Universidad Empresarial Siglo 21

EVIDENCIA DIGITAL

TRABAJO FINAL DE GRADUACIÓN
PROYECTO DE INVESTIGACIÓN APLICADA (PIA)

Carrera: Abogacía
Alumno: Daniela del Valle López
Legajo:
Agosto de 2018

Resumen

En el marco de esta nueva sociedad de la información en constante avance, se hace necesario tomar conocimiento de estas manifestaciones tecnológicas y la manera en la que éstas, inciden en las relaciones humanas, la comunicación y la trasmisión de datos. La propuesta del siguiente trabajo, es un intento de presentación de las condiciones que se podrían tener en cuenta a la hora de la obtención de ~~las~~ pruebas digitales y la utilización de las mismas en los procedimientos judiciales. Se da una introducción ~~a~~ de los nuevos conceptos básicos ligados al mundo digital. Se analiza la relación de la evidencia digital con los principios de legalidad, libertad probatoria y el derecho a la intimidad. Se aborda el Cibercrimen (Ley 23.688-delitos informáticos) y la Convención de Budapest, el principal instrumento internacional que aborda de modo integral, este fenómeno de delitos informáticos. Se analizan también, los mecanismos de preconstitución (nube, correos electrónicos, celulares, redes sociales, imágenes digitales) y los tipos de pruebas que se pueden obtener, el rol de los expertos, finalizando con una revisión del tratamiento de las evidencias digitales en los procesos provinciales.

Palabras Claves

Evidencia digital, convención de Budapest, cibercrimen, debido proceso, intimidad, ISO/IEC 27037.

Abstract

Within the framework of this new information society in constant advance, it is necessary to take cognizance of these technological manifestations and the way in which they affect human relations, communication and the transmission of data. The proposal of the following work, is an attempt to present the conditions that could be taken into account when obtaining digital evidence and the use of them in judicial proceedings. There is an introduction to the new basic concepts linked to the digital world. The relationship of digital evidence with the principles of legality, probation and the right to privacy is analyzed. It addresses Cybercrime (Law 23,688-cybercrime) and the Budapest Convention, the main international instrument that comprehensively addresses this phenomenon of cybercrime. The mechanisms of preconstitution (cloud, emails, cell phones, social networks, digital images) and the types of tests that can be obtained are also analyzed, the role of the experts, ending with a review of the treatment of digital evidences in the provincial processes.

Keywords

Digital evidence, Budapest convention, cybercrime, due process, privacy, ISO / IEC 27037.

Índice

Introducción

En el contexto actual de avance tecnológico, las redes sociales y la constante incorporación de nuevas tecnologías tanto en la vida cotidiana y laboral (plataformas de comercio electrónico, trazabilidad de comunicaciones telefónicas, mensajes de texto, entre otros), los datos digitales adquieren preeminencia en todos los estamentos y experiencias en el desarrollo de las personas en comunidad, entre los cuales, se destaca el derecho.

Estas interacciones virtuales aumentan cada día a través de los distintos medios de conexión, tal como lo confirma un estudio presentado por Kantar IBOPE Media Argentina, el cual indica que, en 2016 el 60% de los argentinos declaró poseer un teléfono inteligente, lo que implica, un incremento del 55% respecto al año anterior (canal AR 2017). De esta manera, toda esta actividad en el mundo virtual toma una importancia relevante en el ámbito judicial, dando lugar u origen a nuevos delitos (informáticos) y cada vez, es más necesario indagar en el tipo de prueba o evidencia que se puede tomar en este tipo de casos involucrados.

Las modernas tecnologías y el cada vez mayor auge de crímenes informáticos, hacen necesario, abordar la problemática de la eficacia de la obtención, conservación, presentación, interpretación y validez de las pruebas dentro del proceso judicial.

En este contexto, entendemos por evidencia digital, a todo conjunto de datos e información que son relevantes para una investigación compuesta de campos magnéticos y pulsos eléctricos, obtenidos mediante el uso de técnicas asistidas por computadoras

En el presente proyecto de investigación aplicada, se desarrollará un análisis jurídico de la evidencia digital, estableciendo comparaciones entre códigos procesales a nivel nacional e internacional, estudiando la forma en que la evidencia digital. es contemplada y utilizada en procedimientos legales.

El problema jurídicamente importante a tratar, se puede formular a través de los siguientes interrogantes:

- ¿Es la evidencia digital, toda prueba en formato electrónico?
- ¿Qué problemas jurídicos presenta la prueba digital, en cuanto a su obtención, incorporación al proceso y valoración de la misma por parte del juez o tribunal?

- ¿Tiene la evidencia un tratamiento especial?
- ¿La libertad probatoria incluye al tipo de Evidencia Digital?
- ¿Las prácticas de recolección de evidencia digital respeta el debido proceso?
- ¿La propuesta de modificación del CCPN (ley 27.063) presenta mejoras en el tratamiento de la evidencia digital?

Como hipótesis tentativa, se plantea en principio, que la obtención e incorporación de evidencia digital como prueba en juicio, requiere su validación por peritos informáticos, garantizando que la misma, se obtuvo sin violar el derecho a la privacidad e intimidad de las personas.

En este sentido, al ser una problemática incipiente y de patente actualidad, la legislación en la materia es insuficiente y presenta algunos vacíos legales. A nivel internacional, el principal antecedente es la Convención de Budapest (Convención Europea sobre Delitos Informáticos - Hungría 2001), pudiendo servir de referencia los avanzados códigos procesales de países europeos, tales como Francia, Alemania y Reino Unido, así como algunos códigos de los Estados Unidos, sobre todo aquellos que regulan el ámbito laboral. A fin de optimizar la legislación nacional en la materia, se postula que la propuesta de modificación del CCPN (Ley 27.063) y, la incorporación a la Convención de Budapest, proponen mejoras a futuro en el tratamiento de la evidencia digital.

El objetivo general de la investigación, es analizar los problemas que presenta la prueba digital en cuanto a su obtención, incorporación en el proceso y valoración de la misma por parte del juez o tribunal. A su vez, se definen como objetivos específicos, desarrollar el concepto de evidencia digital, sus características como prueba o como medio de prueba y su valor legal; describir los antecedentes legislativos en relación a la evidencia digital; analizar su incorporación al proceso, verificando la pertinencia, la necesidad de licitud y el registro de admisibilidad procedimental; y analizar cómo es la regulación específica en el derecho comparado.

La relevancia jurídica de esta investigación, es sobre esclarecer los puntos polémicos de la eficacia de las pruebas en los procesos legales y analizar las normativas vinculadas a la misma.

La relevancia social que presenta este tema, es para dar certeza jurídica a las partes intervinientes en los procesos o al estado para ejercitar el *ius puniendi,* que tendrá como interés la manera en que el dato electrónico o digital puede ser incorporado al proceso para probar la existencia del hecho.

En la cotidianeidad, los abogados reciben todo tipo de consultas, que, de algún modo, se terminan relacionando con la prueba digital. En este punto son los profesionales del derecho, los encargados de decidir los elementos que utilizarán como prueba, sospesando la relación costo-beneficio de incorporar una prueba que de antemano implicará una demora en el proceso, con un resultado incierto a la hora de acreditar hechos que para la parte y el cliente constituyen "verdades".

Las leyes de procedimiento -en casi todos los fueros- no especifican si los mensajes de texto sirven como pruebas, o si injurias graves realizadas por medio de redes sociales configuran como delitos, ni ofrecen herramientas legales para evidenciar comunicaciones por WhatsApp -o al menos no dan a conocer las posibilidades otorgan las herramientas procesales existentes. En efecto, determinar la autoría de documentos virtuales, es hoy un inconveniente complejo para los operadores del derecho, a lo que se añade la dificultad para armonizar el lenguaje entre quienes preguntan (los abogados) y quienes deben responder (los peritos) (Bes, 2014).

Ante esta situación, los abogados y operadores del derecho comienzan a abandonar las miradas tradicionales, ya que los conflictos ligados a la evidencia digital son cada vez mayores (en cantidad y complejidad), resultando cada vez más difícil para las partes acreditar hechos con los clásicos medios de prueba. En este sentido, se continuará solicitando pruebas en papel y el llamado de testigos, pero cada vez, los casos estarán relacionados con mensajes de texto y/o documentos virtuales**.** Si desde el campo del derecho, no se brindan las soluciones que la sociedad necesita, persistiendo con los viejos sistemas probatorios, se terminará incumpliendo la función principal de la existencia de las instituciones judiciales, que tienen como objetivo la búsqueda y construcción de una sociedad más justa y equitativa. Para cumplir tal propósito, se

deberán actualizar y optimizar los medios, para establecer con precisión, la oportunidad y certitud con la cual se puede instituir una evidencia digital en prueba judicial.

Capítulo 1. Evidencia digital

Introducción

En el siguiente capítulo repasaremos una aproximación a la definición de Evidencia Digital, aspectos terminológicos, antecedentes normativos y como es la misma incorporada en el derecho comparado.

Concepto y características

A lo largo de los últimos años, se han desarrollado una serie de intentos de conceptualizar y precisar los alcances de la "evidencia digital". No por una mera cuestión académica, sino porque resulta necesaria una definición acabada, integral, completa y no redundante de lo que ello significa e implica, para que la legislación de la misma permita delinear específicamente de que se está hablando. La tarea resulta difícil, por el propio dinamismo de las nuevas tecnologías, que hace que muchas veces la propia definición necesite ampliarse para incorporar nuevos métodos no contemplados a la hora de realizarla.

De acuerdo con Sergi (2018) en las legislaciones procesales aún no existe una definición normativa unívoca sobre el concepto de evidencia digital. Esta problemática ha sido estudiada por diversos organismos, que han desarrollado diversas propuestas, tomando en consideración sus características más destacadas.

Según la Guía de Prueba Electrónica del Consejo de Europa (2013, p. 23), "*la prueba electrónica es aquella información o datos que han sido creados, almacenados o transmitidos a través de dispositivos electrónicos y tienen relevancia en un procedimiento judicial*".

La IOCE (Organización Internacional de Evidencia Computacional) postula que la evidencia digital es "*toda información generada, almacenada o transmitida a través de medios electrónicos que puede ser utilizado en una corte judicial*" (IOCE, 2000, p. 12).

En el ámbito del *Common Law*, la definición más ampliamente aceptada por la doctrina especializada es la ofrecida por Casey (2011), para quien la evidencia digital es "*cualquier dato almacenado o transmitido utilizando computadoras que sustenta o*

rechaza una teoría sobre cómo ha sucedido un delito o que acredita elementos fundamentales del delito, tales como la intención o posibles coartadas".

Desde una perspectiva más restringida, la evidencia digital es en realidad un tipo de evidencia electrónica (concepto más amplio), aunque en algunas ocasiones son utilizados como sinónimos.

En términos generales, la evidencia electrónica contiene formas de datos análogos como fotos, audios o videos que pueden ser digitalizados y asumir formatos digitales aun cuando en su origen no lo eran. Por este motivo, algunos autores prefieren enfatizar en el concepto más amplio de la evidencia electrónica -incluyendo los datos análogos y digitales que adquieren la forma de datos digitales-, así como los datos en formato digital que son creados, manipulados, almacenados o comunicados por cualquier dispositivo informático o sistema informático, o transmitidos por un sistema de comunicaciones y que tienen relevancia para un proceso (Salt, 2017).

En esta investigación se entiende a la evidencia digital como el conjunto de datos e información, relevantes para una investigación, que se encuentra almacenada o transmitida por una computadora o dispositivo electrónico.

A su vez, las características y diferencias más notables entre los elementos de prueba físicos y los datos informáticos (evidencia digital) fueron desarrollados por el Consejo de Europa, exponiéndose a continuación (Sergi, 2018):

➢ El dato informático no es visible para las personas sin conocimientos y formación técnica especial. Esto implica que requiere algún tipo de traducción tecnológica del formato digital para ser apreciada por los sentidos de los operadores del sistema penal o de cualquier persona. De esta forma, la información almacenada en los dispositivos informáticos no es de gran utilidad para quienes no son especialistas debido a su carácter técnico y a la necesidad de conocimientos específicos que aseguren un tratamiento adecuado que evite alteraciones.

➢ El dato informático es bastante frágil y volátil. En algunos casos, las pruebas electrónicas son almacenadas en dispositivos electrónicos en los cuales cualquier acción puede alterar su estado. El cambio en la memoria de los dispositivos puede ocurrir por alterar el estado original en el que se halló un equipo (por ejemplo, apagarlo o

encenderlo), lo que genera la necesidad de implementar mecanismos especiales para asegurar la cadena de custodia de los datos.

➢ El contenido original puede ser alterado o destruido, incluso mediante el uso habitual del dispositivo electrónico. El estado de la memoria de los dispositivos electrónicos cambia constantemente, ya sea por voluntad del usuario ("guardar documento", "copiar archivo") o bien automáticamente por el sistema operativo ("asignar espacio para programa", "almacenamiento temporal de datos para intercambio entre dispositivos"). En otros términos, la evidencia digital conlleva un alto riesgo de ser alterada, tanto por la acción humana como por el funcionamiento y operatividad de los dispositivos.

