pericial informática porque la impresión de los chats, como actos definitivos e irreproducibles, mantenían su validez legal.

Es tristemente indudable que numerosos judicandos no asimilan que la extracción de la información digital y la pericia sobre esta se desarrollan en momentos técnicos distintos. La extracción es un acto definitivo e irreproducible, en tanto que la pericial posterior es la culminación informática de aquel acto. A modo de analogía, piénsese en la prueba de ADN; la extracción de la muestra debe ser realizada mediante un método y por personal con cierta *expertise*. Sin embargo, la pericia propiamente dicha será realizada en un momento posterior mediante otro método y tal vez con otros expertos.

Ciertamente la estrategia de la defensa técnica debería haber radicado en insistir durante las etapas previas —y como anticipo jurisdiccional de prueba— en la realización de una pericial informática sobre el dispositivo celular efectuada por personal idóneo, único medio a través del cual se puede constatar la existencia de contenidos de índole digital:

> La credibilidad o confiabilidad de la evidencia digital viene dada por el respeto de los principios de repetibilidad y auditabilidad, no por la libre convicción de los juzgadores (...). Reiteradamente el magistrado minimiza la importancia del procedimiento de extracción de la evidencia digital, la confunde con la pericia que tendrá por objeto la búsqueda del dato relevante y deja librada a la valoración del juzgador la

confiabilidad de la misma. [20]

Lamentablemente, este fallo en segunda instancia no fue apelado en su oportunidad.

B. "V. C. E. s/ infracción arts. 153 bis primer párrafo y 149 ter inc. 1".

Durante septiembre del año 2022, el Tribunal Oral en lo Criminal Federal de Santa Fe condenó a un ciberdelincuente basándose en evidencia digital recogida sin respetar los protocolos de extracción. Más precisamente, al recolectarse la evidencia digital de primera mano (una de las computadoras conectada al servidor de un reconocido diario local), inicialmente no se había utilizado bloqueador de escritura (remito nuevamente a mis consideraciones previas respecto de los actos definitivos e irreproducibles). Así y todo, se lo encontró penalmente responsable por el delito previsto en el artículo 153 bis primer párrafo del Código Penal, porque se valió de su experticia para introducirse en la página web de un medio periodístico, intervenir en su red, introducir virus en sus terminales e insertar en su página a la vista, pública, un mensaje específico profiriendo amenazas en contra de una persona determinada. Se le imputó también por el delito de amenazas agravadas conforme al artículo 149 ter, inciso 1, en razón del anonimato detrás del cual se escuda el autor. Del mismo modo, según la magistratura, fue procedente encuadrar su conducta en el artículo 161 del citado cuerpo normativo por impedir la libre circulación de un periódico porque bloqueó la página web del periódico por un lapso de cinco o seis horas, impidiendo el normal funcionamiento y la difusión de las noticias en ciernes.

Por otro lado, en su decisorio, el judicando local consideró como improcedente el planteo de nulidad alegado por la defensa del imputado en lo referente a la falta de observancia de los protocolos vigentes, teniendo en cuenta que estos *sí se habían formalizado*: según su criterio, se realizó una copia forense de la información requerida para brindar solidez a la acusación; aquella fue almacenada, se respetó y preservó debidamente la cadena de custodia (*justamente el bloqueador de escritura es necesario para ello*, y no fue utilizado). Del mismo modo, la magistratura entendió que el accionar prevencional, avalado por el ministerio acusador, se ajustaba al Código Procesal Penal de la Nación (*que no regula el tratamiento de evidencia digital*) y a los protocolos de actuación seguidos por el personal policial en casos análogos. En la realidad de los hechos la extracción de evidencia inicialmente se realizó sin bloqueador de escritura ni consecuente *hasheo*; asimismo la verificación del acontecer delictual se logró en una primera oportunidad a través de impresiones de simples capturas de pantalla (sin utilizar software forense) y su grabación en un *pendrive* y CD, para luego acompañar su certificación *hash*, siendo que los metadatos colectados deberían haber sido sometidos a los algoritmos propios de la función inicialmente: esto se produjo a posteriori, recién cuando los investigadores lograron detener el ataque dirigido a los servidores *host* del diario.

El decisorio jurisprudencial aclaró, asimismo, respecto del procedimiento especial contemplado en el protocolo del Ministerio de Seguridad de la Nación citado por la defensa

> (...), la importancia de la copia de la evidencia digital (...) a fin de poder trabajar sobre ella durante la investigación del ilícito; ésta debe ser bit a bit: completa e idéntica. El 'bloqueador de textos' que menciona el defensor técnico (...), se refiere a un bloqueador de escritura, herramienta que podría utilizarse a la hora de extraer la copia forense de una evidencia digital y que podría instrumentarse a través de un hardware y/o un software específico. Sin embargo, no existe un mandato legal que imponga su utilización. [21]

Es necesario efectuar algunas precisiones respecto de este fallo que lamentablemente tampoco fue apelado: el Convenio de Cibercriminalidad de Budapest, normativa basamental a aplicar ante la ausencia de reglamentación específica, no especifica nada, ni siquiera en sus considerandos, respecto de los procedimientos a seguir; la norma ISO/IEC 27037/2012 recomienda utilización *software* bloqueador de escritura; en la Guía Integral de Empleo de la Informática Forense en el Proceso Penal (Universidad FASTA), se recomienda "bloqueo del medio de almacenamiento, a fin de evitar escrituras indeseadas".

En síntesis, cada vez más refuerzo mi postura de que los jueces, al fundamentar sus decisorios en lo relacionado a probática electrónica, además de conocer el derecho, *deben conocer la tecnología*.

C. "FLEITAS PÁEZ, Ximena s/Grooming": primera parte

Voy a permitir explayarme en ciertos detalles, en este caso en particular, por haber participado activamente en la representación legal de la involucrada, en un hecho de trascendencia nacional. Durante el año 2019 se presenta en mi estudio una clienta, de ocupación docente, acuciada por la incertidumbre de encontrarse imputada por este delito en particular. Asesorada por un colega neófito en la materia, acude ante mí con pedido fiscal de procedimiento abreviado pesando sobre sus hombros. Según argumentaciones del órgano acusador, la fémina le habría enviado un video de carácter íntimo vía WhatsApp a un menor de edad, alumno de un prestigioso colegio privado, en el cual aquella se desempeñaba asimismo como profesora de geografía. Para peor, con una marcadísima trascendencia en los medios de comunicación, locales y nacionales, por haberse viralizado dicha filmación.

El delito endilgado se fundamentaba, asimismo, en la presunción de que la imputada se hubiera comunicado con este

niño a través de la red social Instagram y del servicio de mensajería instantánea ya mencionado, a través del cual le remitiera la filmación. Como pruebas de ello, el órgano investigador utilizó *capturas de pantalla impresas* presentadas por la progenitora del menor, como comprobantes de los presuntos diálogos efectuados por el chat de Instagram, y una *"pericia"* (y lo remarco por lo burdo de la denominación, plasmada en el acta de notificación de imputación) efectuada por un oficial de la Policía de Investigaciones santafesina (PDI). Todos actos procesales que, a criterio de la fiscalía, *eran irrefutables*. Una vez interiorizado de los pormenores de la pesquisa, comenzaron a surgir innumerables dudas e interrogantes.

1) Análisis de las capturas de pantalla.

Indudablemente, las capturas de pantalla, obtenidas en esta oportunidad por métodos fácilmente manipulables, y recibidas por la fiscalía en simple impresión en formato papel, *sin ninguna clase de resguardo*, se invisten de valor probatorio nulo:

> Que quede bien en claro: los 'pantallazos' pueden determinar un nombre y apellido de un remitente y/o destinatario, pero en realidad lo que importa son los números telefónicos asociados a los contactos, situación que a posteriori podría aclararse mediante oficios respectivos a las compañías prestatarias de servicios de telefonía celular; ello es así debido a que no solemos agendar a nuestros contactos con nombres y apellidos reales, sino que mayormente lo hacemos a través de un sobrenombre, apodo, nick o con iniciales. Siendo así, resultaría como adelanto de prueba indiciaria fundamental a la hora de dictar sentencia en algunos procedimientos por delitos tales como amenazas, coacciones, grooming o ciberbullying. Ahora bien, ello no implica que deban ser aceptadas como prueba cada vez que sean aportadas por las partes, sino que deben cumplirse una serie de garantías dado que pueden ser fácilmente manipuladas, siendo de vital importancia la conservación del soporte original donde se contengan los mensajes a fin de acreditar su autenticidad. [22]

2) Pericias en celulares. Violación a la garantía de no autoincriminación.

Costaba entender que no se hubieran efectuado las pericias informáticas sobre los dispositivos celulares de los NNA involucrados (a la víctima misteriosamente le robaron su teléfono *días después* del incidente y al principal testigo *se le reseteó el celular* involuntariamente). En resumidas cuentas, la imputada debía soportar su responsabilidad penal en base a una *pseudopericia* efectuada en su dispositivo móvil por parte de personal policial que no se encontraba capacitado para tal fin, y sin haber dado conocimiento de dicha medida a la defensa. Inclusive cuando se le secuestra el dispositivo de comunicación celular a la fémina, el personal policial *le requiere el patrón de desbloqueo, también estando la defensa técnica ausente*. Flagrante violación (si la hay) a la garantía de no autoincriminación propugnada por nuestro artículo 18 de la Carta Magna nacional.