➢ Masividad de la información digital y la consiguiente dificultad para la búsqueda de la información pertinente para el objeto procesal. La capacidad creciente de almacenamiento de los dispositivos y el bajo costo económico que tienen está generando un número cada vez mayor de documentos digitales. Sin perjuicio de las herramientas informáticas que permiten automatizar los procesos de búsqueda, la identificación de la evidencia digital pertinente en un dispositivo o sistema informático que puede transportar millones de documentos es un desafío logístico para los investigadores y un desafío para las garantías individuales por la posibilidad de encuentros causales[1], conocido como la doctrina del Plain View , o no tan casuales, de información indiscriminada, muchas veces alejada del objeto de prueba que habilitó una medida.

➢ La evidencia digital puede copiarse sin límites: en realidad, si la operación se efectúa correctamente y con los instrumentos necesarios, no se trata propiamente de copias sino de una clonación, ya que los nuevos resultados mantendrían todas las características del original. El contenido electrónico puede copiarse infinitas veces y ser exactamente igual al contenido original. Este atributo único permite realizar múltiples copias exactas al contenido original para ser distribuidas y analizadas por diversos especialistas al mismo tiempo (por ejemplo, puede entregarse una copia *bit a bit* a la defensa para que realice su propia pericia). De este modo, una correcta obtención de la

[1] Plain view doctrine: significa la doctrina o criterio de "a simple vista". Surge de jurisprudencia, que tiene su origen en precedentes judiciales estadounidenses donde se sentó la doctrina del "Plain View Doctrine" (Cam. Nac. Casación Penal, Sala I, causa 11.079 "Barone S.A. s/rec. de casación", del 11/04/1997). Y Se introdujo con la reforma por la ley 25.434 que agregó un tercer párrafo en el Art. 224 del C.P.P.

prueba digital permite que todas las medidas sean siempre actos de prueba reproducibles, en términos procesales (Salt, 2017).

El impacto de la evidencia digital en el sistema procesal probatorio argentino, importa también la necesidad de comprender una serie de términos y conceptos muy propios de sus sistemas y paradigmas, sin los cuales no se puede abordar ningún enfoque respecto a su funcionamiento.

1.2. Aspectos terminológicos y antecedentes normativos

En principio, es necesario plantear algunas definiciones básicas respecto de la terminología utilizada en torno a la evidencia digital, la cual debe ser manejada apropiadamente por los operadores del derecho. La primera distinción que se puede establecer es entre *hardware* -el soporte físico, por ejemplo, una PC o un teléfono inteligente- y *software* -soporte lógico, un programa informático, por ejemplo, el procesador de texto *Word*-. Si bien un teléfono y una computadora no son lo mismo en relación al hardware, pueden compartir un software (por ejemplo, el sistema *Android*).

Por medio del hardware y software se procesa información o datos que se encuentran almacenados en algún dispositivo electrónico, que seguramente es lo que se pretende validar o acreditar como prueba en un juicio, lo que constituye una evidencia digital. Dependiendo del equipo -hardware- y del programa -software- será más o menos difícil acceder a dichos datos que configuran la prueba. Aún obtenida esta información, se afrontará el problema de determinar la identidad del usuario, es decir, la persona física que redactó o cargó dicha información, y asociarlo a una identidad virtual, lo cual implica relacionar a la persona física, autora de los datos o información, con un determinado usuario de cuenta de correo, o de una red social (Bes, 2014).

Continuamos con la ley 25.506 de 2001[2] y el decreto 2628/2002[3] regulan todo lo concerniente a la firma digital y proveen definiciones sobre su alcance y certificación, en lo que constituye un antecedente relevante del objeto de estudio de la presente investigación. De acuerdo con esta normativa, se entiende por firma electrónica al conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizados por el firmante como su medio de identificación, que carece

[2] Ley Nº25.506, Régimen Legal de Firma Digital.
[3] Decreto 2628/2002, Reglamentario de Firma Digital

de algunos de los requisitos legales para ser considerada firma digital. En caso de ser desconocida la firma electrónica, corresponde a quien la invoca acreditar su validez. Por su parte, la firma digital es considerada el resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, de modo que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital, posterior a su firma. Se consigna, además, que los procedimientos de firma y verificación a ser utilizados para tales fines serán los determinados por la autoridad de aplicación, en consonancia con los estándares tecnológicos internacionales vigentes.

Por último, en la normativa citada el documento digital o electrónico es definido como la representación digital de actos o hechos, con independencia del soporte, utilizado para su fijación, almacenamiento o archivo. Un documento digital también satisface el requerimiento de escritura (art. 6° de la mencionada Ley N°25.506).

En cuanto a los conceptos "fuente de prueba" y "medios de prueba", pertenecen a la rama de estudio del Derecho procesal. Mientras que la "fuente" determina aquello que existe en la realidad, independientemente de la existencia de un proceso; el "medio" es un concepto que se explica como aquellas fuentes de prueba que se logran introducir de manera eficaz dentro del proceso. La fuente carecerá de consecuencias jurídicas, en tanto no se la pueda transformar en prueba. Como se planteó con anterioridad, la prueba digital es abundante y numerosa como fuente, aunque escasa como medio. El principal motivo de que ocurra esto es la falta de normativa procesal que contenga estos elementos, sobre todo en el fuero penal. También esta problemática se reitera por la propia velocidad con la que la tecnología se desarrolla en comparación con el derecho (Bes, 2014).

Resulta necesario señalar que tanto la aparición de las nuevas tecnologías, como la adquisición de la importancia que las mismas tienen en nuestra sociedad, son fenómenos que afectaron transversalmente a los sistemas jurídicos de todo el mundo, y sus implicancias son aún mayores en los países más desarrollados, porque es mayor la influencia de los sistemas tecnológicos en ellos. Es por esto que la problemática de los métodos de evidencia digital es enfocada globalmente.

1.3. La evidencia digital en el derecho comparado

Tal como se postuló en el apartado precedente, la evidencia digital ha colocado al proceso penal ante una problemática jurídica en relación a la posible adaptación de los medios probatorios tradicionales a las nuevas tecnologías, enfrentando también al proceso penal a la formulación de nuevos medios de prueba, de coerción probatorios, o medidas de investigación. Por ejemplo, al acceso transfronterizo de datos, los accesos remotos, o la utilización de software maliciosos por parte del Estado. En una u otra tarea, el examen jurídico es complejo y requiere de profundas discusiones condicionadas siempre por el resguardo de garantías constitucionales (principalmente, el derecho a la intimidad) y por garantizar la certeza del elemento probatorios (cadena de custodia)[4] en cuestión (Sergi, 2018).

Al abordar la legislación comparada en la materia se aprecia, en principio, que la misma responde a las brechas digitales existentes entre los países, donde difieren sustancialmente los mecanismos y medios para lograr que la evidencia digital pueda incorporarse como prueba en casos de juicios penales. En principio, se hará un simple relevamiento de la normativa que representa un avance en la configuración de la evidencia digital como prueba. Un primer aspecto a considerar, sobre todo en el fuero laboral, es cómo las nuevas tecnologías permiten la intromisión de los empleadores en la vida personal y períodos de descanso del trabajador. Por tal motiva, en Francia se promulgó legislación que obliga a los empleadores a dar al menos 11 horas de descanso informático; o sea dejar a los trabajadores libres de mails y comunicaciones laborales; habilitándolos para apagar teléfonos inteligentes y computadoras portátiles a partir de las 18 horas (Bes, 2014).

España cuenta con dos leyes que habilitan los documentos electrónicos como prueba, y que a su vez generan la obligación de conservar los datos de tráfico hasta doce

[4] Cadena de Custodia: es el control que se efectúa tanto de las personas que recogen la evidencia como de cada persona o entidad que posteriormente tiene la custodia de la misma. La cadena de custodia debe contener un identificador unívoco de la evidencia, de las fechas en las que los artículos fueron recogidos o transferidos, datos sobre el responsable que realizó la recolección, datos sobre la persona que recibe la evidencia y los datos de las personas que acceden, el momento y la ubicación física, número del caso, y una breve descripción de cada elemento. El pasaje de la evidencia de un sitio a otro y las tareas realizadas, cualquier cambio inevitable potencial en evidencia digital será registrado con el nombre del responsable y la justificación de sus acciones. El objetivo de la cadena de custodia es garantizar la autenticidad de la evidencia que se utilizará como prueba dentro del proceso. Fuente: resolución 234/2016.

meses. En América Latina, Colombia ha promulgado la ley 527 de 1999, que conceptualiza y establece la forma de acreditar los documentos electrónicos.

Respecto de las comunicaciones canalizadas por Internet, en Estados Unidos existen numerosos y diversos precedentes en los que los jueces establecen que la dirección de IP[5] no equivale a una persona, en una postura que se entiende acertada, si bien la dirección virtual que poseen todos los equipos conectados a Internet es determinable, este simple hecho, por sí mismo resulta insuficiente para imputársela a una persona[6], pues quien produjo los datos que conforman la prueba podría ser cualquier usuario de ese hogar o espacio laboral al que pertenece la IP, o mismo un hacker que irrumpió en dicha conexión y la utiliza como lugar de salida o falso (Bes, 2014).

En Argentina, por ejemplo, actualmente las empresas no están obligadas a preservar las evidencias o pruebas digitales – aun cuando existen parámetros claros sobre tiempos y modos de preservación-, ni tampoco reciben consecuencias por su reticencia a exhibir y demostrar las mismas, cuando sí, por ejemplo, se las obliga a preservar los libros contables en formato de papel. Este dato no es menor, ya que llegar tarde o no lograr garantizar la indemnidad de archivos virtuales equivale a perder la prueba informática que pudiera existir.

En la medida en que queda claro que el problema de incorporar a la evidencia digital a sistemas jurídicos que aún no contemplaban este nuevo paradigma, es un problema transnacional, que afecta a casi todos los países del mundo, resultaba inevitable que se intente tomar una determinación desde un ámbito plurinacional, que permita contemplar e incorporar las experiencias previas y características particulares de las distintas naciones en este aspecto, a fin de encontrar una solución integral que pueda unificar criterios en todos los Estados parte. Esta búsqueda de determinar una solución global, y un efecto de unificación normativa en los distintos sistemas jurídicos, se realizó en la Convención de Budapest. La misma, busca establecer un piso mínimo de regulación normativa que recepte los sistemas informáticos de común utilización en la legislación de los Estados parte.

[5] IP(Internet Protocol).: es un número que identifica, de manera lógica y jerárquica, a una Interfaz en red (elemento de comunicación/conexión) de un dispositivo (computadora, tableta, portátil, smartphone) Fuente Wikipedia: https://es.wikipedia.org/wiki/Direcci%C3%B3n_IP.

[6] Ver nota en https://torrentfreak.com/ip-address-cant-even-identify-a-state-bittorrent-judge-rules-120515/

1.4. Convención de Budapest. Convención Europea sobre Delitos Informáticos

Considerada un hito entre los fundamentos de su creación, está la aplicación de una política penal común frente al ciberdelito o ciberdelincuencia, la adopción de una legislación adecuada, mejora de la cooperación. Para cumplir los objetivos, se busca que los medios de prueba especiales previstos, para la obtención e incorporación al proceso de las pruebas digitales, se apliquen no sólo en la investigación de los delitos informáticos sino, en forma general, a todos los procesos penales en los que resulte necesaria la obtención de evidencia digital.

El convenio de Budapest[7] consta de 48 artículos de divididos en cuatro capítulos con sus respectivas secciones. Que incluyen desde definiciones de conceptos, recomendación de medidas a tomar, cooperación internacional, escenarios de asistencia entre los estados partes hasta medidas de investigación.

1.4.1 Principales instrumentos incorporados como novedad para el manejo de la Evidencia digital y sus formas de investigación asociada.

El primer capítulo se encarga de definir términos como *sistema informático*, *dato informático*, *proveedor de servicio* y *datos de tráfico*. En el punto de la definición de dato de tráfico, genera inconvenientes en su consideración y adaptación a los procedimientos ya que no especifica los otros datos que pueden ser recolectados o pedidos como parte de una investigación como son los datos del abonado, datos de contenidos.

El segundo capítulo especifica las conductas delictivas que los ordenamientos de los estados partes tienen que legislas, en nuestro caso con la promulgación de la ley 26.388 [8] (2008), cubrimos esta expectativa. Asimismo, establece medidas procesales para las investigaciones:

Medidas de aseguramiento de datos, conservación rápida de los datos conocida como *Quick Freeze*, ordenando por las autoridades encargadas de la investigación a los administradores de sistemas informáticos donde se encuentran los datos alojados que se quieren reservar, protegiendo la integridad de los mismos evitando

[7] Ver en https://www.oas.org/juridico/english/cyb_pry_convenio.pdf . Versión en español.
[8] Ley 26388 (2008). De delitos informáticos.

que sean eliminados antes o durante la investigación, por un tiempo máximo de noventa días.

Siguiendo con las definiciones en materia investigativa permite el registro y confiscación de dispositivos informáticos (art.19), obtención en tiempo real de datos de tráfico (art. 20) o interceptación de datos relativos a contenido (art.21).

El tercer capítulo trata sobre cooperación internacional y establece disposiciones sobre asistencia mutua en temas como extradición o acceso, conservación, obtención en tiempo real e interceptación de datos.