3) Falta de idoneidad en el personal actuante.

A poco que seguí ahondando en los detalles de la investigación, me topo con actos procedimentales que generaban —sin hesitaciones— nulidades absolutas e insalvables. El personal policial actuante no se encontraba adecuadamente capacitado para efectuar análisis y/o extracción de datos forenses; las buenas prácticas determinaban, para el caso en concreto, la aplicación del Convenio n.º 088/2016 —de adhesión de la provincia de Santa Fe a su homólogo del Ministerio de Seguridad de la Nación n.º 234/2016—, por el que se reglamentó el Convenio de Cibercriminalidad de Budapest (Ley n.º 27.411), *de aplicación obligatoria para las fuerzas de seguridad de esta provincia*.

Todo el personal policial, en consecuencia, que interviniera en el secuestro, manipulación, extracción y análisis forense de dispositivos informáticos o prueba digital debía ser profesional altamente capacitado ("la evidencia digital solo debe ser examinada y analizada por personal idóneo, entrenado y capacitado para ese propósito.: III. PRINCIPIOS ESPECÍFICOS DE INTERVENCIÓN; 2. Examen por Expertos" [23, p. 10]). Al iniciar el análisis tras encender el dispositivo, el empleado policial no detalló en acta la utilización de *software* forense que completara la función de bloqueo de escritura para iniciar la copia forense de la información a analizar (no lo detalló *porque no utilizó ninguno*, a decir verdad). Tampoco se efectuó el *hasheado* de los metadatos que conformaban la evidencia a cotejar, ejercicios ineludibles según lo determina el convenio aludido supra. Sumado a todo ello, el funcionario actuante efectuó una búsqueda de "*información relacionada al hecho que se investiga",* la cual se realizó sobre *el dispositivo en sí y no sobre una copia forense*, con el riesgo inescindible de alterar o suprimir metadatos de relevancia. Así y todo, una vez finalizada la *pseudopericia*, el investigador refirió en su informe que no se encontró ningún archivo de interés (imágenes, videos, documentos) y, al no tener ninguna red social instalada, tornó imposible el análisis de las mismas. Lo ideal hubiera sido, respetando lo preceptuado por las buenas prácticas, *reinstalar las redes sociales* y aplicaciones de mensajería instantánea para poder analizar la información recuperada, aunque siempre efectuado por personal *altamente capacitado*. El convenio 088/2016 establece, en su acápite III —Principios específicos de intervención—, Punto 2 (Examen por Expertos): "el personal que manipule evidencia digital deberá estar especialmente capacitado y entrenado para dicho propósito" (...) "la evidencia digital solo debe ser examinada y analizada por personal idóneo, entrenado y capacitado para ese

propósito" [23, p. 14].

La manipulación del dispositivo celular de la imputada, concluyentemente, no respetó en modo absoluto los principios metodológicos de identificación, adquisición, preservación, análisis y presentación de resultados, necesarios para que el dictamen pericial fuera confiable y válido. La evidencia digital analizada por personal de la PDI no cumplió en modo alguno con los principios propios que hacen que toda prueba electrónica tenga validez como tal.

4) Violación a la esfera de intimidad del imputado.

Otro detalle a resaltar es la intromisión (no autorizada judicialmente) dentro del ámbito privado de un ciudadano. El funcionario actuante —inidóneo— estableció bajo acta que *buscaba analizar redes sociales dentro del dispositivo celular* perteneciente a la joven docente. Una cosa es proceder al resguardo forense de datos simples, crudos, para poder realizar un posterior análisis de aquellos. Y otra cosa muy diferente *es querer entrometerse en forma arbitraria en la esfera de intimidad del individuo, sin la correspondiente autorización judicial, actuando solo por requisitoria fiscal*. Es advertido entonces que, para investigar todo lo relacionado a la esfera de reserva de la presunta imputada, se requiera obligatoriamente la observancia de que la orden sea impartida —fundadamente— por el juez de la investigación penal preparatoria.

A partir de todo lo expuesto, cabe afirmar que la orden impartida por el Fiscal, puesta en crisis por la defensa, respecto del análisis de los contenidos de los dispositivos móviles, claramente implica una intromisión al ámbito de privacidad de una persona. (...). Por ello, es claro que la información que pretende conocer, a través de la medida implica una injerencia al derecho a la intimidad de las comunicaciones resguardado constitucionalmente, y cuya intromisión solo puede ser dispuesta por una orden judicial fundada. Por lo tanto, cabe declarar la nulidad respecto de la orden de peritaje impartida por el Fiscal en fecha 12/10/2016, que obra a fs. 26 y de todo lo actuado en consecuencia, pues el MPF actuó ilegítimamente adoptando facultades que son propias y obligatorias del órgano Jurisdiccional y que vulneran el derecho a la intimidad, consagrado constitucionalmente (arts. 71, 72 inc. 2, 73 y 75 CPPCABA, 6 LPC)" [24].

Del mismo modo y en idéntica línea argumental:

> la Corte Suprema de Justicia en el precedente "Quaranta", del 31 de agosto de 2010 sostuvo que: 'el derecho individual a la privacidad del domicilio de todo habitante -correlativo al principio general del artículo 19- en cuyo resguardo se determina la garantía de su inviolabilidad, oponible a cualquier extraño, sea particular o funcionario público... que nadie puede ser objeto de injerencias arbitrarias en su vida privada (...). 'En conclusión para convalidar el registro del teléfono celular se debió requerir la orden del juez competente a fin de que evaluara la existencia de elementos objetivos idóneos para fundar una mínima sospecha razonable que justificara la medida (...). Además, la requisa se vio justificada recién ex post (...), lo que no permite justificar la intromisión ilegal'. (...) Entendemos que la nulidad de la revisación del celular arrastra el vicio a los actos posteriores del proceso que son su consecuencia inmediata y directa a la luz de la doctrina del fruto del árbol venenoso. [25, p. 33]

Nulidades insanables, si las hubo. Inclusive por imperio del artículo 162 del código de rito.

5) *Alternativas no utilizadas en la investigación por grooming.*

Sorprende sobremanera cómo el organismo acusador no proveyó toda una serie de medidas típicas requeridas para el abordaje de esta clase de casos. En primer lugar, podría haber oficiado a las compañías prestatarias de servicio de internet (ISP) a los fines de determinar si la presunta imputada o su pareja (ella convivía con su novio, también docente, y la hija de ambos) poseían cobertura de servicio de red y, en su caso, quién era el titular de dicho servicio. Lo mismo para el responsable legal de la víctima. Orientado ello a obtener las direcciones IP asignadas a cada uno (requerir solamente datos de usuario o de abonado). Se podrían haber verificado, de este modo, las casillas de mail asignadas a cada uno, creadas a partir de aquellas IP relacionadas por las prestatarias del servicio de internet contratado o a través de sus números de celular, y oficiar en consecuencia, solicitando si hubo intercambio de datos de tráfico.

En segundo lugar, podría haberse efectuado una restauración del backup del servicio de mensajería WhatsApp, con el objetivo de establecer si hubo comunicación entre los números abonados que la víctima utilizaba al momento de los hechos y la presunta imputada, o en su caso los menores testigos. También podría haberse oficiado a las redes sociales Facebook e Instagram, para que informen si los involucrados poseían perfiles asignados, creados de acuerdo a sus datos reales de identidad, o conforme a las casillas de mail, o teniendo en cuenta los números de teléfono utilizados al momento de los hechos. En base a lo informado, se hubiera efectuado una adquisición forense de la Nube, con el objetivo de determinar si entre las personas mencionadas existió alguna clase de conexión o relación virtual (solicitud de contacto, de seguimiento o amistad, aceptados o no), como también intercambio de mensajes, audios, imágenes o videos.

Con idéntico fin, podría haberse oficiado a NCMEC Argentina[2], para determinar si existieron reportes, alertas o comunicaciones *(cybertips*) de perfiles denunciados, surgidos

[2] National Center for Missing and Exploited Children: Centro Nacional para Niños Desaparecidos y Explotados.

aquéllos por activación de protocolos respecto de comunicaciones sospechosas entre víctima e imputada, intercambios de chats y/o de contenidos de sexo explícito a través de las diversas plataformas digitales como Facebook, Twitter, Instagram o Google con las que NCMEC tiene convenios. En su caso, si hubo actuación del protocolo *Photo DNA*[3]. Nada de ello fue llevado a cabo, inclusive cuando estas medidas fueron requeridas al órgano fiscal por esta defensa técnica, terminando por archivarse la investigación, refrendado ello por la magistratura interviniente, tiempo después [26].

D. "FLEITAS PÁEZ, Ximena s/Grooming": segunda parte.

Surge una variación en la línea investigativa de esta defensa técnica: la imputada se transforma en víctima.

1) Presunto acceso no autorizado a las cuentas virtuales de la docente.