Con relación al Acceso transfronterizo de datos en su artículo 32 establece concretamente el acceso trasfronterizo de datos, vinculado solo a casos cuando se intenta acceder en forma local o remota a datos que se encuentran almacenados fuera de la jurisdicción nacional. Siempre y cuando sea con consentimiento y los datos sean de acceso público en fuentes abiertas.

Cualquier situación diferente a la descripta anteriormente será necesario vincular la acción investigadora a través de la cooperación judicial internacional. Ello implica que se deberá remitir la correspondiente solicitud de asistencia judicial internacional fundamentándose en el propio Convenio de Budapest o en otro instrumento internacional que pueda resultar de aplicación.

En este punto un tema no regulado pero que actualmente en las investigaciones es usa son los casos conocidos como de *cooperación asimétrica* que sería el vínculo ya no entre estado sino estado y empresa privada que brinda servicio o que aloja el dato necesario para la investigación ejemplo Google, Amazon. Facebook.

En este punto Koops & Goodwin (2014) señalan que ante una búsqueda transfronteriza no consensuada o ante un caso de cooperación asimétrica, haría que las investigaciones más efectivas, pero actualmente estas formas no están permitidas, establecen que los estados deben trabajara para regular las situaciones de acceso a esta

También nos recuerda que, en la interpretación estricta y dominante del derecho internacional, cualquier actividad de recopilación de pruebas en un estado extranjero, incluida la realización de una mera llamada telefónica, puede considerarse una violación de la soberanía. El acceso a los datos que se almacenan en un servidor ubicado en el territorio de otro estado, o que luego resulta que están sin su consentimiento previo, constituye una violación de la

La única excepción es cuando el estado extranjero haya dado su consentimiento previo, ya sea para una búsqueda específica en una solicitud específica, o en forma genérica para ciertos tipos de búsquedas bajo ciertas condiciones; este último es el caso del artículo 32 del Convenio sobre delitos informáticos, que permite el acceso transfronterizo a los datos con el consentimiento del usuario o proveedor, si ambos países son parte del Convenio.

En este punto también tenemos un caso emblemático de jurisprudencia de Estados Unidos y que genero muchas discusiones en el plano internacional por la cuestiones jurídicas planteadas y por la importancia política de las potencias involucradas Estados Unidos vs Rusia año 2000, este es el caso de dos programadores rusos Gorshkov-Ivanov[9], quienes valiéndose de un fallo en la seguridad del sistema operativo Windows NT ingresaron a los sistemas de varias empresas estadounidenses robaron datos de tarjetas de créditos. Detectado el fraude el gobierno de Estados Unidos inicio sus investigaciones ingresando sin mediar autorización a los servidores de Rusia accediendo a datos ahí almacenados y con esta evidencia obtenida ambos hackers fueron arrestados y acusados de conspiración, fraude informático, piratería y extorsión. Este caso abrió el debate sobre las reglas de privacidad, tratados internacionales, violación de derechos constitucionales, accesos ilegítimos, principio de territorialidad.

Otro caso sobre el acceso transfronterizo fue el de Estados Unidos vs Microsoft[10], un poco más reciente 2013 este caso se dio el marco de una causa de narcóticos un poco más reciente, Microsoft recibió una orden judicial del gobierno estadounidense, para obtener información de una cuenta de mail, bajo la ley de comunicaciones almacenadas (SCA Stored Communicatios Act)[11] en esta oportunidad la empresa remitió los metadatos asociados a la cuenta que estaban alojados en servidores de Estados Unidos no brindando información sobre los mails ya que su contenidos, estaban almacenados en servidores

---

[9] https://www.csoonline.com/article/2118241/alexey-ivanov-and-vasiliy-gorshkov--russian-hacker-roulette.html. *Estados Unidos v. Ivanov* , 175 F. Supp. 2d 36 (Tribunal de Distrito de los Estados Unidos para el Distrito de Connecticut 2001.

[10] Fuentes: https://blogs.microsoft.com/datalaw/initiative/legal-cases/microsofts-search-warrant-case/ https://www.supremecourt.gov/search.aspx?filename=/docket/docketfiles/html/public/17-2.html https://adcdigital.org.ar/estados-unidos-microsoft-desafiando-el-acceso-transfronterizo-de-datos/ https://cdt.org/insight/microsoft-ireland-case-can-a-us-warrant-compel-a-us-provider-to-disclose-data-stored-abroad/

[11] SCA: La Ley de comunicaciones almacenadas, es una ley que trata la divulgación voluntaria de "comunicaciones electrónicas y electrónicas almacenadas y registros transaccionales" en poder de terceros proveedores de servicios de Internet (ISP) . Fue promulgado como Título II de la Ley de Privacidad de las Comunicaciones Electrónicas de 1986 (ECPA). Fuente: https://en.wikipedia.org/wiki/Stored_Communications_Act

de Irlanda, ante rechazo la compañía esto fue declarado en desacato y en el año 2017 se elevó el caso a la Corte Suprema de Estados Unidos declarando que la posición del gobierno de los Estados Unidos afecta el derecho fundamental a la privacidad, sobrepasando las leyes de Irlanda y la Unión Europea que protegen los datos personales, a la vez que regulan quién, cómo y con qué alcance, actores privados como Microsoft pueden transferir datos personales a terceros países.

Conclusiones parciales

Se debe cambiar la mirada tradicional y entender que la evidencia digital requiere de medios de prueba específicos diferentes de los pensados para las evidencias físicas, la evidencia digital deber ser manejada conforme a procedimientos legales, para asegurar que su obtención esté debidamente documentada, preservada y disponible para su utilización y revisión.

En cuanto a la aplicación efectiva de la Convención uno de los requisitos para su incorporación es la modificación de las leyes procesales. Volviendo a nuestro sistema en particular, existen una serie de principios que rigen nuestro derecho penal, y en lo particular, nuestro derecho procesal penal, que muestran ciertos límites a la incorporación de la evidencia digital dentro del sistema jurídico, impidiendo así su consagración normativa, o en general, imponiendo un marco de adecuación para dicho proceso. Resulta evidente que para no violar ninguna de nuestras garantías o principios fundamentales, es necesario desarrollar un marco de aplicación que incorpore también una ampliación en la comprensión de estos valores, que tienen que tener su faceta regulada positivamente en el campo digital. Es, por ejemplo, un hito a analizar, el reconocimiento de que en esta era digital resulta necesario redefinir el alcance del derecho a la privacidad como valor jurídico protegido, ya que gran parte de los datos que entendemos como privados hoy en día, se almacenan en dispositivos electrónicos, y que, en algún momento o circunstancia, pueden hacerse públicos.

Capítulo 2. El cibercrimen y la evidencia digital: su impacto en el derecho procesal penal

Introducción

En el contexto de actual de constate evolución de las tecnologías de la información y la comunicación (Tics), mayor acceso a los medios informáticos y la mejora en el manejo de las habilidades de los sistemas informáticos, trae aparejado una mayor sofisticación en la comisión de delitos informáticos. En este segundo capítulo realizaré una introducción a las principales figuras introducidas por la normativa ley 26.388[12] del 2008.

En un comienzo, la evidencia digital se relacionó directamente a los delitos informáticos y a la cibercriminalidad en general. Ello debido a que estos requerían indefectiblemente de aquella para poder probarse, porque ningún medio alternativo tenía la eficacia probatoria necesaria para judicializar los delitos informáticos. Los medios de prueba convencionales no servían para probar, entre otros, el acceso ilegítimo o el *grooming*[13], posteriormente incorporado en la legislación Ley 26.904 de Noviembre 2013.

Para poder entender el funcionamiento práctico y actual de la evidencia digital en Argentina, primero resulta necesario describir las regulaciones actuales, tanto en el derecho de fondo como en cuanto al derecho procesal respecto a la evidencia digital. Asimismo, es necesario contemplar tanto aquellos delitos descriptos por el nuevo marco normativo de la ley N°26.388, como las referencias (y ausencias) de las normas procesales vigentes en el nuevo Código Procesal Penal de la Nación.

[12] Ley N° 26.388, de Delitos Informáticos.

[13] Grooming: es un engaño pederasta, más conocido por el anglicismo grooming (en español «acicalando»), es una serie de conductas y acciones deliberadamente emprendidas por un adulto, a través de Internet, con el objetivo de ganarse la amistad de un menor de edad, creando una conexión emocional con el mismo, con el fin de disminuir las preocupaciones del menor y poder abusar sexualmente de él. En algunos casos, se puede buscar la introducción del menor al mundo de la prostitución infantil o la producción de material pornográfico. Fuente: https://es.wikipedia.org/wiki/Enga%C3%B1o_pederasta

2.1. Nuevo marco normativo instituido por la Ley N°26.388

Antes de desarrollar el régimen jurídico establecido por la ley N°26.388 es preciso mencionar una serie de antecedentes de proyectos presentados en el Congreso de la Nación a fin de incorporar en la República Argentina una norma que regule la utilización de las herramientas digitales en nuestra realidad diaria, en el espectro del ámbito penal. Sueiro (2015) describe los siguientes: Proyecto de Leonor E. Tolomeo (1996); Proyecto de Carlos R. Álvarez (1996); Proyecto de José A. Romero Feris (1996); Proyecto de Antonio T. Berhongaray (1997); Anteproyecto de Ley de Delitos Informáticos (2001); Proyecto de Marta L. Osorio (2005); Proyecto de Silvia V. Martínez (2005); Proyecto de Andrés Sotos (2005); Proyecto de Delia B. Bissutti (2006); Proyecto de Dante O. Canevarolo (2006); Proyecto de Diana Conti y Agustín Rossi (2006) y Anteproyecto de Ley de Reforma y Actualización Integral del Código Penal.

Si bien es posible percibir en la mayoría de estos proyectos una clara intención de adecuarse al régimen establecido en el "Convenio sobre la Ciberdelincuencia de Budapest", es evidente que sólo se ha seguido sus lineamientos en lo que refiere al derecho penal sustantivo, previsto en el Capítulo II, "Medidas que deberán adoptarse a nivel nacional, Sección 1, "Derecho Penal Sustantivo". Pero, por otro lado, no adecuan la normativa nacional a lo establecido en la Sección 2, destinada al "derecho procesal". En estos proyectos se evidencia la necesidad de incorporar medidas legislativas que permitan establecer procedimientos penales específicos para la obtención de pruebas electrónicas de cualquier delito cometido por medio de un sistema informático.

La Ley N°26.388 modificó el Código Penal para incluir como conductas típicas, asociadas al cibercrimen, la falsificación de documentos electrónicos (CP, arts. 77 y 292); ofrecimiento y distribución de pornografía infantil –la tenencia sólo fue tipificada cuando tiene fines inequívocos de distribución o comercialización- (CP, art. 128); conductas vinculadas a la violación de secretos y la privacidad, que incluyen el acceso ilegítimo a sistemas informáticos ajenos, la intercepción de correspondencia electrónica y otras formas de comunicación, la revelación de secretos y los delitos relacionados con la protección de datos personales (CP, arts. 153, 153 bis, 155, 157 y 157bis); fraude informático (CP, art. 173, inc. 16); daño informático (CP, arts. 183 y 184); interrupción de comunicaciones (CP, art. 197) y la destrucción de pruebas contenidas en soportes

informáticos (CP, art. 255). Estas modificaciones generaron problemas dogmáticos en torno a los tipos penales sancionados (Palazzi, 2009).

2.2. Nuevo Código Procesal Penal de la Nación de 2014

En diciembre del 2014 el Congreso sancionó un nuevo Código Procesal de la Nación[14]. Este incorporó una nueva regulación en materia probatoria. En concordancia con su naturaleza acusatoria, estableció la libertad probatoria (art. 127, Libro IV, "Medios de prueba", Título Primero, "Normas generales") disponiendo que: *"Podrán probarse los hechos y circunstancias de interés para la solución del caso, por cualquier medio de prueba, salvo que se encuentren expresamente prohibidos por la ley. Además de los medios de prueba establecidos en este Código, se podrán utilizar otros, siempre que no vulneren derechos o garantías constitucionales y no obstaculicen el control de la prueba por los demás intervinientes"*.

Esta disposición permite entender, pese a que el Libro IV y los cuatro títulos que lo comprenden (Comprobaciones directas, Testimonios, Peritajes y Otros medios de prueba) no hacen ninguna referencia a la evidencia digital o prueba electrónica, que, si bien está orientada a pruebas físicas o corpóreas, puede igualmente aplicarse a otros medios de prueba distintos a los referenciados, como lo sería la evidencia digital. Este principio de libertad probatoria será desarrollado más adelante.

2.3. Relación con el debido proceso

La introducción en nuestro sistema jurídico de la evidencia digital en el proceso penal resulta un hecho inevitable si se pretende acercar la justicia a la realidad diaria. Y en este enfoque, resulta fundamentalmente necesaria una regulación más específica de ella, porque constituye una garantía también para la concreción del debido proceso.

Sin embargo, hoy existe un vacío normativo en la materia, por lo cual es necesario garantizar alternativamente el debido proceso, el derecho de defensa del imputado, y el justo juicio, mediante la preconstitución de la prueba judicial, o su peritaje ordenado judicialmente, y su ulterior preservación y conservación, de acuerdo a los protocolos y procedimientos propios que requiere la evidencia digital, los cuales se

[14] Ley N° 27063, con fecha diciembre 2014 aprueba la reforma al CPPN.

desarrollarán más adelante. Esto permitirá confirmar la inalterabilidad e integridad de la prueba obtenida, y facultará el control de las partes en la etapa preliminar, y durante la etapa de juicio oral, lo cual reforzará el cumplimiento del debido proceso.

Contar con procedimientos preestablecidos de actuación para la obtención de pruebas digitales resulta cada vez más urgente, teniendo en consideración la entrada en vigencia de la ley 26.685[15] (2011), que persigue la implementación del expediente electrónico y la incorporación de los ya mencionados delitos informáticos en nuestro sistema penal.

2.4. Relación con el principio de libertad probatoria

Analizando el impacto de la evidencia digital en el derecho procesal probatorio, es preciso plantear su vínculo con el instituto que la habilita, es decir, el principio de libertad probatoria.

De acuerdo a lo explicado previamente, el principio de libertad probatoria se encuentra incorporado a nuestro régimen penal mediante el nuevo Código Procesal Penal de la Nación, y consiste en que dentro del ámbito del derecho procesal penal todo objeto de prueba puede ser probado por cualquier medio. Esto permite no sólo la incorporación de medios de prueba no previstos, sino la aplicación analógica de acuerdo a medios probatorios regulados.

Sin embargo, este principio no es absoluto, sino que existen limitaciones probatorias originadas en la propia Constitución Nacional, y los derechos humanos radicados en ella. Por tal motivo la libertad probatoria no puede avalar las pruebas obtenidas en desmedro de garantías constitucionales o prohibidas por la ley. Dichas limitaciones pueden ser:

- *Absolutas*: cuando la limitación recae sobre el objeto de la prueba.
- *Relativas*: cuando recae sobre medios o procedimientos.

De esta forma, el principio de libertad probatoria no puede justificar que el Estado haga cualquier cosa en la búsqueda de la verdad, sin importar que su actuación sea motivada por la investigación de un hecho ilícito que sea de especial gravedad. Si

[15] Ley N° 26685, de Expedientes Digitales.

bien la introducción de este principio en nuestro régimen procesal probatorio abre una puerta a la incorporación de la evidencia digital, su falta de regulación explícita conduce a un vago espacio de interpretación respecto a cómo debe ser obtenida e incorporada.

2.5. Relación con el principio de *nulla coactio sine lege*

Al igual que con el principio de libertad probatoria, la introducción de la evidencia digital en nuestro régimen procesal penal, despierta la necesidad de reinterpretar el principio de *nulla coactio sine lege*. Este instituto consiste en que todos los mecanismos de investigación, procedimientos probatorios o medios de prueba que impliquen algún grado de injerencia en los derechos fundamentales reconocidos por las normas constitucionales, deben estar fundados en una ley, la cual, a su vez, no debe alterar, sustituir o modificar el principio constitucional que reglamenta. Es a raíz de este principio que Bruzzone y Bertolino (2005) establecen una diferenciación entre los medios de prueba en general (aquellos que no tienen ningún grado de injerencia en los derechos mencionados), de los medios asociados a las "medidas de coerción probatoria" donde sí se contempla la afectación a los derechos fundamentales.

En lo que respecta específicamente a la evidencia digital, resulta claro que este principio pone un obstáculo evidente a su legitimidad. Cualquier necesidad que tenga el Estado de ejercer coerción o cualquier actividad a fin de obtener material probatorio en datos de los dispositivos electrónicos de los ciudadanos, implica una injerencia en nuestro ámbito de garantías, por lo cual sólo podrían usarse válidamente si están expresamente previstos por una ley previa, lo cual dispone como válida únicamente aquella evidencia digital recabada que no vulnere derechos o garantías constitucionales.

En relación a este principio Maier (2012) afirma que la vigencia de dicho principio deriva del carácter reglamentario que las normas legales tienen en ésta materia respecto del texto constitucional[16].

2.6. Relación con el derecho a la intimidad

Actualmente, la cantidad de datos que circulan por medios electrónicos es demasiado grande e importante. Información que antes se transmitía por otros medios,

[16] Maier, Julio "Derecho Procesal Penal Tomo 3". Ad Hoc 2012

hoy se encuentra en millones de dispositivos electrónicos. El desarrollo de la tecnología obliga a reflexionar y rediseñar el denominado derecho a la intimidad. Tanto en lo que refiere al cibercrimen como a la incorporación de la evidencia digital como medio probatorio en los procesos penales, es posible establecer vinculaciones que justifiquen el rediseño de aquel instituto.

2.6.1. Poder probatorio de la evidencia digital

A su vez, en cualquier investigación, por cualquier delito que tenga al derecho a la intimidad como bien jurídico protegido, la evidencia digital resulta aportante de un importante poder probatorio dentro del proceso. Es por ello que el concepto de intimidad que se asumía antes de la revolución tecnológica hoy debe ampliarse y tener en consideración el impacto y las consecuencias socioculturales de las nuevas tecnologías. En este sentido, ha surgido un nuevo ámbito de intimidad personal, construido a partir de la vinculación particular entre las personas, los sistemas informáticos y las redes sociales, generado a partir de la masificación del acceso a las herramientas informáticas y de telecomunicaciones. El primer paso para delinear este ámbito, es ver la regulación que tiene el derecho a la intimidad en la Constitución Nacional.

El art. 18, desarrolla el derecho a la intimidad, entendiendo a éste como la posibilidad de excluir a terceros, incluyendo al Estado, del conocimiento de determinados hechos, circunstancias, comunicaciones o datos registrados en diferentes soportes, ya sea virtuales o físicos. La norma expresa: "… *el domicilio es inviolable, como también la correspondencia epistolar y los papeles privados; y una ley determinará en qué casos y con qué justificativos podrá procederse a su allanamiento y ocupación*...".

Se refiere textualmente a lo que sucede en un domicilio, lo que se registró en papeles privados o lo que se comunicó en una carta, pero en la interpretación del mismo, si se busca acercar el espíritu de la norma a la realidad actual, debemos comprender que también incluye otros tipos de espacios privados, como el secreto bancario o fiscal, las comunicaciones telefónicas y otro tipo de comunicación mantenida por medios electrónicos, como el correo electrónico o la comunicación a través de voz IP. Esta tarea resulta necesaria, para no dejar sin protección constitucional aspectos trascendentales para la intimidad de los ciudadanos, como las comunicaciones privadas por medios electrónicos. Esta garantía constitucional no es absoluta, sino que la misma norma

autoriza a los legisladores a establecer un marco sobre el cual existan determinados supuestos de injerencia estatal, a determinar por los códigos procesales penales.

El art. 19, en una acepción más vinculada al principio de privacidad, pero a su vez relacionada intrínseca y complementariamente con el de intimidad, establece: "*Las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están sólo reservadas a Dios, y exentas de la autoridad de los magistrados. Ningún habitante de la Nación será obligado a hacer lo que no manda la ley, ni privado de lo que ella no prohíbe*".

Esta disposición establece un ámbito de protección del ciudadano, dentro del cual se le permite realizar todas las acciones que no afecten a terceros, sea que se realicen de manera privada o pública. Esta idea de privacidad permite también entender y fundamentar la necesidad de garantizar la protección de la intimidad de determinada información o dato, cuando pueda significar un menoscabo en la autonomía individual de una persona, cuestión que puede ser importante a los fines de resguardar a los ciudadanos frente a la intromisión del Estado en sus sistemas informáticos.

Por otro lado, la Convención Americana sobre Derechos Humanos, como parte de nuestro bloque constitucional, dispone en su art. 11: "… *Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación*…". Esta norma complementa a las desarrolladas en los arts. 18 y 19 de la Constitución Nacional.

La relación de las personas con los sistemas informáticos presenta una serie de situaciones bajo las cuales es inevitable no incorporar a estos últimos bajo el derecho a la intimidad. Se genera un consenso alrededor de la idea de que cualquier acceso por parte del Estado a las computadoras personales o los teléfonos inteligentes de sus ciudadanos en muchos casos representa el mismo o inclusive un mayor grado de injerencia en la intimidad que si se produjese el acceso a sus domicilios o sus vehículos.

Pero al mismo tiempo, es cada vez más necesario, a fin de llevar a la verdad a las investigaciones criminales en la mayoría de los delitos, el primero de los mecanismos, para obtener evidencia digital, que el segundo de ellos. La capacidad de almacenamiento de datos de los sistemas informáticos es en general mucho mayor que la que puede encontrarse en un domicilio. Por ejemplo, el registro de una computadora o de la memoria de un teléfono inteligente podría no sólo permitir el conocimiento de los documentos,

fotos, videos, y demás archivos que existen en el momento en que se realiza la extracción, sino que puede obtener también datos del pasado o incluso de terceras personas que hubieran tenido contacto con el dispositivo.

Inclusive, se puede acceder a elementos que el propio ciudadano no haya documentado ni guardado intencionalmente, tales como documentos electrónicos existentes o incluso los borrados por el usuario, aunque hubiera transcurrido un tiempo considerable. De este modo, se obtienen correos electrónicos, incluso aquellos que la persona hubiera decidido eliminar; tendencias y gustos personales y datos sensibles como tendencias religiosas, políticas, orientación sexual; páginas web visitadas; fotos y videos; manejo de cuentas bancarias; personas con las que se comunicó; películas vistas; interacción con otras personas en redes sociales, viajes realizados y planeados, y otros aspectos de la intimidad de las personas.

De esta manera, sería una desafortunada incoherencia jurídica que el registro del domicilio, de la correspondencia epistolar y demás elementos mencionados expresamente en la normativa vigente estén protegidos por el derecho a la intimidad, y los sistemas informáticos no gocen de dicha garantía. Parecería mucho más coherente una interpretación dinámica de la Constitución Nacional, que permita ampliar el espectro de protección del derecho a la intimidad, que habilite la incorporación de los sistemas informáticos privados en el mismo. En este enfoque, podemos ver que igualmente este derecho no es absoluto, sino que la propia norma permite que una ley establezca en qué presupuestos, con qué condiciones y de acuerdo a qué requisitos, el Estado puede intervenir dentro del ámbito de intimidad de sus ciudadanos. En lo que refiere a este accionar, interviene el principio de legalidad, porque es necesaria una ley para habilitarlo.

Si bien se puede pensar que en la vida cotidiana las nuevas tecnologías flexibilizan el derecho a la privacidad; en realidad, en el ámbito jurídico, y más aún en el examen de las facultades con las que cuenta el Estado para acceder a los ámbitos de intimidad, el resguardo debe ser más estricto, debido a que cuanto mayor peligro en la violación a la intimidad, mayor es el cuidado y la estrictez que debe tener el Estado en su manipulación. De modo que no siempre el problema yace en la previsión constitucional o legal, sino en la manera de interpretarla.

De acuerdo al art. 116 de la Constitución, que dispone que "… *corresponde a la Corte Suprema y a los tribunales inferiores de la Nación, el conocimiento y decisión de todas las causas que versen sobre puntos regidos por la Constitución*…", es un juez quien

debe ordenar una medida de coerción probatoria, por lo que es él quien debe interpretar cuándo la misma resulta conforme a derecho. Para ello, debe verificar que se cumplan las exigencias formales establecidas por el legislador para acceder a determinados ámbitos de intimidad. Algunos requisitos específicos que debe contemplar son los siguientes:

- Debe tener una motivación suficiente que permita justificar que es necesario ese grado de intrusión.
- Debe brindar también criterios de proporcionalidad en la disposición de la medida, respecto a dicha motivación, teniendo en cuenta la extensión y la gravedad de la intrusión.
- Y debe constituir el menor gravamen posible para lograr una eficacia de la medida sin violentar o restringir el derecho a la intimidad u otros más allá de lo que resulte necesario.

Finalmente, se puede arribar a la conclusión de que la jurisprudencia no debiera tener que llevar adelante la habilitación de estas medidas coercitivas para investigar los sistemas informáticos, utilizando el vehículo de la analogía. Colisiona la clara realidad de que, por un lado, resulta fundamental en la actualidad la incorporación de los métodos coercitivos de obtención de prueba digital para la investigación de cualquier delito, pero por el otro, sin una ley que regule esos mecanismos, estableciendo los presupuestos, condiciones y requisitos que deben tener, y definiendo los supuestos en que deben proceder, se deja a la interpretación judicial un amplio y vago espectro de actuación, que se comprende irrazonable y riesgoso, entendiendo que afecta a un derecho constitucional como la intimidad.

Si bien no resulta plausible ni razonable jurídicamente que toda medida realizada sobre un sistema informático se considere prohibida por no estar regulada, también hay que reconocer que el sistema normativo actual muchas veces pone en riesgo, por los fundamentos dados, la validez de dicha medida. Su validez o legitimidad la determinan en la actualidad las circunstancias concretas del caso, lo cual obliga al magistrado a realizar un examen laborioso de la situación concreta, analizando los posibles accesos a distintos sistemas informáticos, el objetivo de la búsqueda, los posibles hallazgos, la extensión temporal de la medida, el grado de injerencia que implica, los bienes jurídicos en juego, y otras tantas cosas más. Siendo así, puede haber inclusive, de acuerdo al caso,

distintos grados de intervenciones para cada circunstancia, como, por ejemplo, la intercepción de los correos de la computadora digital, pero no del resto del contenido, o la intercepción de todos los medios de comunicación electrónica, pero no de aquellos sistemas informáticos que no sirvan para comunicarse.