A la vez que quien suscribe se orientaba a esclarecer lo acontecido, acontece una variante de la teoría del caso. Fueron presentadas a la fiscalía constancias que la casilla de correo electrónico de Gmail de la docente había sido accesada ilegítimamente, no pudiendo recuperar su contraseña por aquel entonces, hasta unos meses después. Atento a ello, la imputada no tuvo dominio de dicha cuenta (ni de las aplicaciones vinculadas a Google, entre ellas la *app* nativa Google Fotos) por un prolongado lapso de tiempo. También había recibido avisos vía mail de inicios remotos de sesión no autorizados en su cuenta educativa (Classroom), en su perfil de Instagram desde el navegador web Google Chrome -en dos oportunidades- y desde un dispositivo Motorola modelo Moto G (5S). Mi clienta radicó entonces una denuncia penal en sede de la Policía de Investigaciones, por sospechar que personas desconocidas estaban intentando acceder en forma ilegítima a su perfil privado en aquella red social, procurando una suplantación de identidad. Del mismo modo, fue recibiendo varios mensajes extorsionadores -vía chat interno de Instagram- por parte de otro usuario exigiéndole ciertas conductas, presuponiéndose que estos pedidos estuvieran motivados por la viralización de su video íntimo (filmación que había dado pie a la investigación fiscal primigenia).

2) Extorsión y acceso ilegítimo.

Sin lugar a dudas la fémina fue víctima (prima facie) del delito de extorsión en grado de tentativa, utilizándose las redes sociales como un medio -digital- para cometer el mismo. Es bajo este curso argumental que esta defensa técnica comenzó a barajar la posibilidad de que personas de ignorada identidad, aprovechando un descuido de la víctima, accedieran a su dispositivo de telefonía celular, burlando su patrón de desbloqueo. Obedeciendo quizá a la idea de llevar a cabo un simple divertimento, encontraron, en su "husmeo digital", el descripto video personal de mi defendida, filmación que fuera destinada a ser viralizada en redes sociales, servicios de mensajería instantánea y sitios web de pornografía. Este ilícito es conocido como "Acceso Ilegítimo a un Sistema Informático de Acceso Restringido", contemplado por el artículo 153 bis del Código Penal argentino.

He aquí el surgimiento de un nuevo curso de los acontecimientos, emanado de la relación entre hechos denunciados e investigados, que presentan una particular conexidad: *apropiación de dispositivo celular-sustracción de datos restringidos-extorsión-viralización*. Surgió una altísima posibilidad que alumnos del colegio (como a posteriori se logró comprobar), menores de edad (inimputables), accedieran al *smartphone* de la presunta imputada (ahora víctima), para así manipularlo y descubrir este archivo de video, para luego viralizarlo.

3) Aprendiendo el funcionamiento de Google Fotos.

Ahora bien, el descubrimiento de la filmación no solamente fue algo absolutamente premeditado, sino que exigió por parte de los autores del ilícito una cierta experticia. Sumada a un lapso de tiempo prudencial, permitió el logro del objetivo buscado: el video (que inicialmente iba a estar dirigido a la pareja de la docente para una ocasión particular, pero luego fuera eliminado por razones personales) quedó alojado en la Papelera de Reciclaje de la aplicación nativa del sistema operativo Android: *Google Fotos*. La víctima jamás supo (excepto cuando ya fue demasiado tarde) que aquella filmación no sería eliminada de la memoria interna del dispositivo por un plazo (establecido en forma automática por la misma *app*) de *sesenta días*. Fue en dicho período que accedieron en forma no autorizada a su dispositivo, compartiendo dicho video en forma ilegítima. Técnicamente, la *app* Google Fotos mantiene, en su Papelera de Reciclaje, los distintos archivos gráficos y de video *exhibidos con una vista previa*, detalle importante cuando un extraño intenta buscar filmaciones o fotografías de carácter íntimo.

Gracias a la intervención de un asesor técnico privado altamente capacitado (cuya participación se normativiza a través del artículo n.º 183 segundo párrafo, Código Procesal Penal), se realizó una pericia informática forense sobre el celular, propiedad de la docente. Se analizaron datos de restauración de una tarjeta de memoria extraíble micro SD

[3] PhotoDNA es una tecnología de identificación de imágenes que se utiliza para detectar pornografía infantil y otro contenido ilegal que se informa al Centro Nacional para Niños Desaparecidos y Explotados según lo exige la ley.

incorporada, cuentas de correo electrónico vinculadas al perfil de Google asociado a dicho dispositivo, información de cuenta recopilada gracias al servicio web de recuperación de datos Google Takeout, al igual que metadatos similares relacionados con la restauración forense del *smartphone* en sí. Luego de una minuciosa búsqueda y análisis de archivos en formato gráfico y de video que realicé a través de software de análisis como FTK Imager, Encase Forensics y Autopsy, fue imposible detectar la presencia del video propagado que dio inicio a la investigación. Pero sí descubrí dos archivos gráficos con la extensión .jpg con una asignación nativa, muy específica.