A nivel derecho comparado un antecedente importante que podemos traer a colación es el histórico caso Katz v. Estados Unidos[17] (1967), este caso analiza el *derecho a la privacidad* y la definición legal de una *búsqueda* de bienes intangibles, como la electrónica. Comunicaciones basadas como llamadas telefónicas. El fallo introduce la expectativa razonable de privacidad. El caso Katz hizo que las escuchas telefónicas del gobierno por parte de las autoridades estatales y federales estuvieran sujetas a los requisitos de la Cuarta Enmienda[18]

2.6.2. El cibercrimen y su afectación al derecho a la intimidad

A partir de lo expuesto, resulta evidente destacar que la aparición del cibercrimen también exigió un rediseño del derecho a la intimidad, en cuyo caso el accionar de los legisladores fue relativamente más exitoso. Ello es así porque una gran parte de los delitos informáticos, atentan justamente contra la mencionada garantía constitucional, y su tipificación en el nuevo marco normativo instituido en Ley N°26.388 (2008), demuestra que es el derecho a la intimidad el bien jurídico protegido. Este es el caso, por ejemplo, de las conductas vinculadas a la violación de secretos y la privacidad, que incluyen el acceso ilegítimo a sistemas informáticos ajenos, la intercepción de correspondencia electrónica y otras formas de comunicación, la revelación de secretos y los delitos relacionados con la protección de datos personales (CP, arts. 153, 153 bis, 155, 157 y 157

[17] "Katz v. Estados Unidos". www.oyez.org/cases/1967/35.

[18] La cuarta enmienda de la Constitución de los Estados Unidos protege dos derechos fundamentales: el derecho a la privacidad y el derecho a no sufrir una invasión arbitraria. La pesquisa es el procedimiento en el que un funcionario o agente del gobierno viola una expectativa razonable de privacidad. Fuente: https://www.law.cornell.edu/wex/es/legislaci%C3%B3n_sobre_pesquisas_y_confiscaciones_cuarta_enmienda.

bis). Como lo señala Palazzi (2009), estos artículos amparan la reservan la confidencialidad y el derecho a la privacidad del titular del sistema y del dato informático.

Si bien hay muchos aspectos a trabajar y discutir en las normas y disposiciones instauradas en la nueva ley, como la extensión de las penas, los elementos objetivos de la tipicidad de algunos delitos, o la incorporación de delitos nuevos no comprendidos en la ley, entre otros, lo que es posible destacar en esta ley es que ya la tipificación de estos delitos requiere el rediseño de derecho a la intimidad. Y necesariamente volvemos al art. 153 bis el conocido Hacking o intrusismo informático debe considerarse un delito, sin una afectación concreta a otros derechos o bienes jurídicos a proteger, estamos reconociendo que estos sistemas se consideran bajo el amparo del derecho a la intimidad.

Esta modificación pone en valor la necesidad de proteger los datos personales que las personas incorporan a sus sistemas informáticos, así como la propia actividad que ellas realizan con aquellos, debido a que la mera actividad de que un tercero acceda a dicha información constituye un accionar delictivo, agravado aún si dichos datos se dan a conocer o se manipulan de distintas maneras. El problema a abordar, como se mencionó previamente, es que por una operativa lógica la obtención y producción de evidencia digital resulta clave para investigar estos delitos. Y para ello, resulta fundamental y necesario la constitución de un régimen procesal que le dé un adecuado trato a este medio probatorio, en consideración de todos los derechos, garantías y bienes jurídicos relacionados, para que se pueda llevar una adecuada tarea jurisdiccional y atender estas nuevas realidades tecnológicas que afectan transversalmente a toda la sociedad, por lo cual también afectan a todo el sistema jurídico.

Conclusión parcial

Si bien la Ley 26.388, sancionada en el año 2008, permitió modificar el Código Penal incorporando los delitos informáticos (considerados como tales la distribución y tenencia, con fines de distribución, de pornografía infantil; la violación del correo electrónico; el acceso ilegítimo a sistemas informáticos; el daño informático y la distribución de virus; el daño informático agravado e interrupción de comunicaciones),

Es un avance para dar claridad y personalidad a la tipificación de las nuevas modalidades delictivas trato de ser amplio en la descripción de los tipos, pero va a ser una constante

en el tiempo la modificación de las mismas ante la evolución y sofisticación de los delincuentes

Sin embargo, desde el punto de vista jurídico la dificultad se ha agravado, toda vez que el avance de las tecnologías y la utilización de Internet en la vida cotidiana, han llevado la cuestión informática a cualquier investigación, involucrando todo tipo de hechos. Junto con sus complicaciones, la evidencia digital atraviesa hoy el sistema de manera transversal (desde cualquier caso menor y simple hasta los más complejos y casos del derecho penal común, así como los delitos de cuello blanco). De este modo, en el ámbito del derecho procesal penal, y en relación con la vigencia de las garantías legales y constitucionales, se presentan desafíos novedosos que requieren una adecuación del marco normativo.

Capítulo 3. Sistemas y mecanismos de apreciación de la prueba digital

Introducción

Dentro de la actividad probatoria que implica un esfuerzo de todos los sujetos procesales en lo que respecta a la producción, recepción y valoración de los elementos de prueba. En este capítulo se desarrollará los sistemas de valoración y mecanismo de preconstitución de las evidencias digitales, los principios rectores que debería respetar la recolección de la evidencia digital, el rol de los expertos en las pericias y los tipos de Evidencia Digital que se puede aportar a la investigación según el tipo de delito investigado.

3.1. Sistemas de valoración de la prueba

De acuerdo a Cafferata Nores (1998), los principales sistemas de valoración de la prueba son: el de la prueba legal, el de la íntima convicción y el de la libre convicción o sana crítica racional.

a) Prueba legal, es la ley procesal la que establece o pre-fija ante cada prueba como debe darse por convencido, el juez de la existencia del hecho, aunque íntimamente no esté convencido.
b) Íntima convicción, el juez es libre de convencerse según s intimo parecer, que se acompaña con la no obligación de dar fundamentos de sus decisiones.
c) La sana crítica racional, al igual que la anterior no ata la acción de convencerse a la formalidad establecida en la prueba legal, pero a diferencia del anterior si debe fundamentar sus decisiones y esta debe haber sido fundada en hechos de la causa.

De acuerdo con Bes (2014), actualmente existen cuatro sistemas de valoración de prueba: la sana crítica, prueba tasada, libres convicciones o íntima convicción, y apreciación en conciencia. La diferencia sustancial entre estos procedimientos valorativos es la libertad del magistrado a la hora de adoptar una convicción que se exprese luego en sus fallos.

Si se toma la sana crítica, cabe consignar que la ley no impone normas generales para determinar los hechos ni determina en forma abstracta el valor de las pruebas, sino

que deja en libertad al juzgador el admitir todo tipo de prueba que estime útil al esclarecimiento de la verdad y para apreciarla conforme a las reglas de la lógica, la psicología, y la experiencia común. En contrapartida, en la prueba tasada no existe valoración alguna, ya que es dada por el legislador de manera anticipada. Un ejemplo de prueba tasada es la confesión expresa.

Por su parte, el sistema de libres convicciones supone un grado de convencimiento tal que impide todo tipo de dudas, aplicado primordialmente en los juicios por jurados populares, que sin estar condicionados por una formación jurídica previa desarrollan una actividad con predominante sentido moral. Por último, la apreciación en conciencia posibilita a los jueces seleccionar y jerarquizar los medios probatorios. Esto implica que en sus sentencias se les permita una libre selección de los elementos de prueba que consideran más contundentes, y tiene su fundamento en la oralidad del propio proceso, pues son los jueces quienes a través de sus sentidos experimentaron la producción de la prueba como protagonistas activos del litigio, jerarquizando a conciencia cada una de ellas.

En todo caso, ante una evidencia digital, los jueces deben estar preparados y actualizados, contar con los conocimientos suficientes para que, en la apreciación en conciencia, no descarten pruebas que pueden ser determinantes para la formación de su convicción. Sólo así el lector del fallo podrá comprender -que no es lo mismo que compartir- el razonamiento que lo condujo a adoptar la decisión tomada (Bes, 2014).

Ahora bien, tanto los correos electrónicos como los mensajes de texto (SMS) pueden conformar una evidencia digital, siendo complejo el proceso a través del cual se los puede llegar a admitir como prueba. El correo electrónico es un sistema que brinda el servicio de Internet, mediante el protocolo SMTP (Simple Mail Transfer Protocol o Protocolo Simple de Transferencia de Correo), el cual por extensión puede aplicarse a sistemas análogos que utilizan otras tecnologías. Por medio de mensajes de correo electrónico se puede enviar no sólo texto sino todo tipo de documentos o archivos digitales. Su eficiencia, conveniencia y bajo costo han acabado por reemplazar al correo tradicional para la mayoría de los usos y necesidades de comunicación.

En cuanto a su funcionamiento, las computadoras se conectan mediante una red, y obteniendo las aplicaciones necesarias de servidores de ficheros, se conectan a Internet mediante un router, usando servicios Web mediante el servidor y protegiéndose con diversos *firewalls*. Todo este armado es controlado desde la posición del administrador,

que es un actor privilegiado, ya que realiza el mantenimiento de toda la red. La consecuencia es que un ordenador cliente envía el correo electrónico desde su máquina y pasa al servidor, para enlazar, mediante el router, con la red de redes (Internet). El administrador es consciente, o puede ser consciente, del contenido de un correo en cualquier momento, aun cuando éste no haya sido enviado o se encuentre en el servidor. Y es quien tiene más facilidades -además de formación técnica- para que esto se produzca. Además, los correos enviados siempre dejan rastros, en forma de archivos l*ogs*, que se pueden hallar en las computadoras de los clientes y en el servidor. La intimidad aquí se ve severamente afectada, quedando sujeta a la voluntad del Administrador.

El uso del correo electrónico está ampliamente extendido, y se ha negado la autenticidad de los mismos presentados en impresiones a un juicio, por lo que no sirven como prueba directa, ya que el contenido, remitente, hora y fecha de un correo electrónico (*mail*) son modificables, siempre y cuando se cuente con los conocimientos y el equipamiento técnico adecuado. En todo caso, está fuera del alcance de quien desconoce todas las variables existentes sobre las cuales pueden hacerse posibles fraudes y maniobras que adulteren un correo electrónico. Sin embargo, complementado con otro tipo de prueba, puede llegar a ser valioso y tenido en consideración, una vez que la pericia informática lo da por válido.

En todo caso y circunstancia, si se pretende acreditarlo como prueba, el correo impreso debe ser sustentado por una prueba pericial que valide el contenido del mail, y prueba de informes a las distintas empresas prestatarias del servicio de correo Electrónico, que serán quienes puedan validar la cabecera (fechas de envío y recepción del mail). En estos casos, claramente los medios a los que deberá apelar el juez son la pericia informática, pero pedida como medida preliminar, ya que la información es fácilmente alterable, o aún más grave, suprimible de los registros por quien posea acceso a los servidores. Otra cuestión a tener en cuenta es si son casillas administradas desde una red interna, o por servicios de correo como Yahoo, Hotmail, Gmail, entre otros. La diferencia radica en la cantidad de información que se almacene y la vulnerabilidad de dichos sistemas (Bes, 2014).

El SMS refiere a los mensajes de texto que se envían por teléfono celular. Es hoy el medio más generalizado y comúnmente aceptado -por ejemplo, a través de WhatsApp-, y preocupa a los operadores del derecho la falta de jurisprudencia uniforme para tomarlos en cuenta como prueba.

3.2. Principios rectores de la Evidencia digital.

De acuerdo con la ISO/IEC 27037:2012[19] la evidencia digital es gobernada por tres principios fundamentales: la relevancia, la confiabilidad y la suficiencia. Estos tres elementos definen la formalidad de cualquier investigación basada en evidencia digital, bien ésta sea utilizada para que sea admisible en corte o no.

La relevancia es una condición técnicamente jurídica, que habla sobre aquellos elementos que son pertinentes a la situación que se analiza o investiga, con el fin de probar o no una hipótesis que se ha planteado alrededor de los hechos. Todo aquello que no cumpla con este requisito será irrelevante y excluido del material probatorio recabado para efectos del caso bajo estudio.

La confiabilidad es otra característica fundamental, que busca validar la característica de un proceso aplicado en cuanto a ser auditables y repetibles para obtener una evidencia digital, esto es, que la evidencia que se extrae u obtiene es lo que deber ser y que, si un tercero sigue el mismo proceso, deberá obtener resultados similares verificables y comprobables.

Finalmente, y no menos importante la suficiencia, la cual está relacionada con completitud de pruebas informáticas, es decir que, con las evidencias recolectadas y analizadas tenemos elementos suficientes para sustentar los hallazgos y verificar las afirmaciones efectuadas sobre la situación investigada. Este elemento está sujeto a la experiencia y formalidad del perito informático en el desarrollo de sus procedimientos y priorización de esfuerzos.