4) Funcionalidad de las API. De un video viralizado a selfies ocultas.

La mayoría de los sistemas operativos para móviles Android (en sus distintas versiones) mantienen —hasta el día de hoy— variadas aplicaciones (nativas o descargables desde el antiguo Market o el actual Google Play) para visualizar sus fotos. Las API[4] que aquéllas utilizan, en las variadas versiones de este sistema operativo, normalmente determinan por defecto (y de acuerdo a los algoritmos introducidos por los distintos desarrolladores) que la *app* de cámara de Android guarde una foto de tamaño original conforme a la lente incorporada al dispositivo, si se proporciona un espacio de almacenamiento para hacerlo. Esto lo efectúa el mismo sistema operativo a través de aquellas API. Al tomarse una fotografía, se generan datos EXIF[5], que es un conjunto de información que acompaña a cada archivo gráfico (o de video) generado. Es así que cuando desde el dispositivo móvil realizamos una foto (o una filmación), automáticamente se incluyen fecha y hora, datos de la cámara utilizada, valores ISO [27] [6] e incluso la ubicación geográfica de la foto, si en ese momento se tenía la geolocalización activada. E irremediablemente y por defecto, cada archivo será guardado con denominación de extensión gráfica (o de video) junto a la fecha completa, hora, minutos y segundos como nombre de archivo (por ejemplo, *IMG_20200622_180234.jpg*). En base a lo antes expuesto, logrando analizar en particular los nombres de los archivos en formato gráfico recuperados, pude determinar que los mismos fueron grabados en la memoria micro SD (por parte de la *app* Android Cámara) en una fecha y horarios determinados: momentos en los cuales la docente se encontraba realizando actividades extracurriculares de campamento en la provincia de Córdoba. Se logró establecer asimismo que, conforme a la cercanía de los rostros en las imágenes, era indudable que los autores de las fotos eran menores de edad, y se habían tomado bajo la modalidad conocida como *"selfie"*: dos fotografías con tres niños en cada una, *todos ellos alumnos de la institución y concurrentes al campamento de referencia*.

Como conclusión, se pudo lograr deducir —con un alto grado de verosimilitud— de que estos menores de edad pudieron estar involucrados en la comisión del delito contemplado por el artículo 153 bis del Código Penal argentino: dichas fotos son indicios reales de que pudieron apropiarse indebidamente del dispositivo celular de la docente mientras ella se dedicaba a las labores propias del campamento, burlar su patrón de bloqueo (que ella reconoció como simple: solamente la letra "Z"), y acceder a contenidos digitales de índole privada, lo cual se encuentra penado por la ley. Es más que claro que la conducta típica desarrollada por los autores fue *el acceso no autorizado al dispositivo*, independientemente de si detectaron, visualizaron o viralizaron los contenidos almacenados en aquel.

VI. Colofón.

A. Necesidad del control judicial en la investigación penal preparatoria.

El sistema acusatorio, merced a la oralidad que lo caracteriza, delega inicialmente la carga de la prueba en manos del órgano acusador; así, corresponde entonces a la fiscalía (o a la querella, en los casos en que su intervención sea posible) probar la responsabilidad penal del imputado en los hechos que se investigan. A consecuencia de ello, la gestión incriminadora lleva a la necesaria contradicción entre los actores del proceso, la cual se torna evidente desde el momento en que existe una parte interesada en recabar prueba y otra interesada en verificar si esta es legítima o no, o producir contrapueba que refute la anterior. Es importante que esto exista ya desde la propia investigación penal preparatoria, debido a que probablemente algunos indicios surgidos en aquella etapa ya puedan incorporarse directamente al debate, sino además porque, en general, la investigación preliminar busca perfilar el resultado del proceso. La cuestión se torna más escabrosa cuando juez o fiscal no permiten la participación de la defensa o la querella en los actos generadores de prueba de cargo:

> No es entendible la negativa, sin más, del órgano investigador a permitir la intervención de la defensa en la etapa de investigación ni su negativa a tomar en cuenta las pruebas ofrecidas por ella; pues así lo único que se logra es una decisión conclusiva que puede resultar incompleta y sesgada, en el tanto se dejan de lado apreciaciones e hipótesis que luego, en debate, pueden resultar incluso más convincentes y fuertes, desmejorándose así la posición de la fiscalía en la etapa crucial

[4] Application Programming Interface: interfaz de programación de aplicaciones.