Si bien puede haber otros elementos que ayuden en el gobierno de la evidencia digital, ISO[20] ha determinado que estos tres, establecen las condiciones necesarias y suficientes para que los expertos en informática forense recaben, aseguren y preserven elementos materiales probatorios sobre medios digitales, los cuales podrán ser revisados y

[19] Guidelines for identification, collection, acquisition and preservation of digital evidence ISO/IEC 27037:2012. Es el primer estándar a nivel mundial para adquirir evidencias digitales.
[20] ISO (International Standarization Organization) es la entidad internacional encargada de favorecer normas de fabricación, comercio y comunicación en todo el mundo, brindando estándares internacionales

analizados por terceros interesados y sometidos a contradicción según ordenamiento jurídico donde se encuentren.

En este contexto, se detallan algunas preguntas (a manera de ejemplo) que pueden ser útiles para efectos de validar los tres principios enunciados:

Relevancia

• ¿La evidencia que se aporta vincula al sujeto con la escena del crimen y la víctima?
• ¿La evidencia prueba alguna hipótesis concreta que se tiene del caso en estudio?
• ¿La evidencia recolectada valida un indicio clave que permita esclarecer los hechos en estudio?

Confiabilidad

• ¿Los procedimientos efectuados sobre los dispositivos tecnológicos han sido previamente probados?
• ¿Se conoce la tasa de error de las herramientas forenses informáticas utilizadas?
• ¿Se han efectuado auditorias sobre la eficacia y eficiencia de los procedimientos y herramientas utilizadas para adelantar el análisis forense informático?

Suficiencia

• ¿Se ha priorizado toda la evidencia recolectada en el desarrollo del caso, basado en su apoyo a las situaciones que se deben probar?
• ¿Se han analizado todos los elementos informáticos identificados en la escena del crimen?
• ¿Se tiene certeza que no se ha eliminado o sobrescrito evidencia digital en los medios analizados?

3.3. Tipos de evidencia digital que puede ser recolectada y aportada a la investigación

En el año 2014, se presenta ante la Procuración General de la Nación, el instrumento desarrollado por el ministerio Publico Fiscal a cargo del Dr. H. Azzolin[21] y

[21] Fiscal encargado de la primera fiscalía especializada en Ciberdelitos del país.

aprobado por la Reunión Especializada de Ministerios Públicos del Mercosur (REMPM). Este instrumento se conoció como "Guía de obtención, preservación y tratamiento de evidencia digital[22]

A continuación, se detallará un listado de la evidencia digital no taxativa del tipo de evidencia que se puede aportar a una investigación que puede ser recolectada de los dispositivos de almacenamiento informático secuestrados, y que, dependiendo de cada delito en particular, merecerá un mayor análisis, a saber:

- Defraudaciones y estafas informáticas:

  - Información contable de acciones en línea
  - Software y documentos contables
  - Datos de tarjetas de crédito
  - Correos electrónico y notas varias
  - Registros financieros de activos, cheques y órdenes de pago
  - Libros de direcciones y calendarios

- Abuso infantil y pornografía:

  - Registros de chats y blogs[23]
  - Software de reproducción, captura y edición de video
  - Imágenes y videos de contenido sexual
  - Juegos infantiles o de contenido sexual
  - Directorios de archivos encriptados o no visibles mediante los cuales clasifica el contenido de las distintas víctimas
  - Correos electrónicos, notas y cartas varias.

- Acceso no autorizado a sistemas informáticos

  - Software específico (ej. programas autoejecutables, troyanos, registradores de teclas, etc.)
  - Software y códigos de programación

[22] PGN-0756-2016 Aprobada en marzo 2016.
[23] Blogs: Un blog o bitácora es un sitio web que incluye, a modo de diario personal de su autor o autores, contenidos de su interés, que suelen estar actualizados con frecuencia y a menudo son comentados por los lectores. Fuente: https://es.wikipedia.org/wiki/Blog.

- Registros de actividad en internet
- Archivos de texto y documentos con nombres de usuario y contraseñas
- Registro de sesiones de chat y blogs
- Listado de computadores a las cuales accedió
- Registro de direcciones IP (Internet Protocol).

- Copia ilegal de software:

- Registros de chat
- Correo electrónico
- Software específico (ej. generador de claves o códigos de activación; herramientas de cracking[24])
- Archivos de texto y documentos con números de serie y usuarios.

- Homicidios:

- Lista de direcciones
- Correo electrónico, cartas y notas varias
- Registros financieros
- Registro de actividad en internet
- Documentos legales y testamentos digitalizados
- Registros de chats
- Mapas
- Fotos y/o videos de la víctima

- Amenazas y/o acoso vía correo electrónico:

- Libros de direcciones
- Diarios íntimos
- Correos electrónicos, notas y cartas
- Registro de actividad en internet
- Registros telefónicos
- Investigación sobre el historial (background) de la víctima

[24] Herramientas de Cracking: Mientras que el hacking consiste en burlar los sistemas de seguridad para obtener acceso a los equipos informáticos (lo que puede ser bueno o malo), el cracking consiste en lo mismo, pero con intenciones delictivas. La opinión general es que los hackers construyen, mientras que los crackers destruyen. Fuente: https://www.avast.com/es-es/c-cracking.

- Mapas de las locaciones de las víctimas
- Imágenes, videos y/o cualquier tipo de registro de vigilancia
- Documentos legales

- Investigaciones referidas a estupefacientes:

  - Libros o Agendas de Direcciones
  - Correos electrónicos, notas y cartas
  - Calendarios
  - Bases de Datos
  - Prescripciones médicas
  - Documentos falsos para acreditar la identidad
  - Registros financieros
  - Registros de actividad en internet

- Fraude de telecomunicaciones:

  - Software específico de clonado y de programación de teléfonos celulares
  - Bases de datos de clientes
  - Números de serie electrónico
  - Números de identificación de celulares
  - Correos electrónicos, notas y cartas
  - Registros financieros
  - Registros de actividad en internet
  - Archivos extraídos de diversas tarjetas SIM

- Violencia doméstica:

  - Libros o agendas con direcciones
  - Diarios íntimos, entradas en Blogs personales o comentarios en redes sociales
  - Correos electrónicos, notas y cartas
  - Registros financieros
  - Registros telefónicos

3.4. Distintos mecanismos de Obtención de prueba

La prueba digital, de una naturaleza totalmente diversa a la prueba física, resulta al análisis de sus formas de producción, extremadamente volátil, sensible e intangible. Hay que destacar que la misma no consta en el dispositivo en que se almacena, sino que es autónoma de aquel. Su traducción se realiza por medio de una interfaz de lenguajes, como el código binario en principio, hasta que aparece representado como texto, imagen, o video, en las pantallas de los dispositivos digitales, los cuales emplean la electricidad para su almacenamiento y conducción.

Entendiendo esto, es posible advertir que la prueba digital requiere un tratamiento pericial de preservación, conservación y de protección de la cadena de custodia[25] especial. La volatilidad y sensibilidad que hacen a la integridad de la prueba digital torna indispensable el empleo de procedimientos no convencionales para su correcta conservación, que impliquen una capacitación especializada de los empleados, funcionarios, magistrados, auxiliares y demás operadores de la Justicia.

Un ejemplo claro de ello es que si bien el secuestro de un efecto físico, corpóreo, material o tangible, como un arma de fuego, no necesita de los mismos mecanismos de preservación para asegurar la cadena de custodia que los necesarios para la preservación de la prueba digital o intangible, contenida en un dispositivo electrónico, como un teléfono celular con información en su tarjeta de memoria (SIM). Mientras el arma puede ser preservada en una bolsa plástica dentro de una caja de seguridad del juzgado, el dispositivo electrónico debe resguardarse en una bolsa antiestática o de Faraday, a fin de que ningún sujeto pueda conectarse al mismo y borrar la información contenida en él, o bien realizar una descarga electroestática sobre aquel a fin de cometer el mismo objetivo.

[25] Cadena de Custodia: es el control que se efectúa tanto de las personas que recogen la evidencia como de cada persona o entidad que posteriormente tiene la custodia de la misma. La cadena de custodia debe contener un identificador unívoco de la evidencia, de las fechas en las que los artículos fueron recogidos o transferidos, datos sobre el responsable que realizó la recolección, datos sobre la persona que recibe la evidencia y los datos de las personas que acceden, el momento y la ubicación física, número del caso, y una breve descripción de cada elemento. El pasaje de la evidencia de un sitio a otro y las tareas realizadas, cualquier cambio inevitable potencial en evidencia digital será registrado con el nombre del responsable y la justificación de sus acciones. El objetivo de la cadena de custodia es garantizar la autenticidad de la evidencia que se utilizará como prueba dentro del proceso

Para esta tarea la de obtención de la evidencia digital nos remitimos nuevamente a la norma ISO/IEC 27037:2012[26] *Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence*, como anteriormente vimos establecía los principios rectores de la evidencia digital, también que establece una guía de cómo llevar a cabo la actuación pericial en el escenario de la obtención, identificación y secuestro de la evidencia digital. Esta norma está más enfocada en los avances tecnológicos y en sus dispositivos actuales, reemplazando las antiguas directrices de la RFC 3227:2002[27]. Dentro de las especificaciones del manejo de los datos en la obtención especifica puntualmente la importancia de la cadena de custodia donde este concepto no solo está ligado a la recolección de evidencia digital, sino que incumbe a todo proceso de obtención de evidencia en un proceso de investigación. Es un mecanismo que se utiliza para garantizar que la prueba no ha sufrido alguna alteración desde el momento de su recolección hasta su utilización en un proceso concreto. Debe incluir:

- Un identificador univoco de la evidencia.
- Quién, cuándo y dónde se accede a la evidencia.
- El pasaje de la evidencia de un sitio a otro y tareas realizadas.
- Todo cambio potencial en la evidencia digital debe registrarse con el nombre del responsable y la justificación de las acciones realizadas.

Otra de las consideraciones a tener en cuanta en el momento de la adquisición de la evidencia digital es no alterar el archivo de origen, es decir evitar al máximo su manipulación, y garantizar su autenticación para lo cual utilizaremos, los códigos Hash son mecanismos de detección de manipulaciones, modificaciones que afectan la integridad de los mensajes. Tiene como funciones primordiales la autenticación (permite corroborar la identidad de un archivo) y preservación de integridad de los datos (asegura que la información no haya sido alterada por personas no autorizadas u otro medio desconocido), resultando entonces de vital importancia a los fines de controlar la preservación de la cadena de custodia y evitar planteos de

[26] Fuente de datos: https://www.iso.org/standard/44381

[27] RFC 3227:2002: Guía Para Recolectar y Archivar Evidencia" (*Guidelines for Evidence Collection and Archiving*) [GuEvCo02], escrito en febrero de 2002 por Dominique Brezinski y Tom Killalea, ingenieros del Network Working Group. Es un documento que provee una guía de alto nivel para recolectar y archivar datos relacionados con intrusiones. Muestra las mejores prácticas para determinar la volatilidad de los datos, decidir que recolectar, desarrollar la recolección y determinar cómo almacenar y documentar los datos

El hash se define como la conversión de determinados datos en un número de longitud fijo no reversible, mediante la aplicación de una función matemática –algoritmo unidireccional. Calcular el hash de la copia forense permitirá verificar si la misma fue alterada con posterioridad a su obtención. Si pasado un tiempo de realizada la misma alguien plantea que fue alterada, bastará calcular el hash para ver si es el contenido es el mismo del originalmente obtenido (en este caso, se demuestra que la copia no fue manipulada).

Ya vimos antes algunos términos y aspectos técnicos de la obtención de evidencia digital.

Ahora podríamos dividir o establecer dos grupos al momento de la obtención de la evidencia, los cuales fueron claramente diferenciados por Delgado (2016), por un lado, el acceso a datos contenidos o producidos en dispositivos electrónicos (provistos por la parte interesada u obtenidas por parte de los operadores judiciales) y por otro lado el acceso a datos transmitidos en forma electrónica a través de las redes de comunicación (telefonía fija o móvil por ejemplo) o transmitida a través de la red de Internet (como por ejemplo acceso a contenidos de páginas web, obtención de datos sobre navegación web realizada por un individuo, obtención de información sobre los contenidos que una persona inserta en Internet).

Las diferentes formas de acceso a los datos en dispositivos electrónicos se detallan en el siguiente cuadro:

Acceso a datos en dispositivos electrónicos

A. Obtención de los datos por la parte interesada.	• Datos contenidos en el dispositivo propio. • Datos contenidos en dispositivo ajeno.
B. Obtención de datos por parte de operadores judiciales en la investigación de delitos.	• Registro de dispositivo aprehendido fuera de domicilio o en el propio domicilio. • Registro de información accesible en otros sistemas informático desde el mismo dispositivo.

	• Registro remoto mediante troyanos, malware (códigos maliciosos) o similar. • Registro transfronterizo.

Fuente: Diario La Ley, Nº 6, Sección Ciberderecho, 11 de abril de 2017, Editorial Wolters Kluwer

Como vemos en el cuadro, la obtención de datos, en algunos casos puede ser provista por la parte interesada y en otros casos puede ser obtenida por los operadores judiciales, en este último, es donde se presentan las novedades tecnológicas que traen consigo los puntos de discusión en cuanto a su validez y licitud, sobre todo en los caso de acceso sin el secuestro físico del dispositivo, como es el caso de los accesos remotos y el acceso transfronterizo, la utilización de software especial de acceso remoto, permite obtener los datos sin necesidad de tener que contacto físico con el almacenamiento de los datos. Estas nuevas tecnologías permiten interceptar y copiar en tiempo real contenidos recibidos o transmitidos comodatos de tráfico, contenido, geolocalización, así mismo acceder a datos archivados en el dispositivo a investigado sin tener ningún tipo de contacto con él. El otro punto novedoso, pero del que ya hablamos en el capítulo 1.4.1. es el de acceso trasfronterizo de datos y como dijimos se da cuando el dato al que necesitamos acceder se encuentran almacenados en un sistema informático o servidor situado fuera del territorio nacional.

3.4.1. Correo electrónico

Ante la ausencia de una regulación jurídica que establezca un proceso propio para la prueba digital, y en particular en lo que refiere a los correos electrónicos, es posible obtener dos tipos de preconstitución de la evidencia digital: física y electrónica. Para realizar ambas, es necesario recurrir a dos profesionales: un perito informático y un escribano público. Ambos deben estar presentes al momento de realizarse la preconstitución de la prueba. Los pasos para la preconstitución de prueba almacenada en un correo electrónico son los siguientes:

- El titular de la cuenta de correo electrónico accede a su cuenta en presencia de los dos profesionales.

- Se ubica la información pertinente requerida del correo electrónico.
- El perito informático realiza una captura de pantalla del correo electrónico pertinente, y la imprime.
- Las impresiones en papel deberán ser firmadas por el escribano público, para que éste otorgue fe pública de que el contenido es idéntico al que se visualiza en la pantalla. De esta manera se obtiene la Preconstitución Física de la evidencia digital.
- Luego, se debe exportar desde el correo electrónico el disco rígido de la PC.
- Se debe grabar en un disco DVD, no regrabable ni multifunción, el documento digital que tiene exportado el correo electrónico que se desea aportar como objeto de prueba.
- Por último, se debe aplicar dos códigos Hash, a los efectos de demostrar a futuro la inalterabilidad e integridad de la prueba digital. De esta manera, se obtendrá la Preconstitución Electrónica de la evidencia digital.

3.4.2. Imagen Digital

Las fotografías digitales brindan más datos e información que las imágenes plasmadas en ellas, lo cual se puede advertir ingresando a las propiedades del archivo, lo cual brinda acceso a los denominados metadatos (fecha, día y hora en que ha sido tomada la foto, dispositivo que se usó, si el documento fue alterado y la geolocalización de la imagen el día en que fue tomada). Es por ello que cuando más adelante se hace referencia a la imagen digital, se tendrán en cuenta estas características.

En cuanto a la preconstitución de la evidencia digital sobre imágenes digitales, es posible encontrar dos aspectos probatorios de acuerdo al instrumento resultante: la física y la electrónica. Para realizar este procedimiento, también se requiere de un perito informático y un escribano público:

- El titular de la PC debe acceder a su equipo, en presencia de los dos profesionales.
- El perito informático deberá imprimir en papel las imágenes digitales.
- Estas impresiones deberán ser firmadas por el escribano público, otorgando fe pública de que el contenido es idéntico al que se visualiza en la pantalla. Con esto se cumple la preconstitución física de la evidencia digital sobre imágenes digitales.

- Deberá grabarse en un disco DVD, no regrabable ni multifunción, la imagen o imágenes que se consideran pertinentes como evidencia.
- Por último, se aplican dos códigos Hash, a los efectos de demostrar a futuro la inalterabilidad e integridad de la prueba digital. De esta manera, se obtendrá la Preconstitución Electrónica de la evidencia digital.

3.4.3. Evidencia en la nube[28]

Según Koops & Goodwin (2014), este tipo de tecnología es un modelo de servicios en el cual los datos de un sistema informático se almacenan, administran y respaldan en forma remota en este caso servidores que están en la nube y que son administrados por un proveedor de servicios dentro de los más utilizados podemos mencionar Amazon Cloud, Box, Dropbox, Google Drive, OneDive, ICloud entre otros. Este tipo de evidencia es uno de los que presenta mayores controversias en principio presenta dos obstáculos importantes: por un lado, la información se puede ser alojada en un datacenter (servidor) que está fuera del territorio de la Nación y, por otro lado, conocer con precisión su geolocalización no resulta fácil, ya que el propio sistema no establece esa información a los usuarios. Al igual que los demás casos, para llevar adelante este procedimiento se requiere la presencia de un perito informático y un escribano.

La nube refuerza los desafíos existentes para la recopilación de evidencia digital en la investigación criminal, que requiere no solo una acción rápida debido a la vulnerabilidad de la pérdida de datos, sino también las capacidades para el acceso remoto de datos. Un desafío particular es que tal recolección remota de evidencia se extiende rápidamente más allá de las fronteras nacionales. Koops & Goodwin (2014)

[28] Nube: del inglés cloud computing, es un paradigma que permite ofrecer servicios de computación a través de Internet. En este tipo de computación todo lo que puede ofrecer un sistema informático se ofrece como servicio de modo que los usuarios puedan acceder a los servicios disponibles "en la nube de Internet, siendo un paradigma en el que la información se almacena de manera permanente en servidores de Internet. Fuente: Guía integral de empleo de la informática forense en el proceso penal. Infolab “Defending a New Domain” en www.foreignaffaires.com/articles/66552/willian-j-lynn-iii/defending-a-new-domain

3.4.4. Celulares inteligentes (smartphones)

En el caso de los smartphones, dispositivos móviles inteligentes muy populares que tiene además de las funciones básicas de los teléfonos convencionales (mensajes de texto, llamadas, agenda de contactos, fotos, etc.) sino que además tiene las funciones y capacidad de una computadora portátil y portable que además tiene procesador de texto, planillas de cálculo , sistema operativo (Android, IOS, Windows, etc.) y sumado a esta la constate evolución de las aplicaciones conocidas como APP[29] suma más oportunidades en la búsqueda de datos en una investigación , contraseña, datos de navegación, viajes cuentas bancarias y datos de geolocalización entre otros, también se requiere la presencia del perito informático y el escribano público. El procedimiento a realizar es el siguiente:

- Fotografiar el celular en presencia del escribano público, y que éste firme las fotografías fechándolas, a fin de dar fe de que ese es el celular del cual se va a extraer información.
- Filmar desde el inicio y hasta que culmine la descarga, todo el procedimiento.
- El perito deberá conectar el teléfono a una computadora mediante un cable USB.
- Cuando ambos dispositivos se encuentren compatibilizados y sincronizados, se debe acceder a todas las carpetas y copiar la información pertinente de cada una de ellas, desde el ordenador.
- En caso de que la información pertinente sea una imagen, un mensaje, o una conversación, se puede realizar una captura de pantalla sobre ella.
- Se debe grabar en un disco DVD, no regrabable ni multifunción, la información pertinente que se desea aportar como objeto de prueba.
- Por último, se aplican dos códigos Hash, a los efectos de demostrar a futuro la inalterabilidad e integridad de la prueba digital.
- Una vez culminado el procedimiento, la grabación del mismo debe ser firmada por el escribano público, quien debe labrar un acta de procedimiento de preconstitución de prueba.

[29] App: son aplicaciones informáticas diseñada para ser ejecutada en teléfonos inteligentes, tabletas y otros dispositivos móviles. Ejemplo: deportivas runtastic, app de bancos, de viajes Despegar, idiomas duilongo, entre muchas más. Fuente: https://es.wikipedia.org/wiki/Aplicaci%C3%B3n_m%C3%B3vil

En este punto en el año 2013 el Poder Judicial de la Provincia de Neuquén aprobó una norma reglamentaria denominada Protocolo para Pericias Informáticas sobre Telefonía Celular (Gómez, 2013) en la que se expresa que este tipo de pericias en lo que refiere a la extracción de la evidencia digital debe ser practicada por un profesional informático. Con lo cual se mantiene el criterio de separación de las actividades de identificación y preservación que puedan realizarse en el lugar del hecho de aquellas otras que involucran la extracción y el análisis de evidencia digital y la presentación de informes, quedando estas últimas a cargo en forma excluyente de profesionales con titulación en ciencias informáticas y que ejerzan como peritos informáticos o su equivalente con el rol de DES[30] que define el estándar internacional. Esta clasificación la veremos más adelante al analizar la norma ISO-27037-2012.

3.4.5. Red Social

En la contemporaneidad, gran parte de la interacción social diaria, tanto en jóvenes como en no tan jóvenes, pasa por las redes sociales (tales como Facebook, MySpace, Sonico, Linkedin, Instagram, Twitter etc.). Es por ello que la preconstitución de prueba digital sobre las redes sociales es tan importante. Un obstáculo importante que presenta este proceso, es que no resulta posible conocer en qué servidores o Data Center se encuentra almacenada la información que uno considera pertinente para producirla como evidencia, algo muy similar a lo que pasa con la computación de la nube. Debido a lo cual, al realizarse la preconstitución en tiempo real y en vivo, se suele filmar el procedimiento. Al igual que en todos los demás casos, es requisito la presencia del escribano público y del perito informático. Y al igual que en los otros casos, se debe presentar tanto la preconstitución física como electrónica de la evidencia digital. A continuación, se describe el procedimiento:

- Primero, se filma desde el inicio y hasta que culmine la descarga, todo el procedimiento.
- Es necesario que el titular de la cuenta de red social de la cual se requiera la información acceda a ella en presencia de ambos profesionales.

[30] DES: siglas en ingles Digital Evidence Specialist más conocido como perito informático.

- Posteriormente, el perito deberá imprimir en papel distintas capturas de pantalla de la red social, plasmando en ellas los datos que se quieran utilizar como evidencia.
- Las impresiones en papel deberán ser firmadas por el escribano público, otorgando fe pública de que el contenido es el mismo que se visualiza en la pantalla. Cumplida con esta parte del procedimiento, ya se obtiene la preconstitución física de la evidencia digital.
- Por otro lado, las capturas de pantalla deberán ser emigradas por el perito al disco rígido de la PC.
- Con posterioridad, se deberá grabar en un disco DVD, no regrabable ni multifunción, las capturas guardadas en el disco rígido.
- Luego, se le aplicarán dos códigos Hash a los efectos de demostrar a futuro la inalterabilidad e integridad de la prueba digital. De esta manera, se tendrá por cumplida la Preconstitución Electrónica de la evidencia digital.
- Por último, la grabación será firmada por el escribano público, y el mismo deberá labrar un acta del procedimiento de preconstitución de prueba, indicando el día, mes, año, la hora de inicio y de culminación del proceso.

En cuanto a las redes sociales se están realizando varias acciones sobre fuentes abiertas OSINT es un acrónimo de Open Source Inteligence o inteligencia de las fuentes abiertas es un término empleado originalmente por la fuerzas militares y que ahora se extendieron a las investigaciones judiciales, que utiliza una serie de herramientas para hacer un rastreo de los datos disponibles, abiertos y descalificados, en este caso las redes sociales son una fuente muy importante de obtención de información debido a ello, ha surgido una nueva disciplina denominada SOCMINT[31] (Social Media Intelligence), cuyo objetivo, en teoría, es proporcionar inteligencia, basada en la información obtenida de esas redes sociales.

[31] El juez Lijo procesó a una mujer por amenazar a Mauricio Macri y a su familia", Centro de Información Judicial, 23 de mayo de 2016, disponible en: http://cij.gov.ar/nota-21585-El-juez-Lijo-proces–a-una-mujer-por-amenazar-aMauricio-Macri-y-a-su-familia.html

3.5. Allanamientos y requisas y secuestros– Doctrina de la Plain View

En la mayoría de los códigos procesales en mayor o menor medida están definidos las medidas coercitivas que regulan, por ejemplo, la intercepción de correspondencia, la intervención de comunicaciones y los puntos que necesitamos definir que son el allanamiento y las requisas.

A saber, el Código Procesal Penal de la Nación el allanamiento, cuando hubiere motivo para presumir que en determinado lugar existen cosas vinculadas a la investigación del delito, disponiendo que en eso casos el Juez ordene por auto fundado el registro de dicho lugar. (Artículo 224). También prevé que, en caso de urgencia, cuando medie delegación de la diligencia, la comunicación de la orden puede transmitirse por medios electrónicos.

El código procesal de la Provincia de Neuquén (Ley N° 2784 Año 2011), incluye en su ordenamiento el registro y secuestro de datos ubicados en equipos informáticos o medios de almacenamientos, como así también establece la posibilidad de registro remoto.

También podemos mencionar un proyecto de ley de la Provincia de Mendoza que tiene como fin incorporar a su ordenamiento procesal (Ley N° 6730 Año 1999) un articulado que regula el procedimiento de obtención e incorporación al proceso penal de la prueba digital. Que entre otras disposiciones establece una diferencia entre el allanamiento físico de un allanamiento digital definiéndolo "…Cuando el registro debe efectuarse en cualquier dispositivo electrónico la orden será dictada, a solicitud del fiscal interviniente o del funcionario en quien éste delegue la misma, por auto fundado de juez competente bajo pena de nulidad, siempre que haya motivos suficientes para presumir que una persona posee en los dispositivos electrónicos elementos relacionados con un delito…"

Con la ley N° 27.063 del nuevo CPPN incorpora dos artículos, el Art. 143 en donde especifica o habilita la intercepción y secuestro de correspondencia o cualquier medio de comunicación electrónica. En sintonía tenemos el Art. 144 que establece la incautación de datos de un sistema informático o de una parte de éste, o de un medio de almacenamiento de datos informáticos o electrónicos, con el objeto de secuestrar los componentes del sistema, obtener copia o preservar datos o elementos de interés para la investigación.