[5] Exchangeable Image File Format: formato de archivo de imagen intercambiable.

[6] La sensibilidad ISO, antes denominada ASA, determina la capacidad del sensor de su cámara para percibir la luz. Cuanto mayor sea la sensibilidad, más sensible será el sensor a la luz y menos tiempo necesitará para captar una escena. De este modo, podrá trabajar con velocidades de obturación rápidas para evitar el desenfocado.

del proceso [28].

Como señala Alexy, haciendo alusión a la teoría de la argumentación de Perelman, "quien actúa con parcialidad, supuesto que sea sincero, convence sólo a aquellos entre los cuáles él se encuentra. Quien quiere convencer a todos, debe ser imparcial. Esto presupone que él presente también los respectivos contraargumentos" [28].

En realidad, los judicandos sí deben ejercer un rol de control, pero del celoso cumplimiento y de la observancia de las garantías constitucionales por parte de la policía y del organismo acusador. No por nada los sistemas procesales en numerosas provincias lo denominan, justamente, "*juez de garantías*".

Llegado a la culminación de este punto de análisis, es necesario echar una última luz sobre otras realidades. Teniendo en cuenta las reglas de la sana crítica, receptadas en los distintos códigos procesales, son los magistrados quienes deberán, por un lado, internalizar aspectos técnicos propios de otras profesiones —más afines a la informática que al derecho—, a fin de nutrirse de las equivalencias suficientes para comprender acerca de aquello que tienen que resolver. Ello siempre teniendo presente las cualidades esenciales de los entornos digitales involucrados, a los cuales aquellos muchas veces no están acostumbrados: "Lo importante acá no es tanto que los jueces y fiscales se aggiornen al uso de las nuevas tecnologías (aunque sea algo inevitable), sino que logren comprender acabadamente cómo funcionan y cuáles son sus características más salientes, lo que a su vez permitirá un correcto encuadre normativo" [29, p. 351]. Y lograr, de este modo, una adecuada armonía entre la aplicación de las leyes procesales y el mantenimiento de las garantías constitucionales.

REFERENCIAS

[1] J. E. Bura Peralta, "Reflexiones acerca de la recolección de la evidencia digital en las instancias iniciales del proceso penal. Su presentación judicial. Valoración legal como actos definitivos e irreproducibles," *Revista Derecho y Tecnología: el avance de las nuevas tecnologías en el Derecho*, vol. I, Rubinzal Culzoni, dic. 2022.

[2] A. H. Di Iorio, *Guía Integral de Empleo de la Informática Forense en el Proceso Penal*, 2da ed. Mar del Plata: Universidad FASTA, 2016.

[3] M. A. Nessi, *Manual de Evidencia Digital*. Lima: American Bar Association - ABA ROLI, 2017.

[4] E. Molina Quiroga, "Ley de expedientes digitales y notificaciones electrónicas judiciales," *La Ley*, vol. 2011-C, p. 1224, jun. 2011.

[5] A. H. Di Iorio *et al.*, *El Rastro Digital del Delito*. Mar del Plata: Universidad FASTA Ediciones, 2017.

[6] M. G. Salt, "El acceso transfronterizo de datos y las técnicas de acceso remoto a datos informáticos: nuevos desafíos de la prueba digital en el proceso penal," Tesis doctoral, Córdoba, mayo 2017.

[7] A. A. Baytelman y M. J. Duce, *Litigación penal, juicio oral y prueba*. Santiago de Chile: Universidad Diego Portales, 2004.

[8] J. C. Baclini y L. A. Schiappa Pietra, *Código Procesal Penal de Santa Fe comentado, anotado y concordado*. Rosario: Editorial Juris, 2017.

[9] A. H. Di Iorio, *Cibercrimen II*. Buenos Aires: Editorial B de F, 2018.

[10] "eMule," *Perito Informático*. [En línea]. Disponible: https://peritoinformatico.es/claves-defensa-acusacion-pornografia-infantil/. [Accedido: 15-feb-2022].

[11] Ministerio Público Fiscal de la República Argentina, "Guía De Obtención, Preservación y Tratamiento de Evidencia Digital," Resolución PGN 756/2016, 2016.

[12] "ISO/IEC 27037:2012 Nueva Norma para la Recopilación de Evidencias," *Perito IT*, oct. 2012. [En línea]. Disponible: https://peritoit.com/2012/10/23/ISOIEC-270372012-NUEVA-NORMA-PARA-LA-RECOPILACION-DE-EVIDENCIAS/.

[13] V. Anselmino, "Las garantías constitucionales y la regla de exclusión probatoria en el proceso penal," *Anales de la Facultad de Ciencias Jurídicas y Sociales, U.N.L.P.*, no. 42, 2012. [En línea]. Disponible: http://sedici.unlp.edu.ar/bitstream/handle/10915/27004/Las_garant%C3%ADas_constitucionales_y_la_regla_de_exclusi%C3%B3n_probatoria_en_el_proceso_penal.pdf?sequence=1.

[14] *Código Procesal Penal de la Provincia de Santa Fe*, Ley Nº 12.734.

[15] R. Núñez, *Código Procesal Penal de Córdoba anotado*. Buenos Aires: Editorial Marcos Lerner, 1978.

[16] F. D'Albora, *Código Procesal Penal de la Nación anotado, comentado y concordado*. Buenos Aires: Editorial Lexis Nexis, 2002.

[17] J. I. Cafferata Nores, *La Prueba en el Proceso Penal*. Buenos Aires: Editorial Depalma, 2001.

[18] J. Fusalba y J. M. López Zavaleta, "Los registros domiciliarios con análisis de dispositivos de almacenamiento de datos en el lugar. Qué ocurre en las investigaciones de delitos que involucran la integridad sexual de menores. Realidad judicial y la implicancia de la adhesión de la República Argentina al Convenio de Budapest sobre Ciberdelincuencia. Necesidad de reformas procesales," en *Cibercrimen II*, D. Dupuy, Dir., Montevideo - Buenos Aires: Editorial B de f, 2018, pp. 205-218.

[19] Cámara Nacional de Apelaciones en lo Criminal y Correccional, Sala 4, "A., J. A. y otros s/ nulidad Asociación ilícita y otros."

[20] V. Regali, "Las garantías procesales en la obtención de evidencia digital," *Microjuris*, 25-abr-2021. [En línea]. Disponible: https://aldiaargentina.microjuris.com/2021/04/27/doctrina-las-garantias-procesales-en-la-obtencion-de-evidencia-digital/.

[21] Tribunal Oral en lo Criminal Federal de Santa Fe. "V. C. E. s/

infracción arts. 153 bis primer párrafo y 149 ter inc. 1 del C. Penal"- [En línea]. Disponible: https://aldiaargentina.microjuris.com/2022/10/13/fallos-hacking-condena-por-ingresar-al-sistema-informatico-de-un-medio-periodistico-e-insertar-un-virus-en-sus-terminales-para-publicar-en-su-pagina-a-la-vista-del-publico-un-mensaje-intimidante-d/

[22] J. E. Bura Peralta, "Acreditación y valoración judicial sobre calumnias e injurias vertidas a través de redes sociales," *https://www.google.com/url?sa=E&source=gmail&q=elDial.com*, 29-abr-2019.

[23] Ministerio de Seguridad. Convenio de Adhesión al Protocolo General de Actuación para las Fuerzas Policiales y de Seguridad en la Investigación y Proceso de Recolección de Pruebas en Ciberdelitos (Resolución MS N°234/2016. [En línea]. Disponible: https://www.argentina.gob.ar/sites/default/files/conv-088_16_stafe_ciberdelitos.pdf

[24] Cámara de Apelaciones en lo Penal, Contravencional y de Faltas de la CABA, "Núñez, Jesús Omar s/artículo 91 CC," Causa n.º 3712-00-00/16.

[25] Cámara Nacional Criminal y Correccional de Capital Federal, Sala VI, "Villareal, Walter Andrés y otro," Causa 1404/12, 19-oct-2012.

[26] Colegio de Jueces de Primera Instancia - Distrito Judicial Nº 1 (Santa Fe), "Fleitas Páez, Ximena s/Grooming," CUIJ N° 21-08098928-5, Resolución de archivo, 01-feb-2021.

[27] "Fotografía: la sensibilidad ISO," *L'Atelier Canson*. [En línea]. Disponible: https://www.lateliercanson.es/fotografia-la-sensibilidad-iso.

[28] R. Alexy, *Teoría de la argumentación jurídica*. Madrid: Centro de Estudios Políticos y Constitucionales, 2007.

[29] J. Bura Peralta, "El rol del abogado querellante frente a la investigación de los delitos del área digital," en *Tratado de la prueba electrónica*, Tomo III, Cap. 4, G. E. Bielli, C. J. Ordoñez y G. H. Quadri, Dirs., Buenos Aires: Thomson Reuters La Ley, 2021, pp. 325-390.