En general en nuestro ordenamiento estable que si en estricto cumplimiento de la orden de allanamiento, se encontrare evidencia de la comisión de un delito distinto al que motivó la orden, procederá a su inmediata comunicación al fiscal interviniente, siempre y cuando estemos hablado de encuentros casuales o fortuitos estaríamos dentro de lo que se conoce como la doctrina de la Plain View, que tiene si génesis en la jurisprudencia de Estados Unidos Harris v. United States" (390 US 234 -1968). En nuestro ordenamiento se introdujo la modificación ley 25.434 (2001) que agregó un tercer párrafo en el Art. 224 del C.P.P, validando los encuentros fortuitos.

De acuerdo con Petrone (2014) esta extensión en la búsqueda, no puede aplicarse al ámbito de la evidencia digital, por la misma naturaleza del dato difícilmente se puedan encontrar o apreciar el dato en forma casual sin la revisión de todos los datos del sospechoso. Así mismo declara imposible actuar en forma análoga ante un documento físico y digitales.

Ello porque, a diferencia de lo que ocurre con la evidencia material, los datos digitales almacenados en un dispositivo no son observables por los sentidos: su apreciación requiere que los códigos que componen los datos sean traducidos por un programa o interface. Los datos almacenados no son otra cosa que códigos que se revelan luego con la forma de un documento o una imagen, recién luego de ser ejecutados por la interface que las interpreta. Esta es la razón por la cual, quien ejecuta una orden no puede "observar a simple vista" directamente la evidencia digital; ésta no puede ser apreciada sino mediante la utilización de medios tecnológicos.

3.6. Analisis sobre la evidencia digital -Pericia judicial – Rol del experto

Una vez presentada la evidencia de acuerdo a los correctos procedimientos de preconstitución, los auxiliares de la justicia deben realizar las pericias sobre la prueba presentada.

En este punto volvemos a la norma ISO-27037-2012[32] que establece lineamientos generales para el trabajo de campo de los expertos, el mismo es de carácter facultativo no obligatorio, recomendable como una buena práctica seguirlas. Entre ellas es la de realizar la pericia en dos etapas y por áreas diferentes para lograr mayor objetividad.

El protocolo especifica que el primer contacto con la escena este a cargo de DEFR (Digital Evidence First Responder) reconociendo para esta tarea al personal de las fuerzas de seguridad, judicial u organización similar, siendo este primer contacto crítico, ya que una incorrecta recolección de la evidencia podría generar vicios de nulidad.

Como ya vimos anteriormente luego de recolectada la evidencia , es trasladada generalmente a un laboratorio para ser analizada que sería nuestra segunda etapa y en este punto la experticia e idoneidad profesional encargado del análisis forense debe ser comprobable según el art. 254 CPP[33] y la norma 270034:2012 establece la figura del especialista denominado DES (Digital Evidence Specialist) más conocido como el perito informático.

Determinadas los roles encargados de la actividades de recolección y análisis y teniendo en cuenta las características propias de la evidencia es muy importante que el almacenamiento de la evidencia, una vez recibida, se haga en bolsas de Faraday[34] o bolsa antiestática precintada. Esto se realiza de este modo para evitar cualquier tipo de afección al dispositivo electrónico. Las pericias deben realizarse en recintos seguros, especialmente acondicionados para pruebas sobre dispositivos digitales o electrónicos, pudiendo realizarse el peritaje tanto para el hardware como del software. Los recintos deben contar con equipos autónomos de energía ante posibles interrupciones del servicio eléctrico. La sala en la que se llevará adelante la pericia debe constituir una jaula de

[32] ISO-27037-2012: Guidelines for identification, collection, acquisition and preservation of digital evidence. Procedimiento de actuación pericial.

[33] Código Procesal Penal Nacional. Artículo 254. Concepto
La formalización de la investigación preparatoria es el acto por el cual el representante del MINISTERIO PÚBLICO FISCAL comunica en audiencia al imputado, en presencia del juez, el hecho que se le atribuye, su calificación jurídica, su grado de participación y los elementos de prueba con que cuenta.
A partir de este momento comenzará a correr el plazo de duración del proceso.
Lea más: http://leyes-ar.com/codigo_procesal_penal/254.htm

[34] Bolsa Faraday: estas bolsas están especialmente diseñadas para la recolección, preservación, transporte y análisis de dispositivos móviles e inalámbricos. Bloquean toda señal celular, WIFI o de radio. Fuente: https://www.division-forense.com/bolsa-faraday.html

Faraday[35], a los efectos de evitar posibles ciberataques o ataques electrónicos, los cuales pueden tener diversas formas, como:

- Un virus.
- Malware (códigos maliciosos).
- Conexiones remotas no autorizadas vía Wifi o Bluetooth.
- Ataques de electroestática.

Por otro lado, el perito encargado de realizar la pericia debe emplear una indumentaria adecuada a la misma, debido a que muchos componentes de los dispositivos electrónicos son sensibles al empleo de bajo voltaje. Dicha indumentaria estará compuesta por guantes de látex antiestático y brazalete o pulsera antiestática de descarga a tierra. Los mismos cumplen la función de evitar la afectación mediante descargas involuntarias de los dispositivos electrónicos en donde se almacena la información.

Con todo el condicionamiento necesario, el siguiente paso a seguir por parte del perito judicial, es comenzar a usar el dispositivo. El primer acto de estas pericias digitales es realizar una copia forense de la información contenida en el dispositivo electrónico. En la mayoría de las provincias (Piccirilli, 2013), los peritos cuentan actualmente con duplicadores forenses, los cuales permiten justamente cumplir con esta copia, sin alterar el disco de origen, con una modalidad en que no sólo graban el espacio utilizado por el dispositivo, sino también el vacío, a fin de recuperar información de aquellas zonas que han sido formateadas o borradas. Este tipo de copia se denomina Bit a Bit, y permite mantener la integridad de la evidencia y la cadena de custodia que requiere. Una vez realizada la copia, el mismo software forense suelen tener herramientas para ayudar a los peritos a encontrar la información pertinente que se busque como evidencia. Para ello, basta la simple introducción de datos sobre la búsqueda para que los algoritmos del sistema busquen todo aquello que resulte relevante. Así se tiene por cumplida la pericia.

Conclusiones parciales

Se está avanzando en todo lo relacionado con la tecnología informática, se encuentran más recomendaciones relacionadas con el tratamiento la evidencia digital, como el

[35] Jaula de Faraday: Se conoce como jaula de Faraday al efecto por el cual el campo electromagnético en el interior de un conductor en equilibrio es nulo, anulando el efecto de los campos externos. Fuente: https://es.wikipedia.org/wiki/Jaula_de_Faraday.

protocolo de procedimientos para evidencias en teléfonos celulares, pero siguen siendo insuficientes, por ejemplo, en la obtención de evidencias en las fuentes abiertas, hoy se pueden obtener más datos que en una investigación física y no está regulado.

La investigación de los delitos y preconstitución de la evidencia digital requiere de conocimientos específicos además requiere de capacitaciones de los operadores y constate actualización. Los expertos deben reconocer y ser conscientes que una correcta utilización de las buenas prácticas que nos guían como peritos o sin el respaldo legal que englobe todas estas acciones, se puede dar lugar a que se cometan errores que vicien de nulidad algo que a posteriori puede ser utilizado como prueba.

Capítulo 4. La evidencia digital en los procesos provinciales

Introducción

La Argentina posee 24 códigos procesales unos por cada provincia y otro por la ciudad Autónoma de Buenos Aires, es decir jurisdicción cada provincia y dicta sus propios códigos procedimentales.

Seguidamente daremos una breve introducción sobre los códigos más avanzados en materia de evidencia digital.

4.1. Ciudad Autónoma de Buenos Aires

En lo que respecta a la CABA, el Código Procesal Penal (ley 2303/17) no hace mención alguna a la evidencia digital, ni habilita ningún medio electrónico probatorio. Sin embargo, el Reglamento General de Organización y Funcionamiento del Poder Judicial de la Ciudad dedica, en el artículo 1.12, que regula el armado de expedientes judiciales, en particular en el 1.12.3, que trata la incorporación "… *del expediente digital u otra modalidad de registración fehaciente que los desarrollos informáticos y telemáticos en curso pongan a disposición del servicio de justicia."* Para ello, la norma faculta a los jueces a *"...otorgar validez y eficacia equivalente al documento en soporte papel a otros documentos que contengan textos, imágenes, o sonido, almacenados o transmitidos por medios electrónicos, informáticos, magnéticos, ópticos, telemáticos o producidos por nuevas tecnologías, aun los que contengan actos o resoluciones judiciales…".* No obstante, esta capacidad, limita la aplicación de esta disposición, a la condición de que "…*siempre…sea posible garantizar su autenticidad, integridad y seguridad, aunque no se impriman en papel ni sean firmados."*

De esta manera, esta moderna norma introduce la posibilidad de incorporar documentos electrónicos al expediente, y a su vez impone a los magistrados la carga de garantizar la autenticidad, integridad y seguridad de los mismos.

A su vez, el art. 1.12.3.1. establece la posibilidad de que los miembros del poder judicial (magistrados, funcionarios judiciales y miembros del Ministerio Público Fiscal) se remitan entre sí documentos electrónicos, y que puedan tomar declaraciones

testimoniales mediante videoconferencias u otra "tecnología similar", lo cual abre las posibilidades a otros mecanismos parecidos. Seguidamente, el art.1.12.3.2. habilita a las partes a utilizar esos medios para presentar sus peticiones a los tribunales, con el condicionamiento de que presenten el documento original en soporte papel. Por último, las dos disposiciones finales expresan, la facultad de las partes de "…*emplear como auxilio recursos tecnológicos que permitan proyectar imágenes, sonidos o texto…"* cuando el proceso establezca que se expresen oralmente, y la promoción, en la medida que los recursos lo permitan, del acceso público a la información referida a la tramitación de expedientes, mediante medios informáticos, telemáticos o producidos por nuevas tecnologías.

Resumiendo, podemos afirmar que esta disposición admite que la totalidad de los juicios se instrumenten en formato digital, la producción de prueba en dicho formato y el acceso público a la información. Asimismo, admite las comunicaciones entre magistrados por medios telemáticos, y el uso de video conferencias para recibir declaraciones o testimonios. En los juicios orales, habilita el uso de herramientas tecnológicas para producir imágenes, sonidos o texto. Sin embargo, hay que destacar que este sistema, con todos estos avances, hasta el momento no se ha puesto en funcionamiento.

4.2. Provincia de Entre Ríos

El Código Procesal Penal de la provincia de Entre Ríos hace un reconocimiento expreso de algunos medios de prueba electrónicos. Entre ellos se encuentran los casos de los reconocimientos de imágenes y de voz, siendo este último el establecido en el art. 326, que consiste en un mecanismo en el cual el imputado debe brindar una grabación de su voz, a fin de que la misma, con el contraste de otras dos voces similares o más, a fin de que el reconociente indique cuál es la reconocida. Mientras el primero, regulado en el 325, consiste en habilitar cuando sea necesario identificar o reconocer a una persona que no pudiese estar presente, su identificación mediante imágenes fotográficas o fílmicas, si hubiese disponibles.

Por otro lado, en los arts. 297 a 302 se regula la declaración testimonial filmada. El primero dispone que en la medida en que el juez o el fiscal lo encuentren conveniente, por las características del testigo o sus circunstancias, podrán disponer que su declaración se registre fílmicamente. El art. 298 establece las formalidades a la que estará sujeta dicha

declaración, destacándose de ella que el acto debe ser filmado íntegramente sin interrupciones, captando también a la persona que hace las preguntas, y que deberán tomarse las medidas pertinentes para asegurar la conservación de la genuinidad del soporte de la filmación, la cual también deberá transcribirse por escrito y agregarse al expediente (art. 299). Seguidamente, el art. 300 habilita la disposición de filmar otros actos procesales, en caso de que haya circunstancias especiales que lo justifiquen, y tomando los mismos recaudos del 298, lo cual ya dispone un principio general de permitir filmar los actos procesales. El art. 301, por su parte, otorga a las partes la facultad de peticionar al Fiscal la filmación de las medidas probatorias que se practiquen, siempre y cuando aporten los medios conducentes. Finalmente, el art. 302 regula la "Testimonial especial filmada", que procede cuando *"…las víctimas deban ser resguardadas por las características de los hechos a investigar…"*, para la cual se establecen las mismas formas previstas en el art. 298, con algunas adiciones:

- El espacio físico en el que debe llevarse a cabo debe ser: "*…una sala que deberá estar vinculada a otra mediante un espejo que permitirá sólo la visión de los que están en esa. Ambas dependencias deberán estar interrelacionadas con elementos de audio y la primera con elementos adecuados para realizar una correcta filmación de lo que allí suceda*".

- Deberá estar presente solo el Fiscal o persona designada por aquel, la cual debe estar: *"…munida de auriculares o audífonos que posibiliten que quienes están en la otra sala se comuniquen solo con ella…".*

- La participación o presencia de peritos que podrán interrogar luego a las partes.

4.3. Provincia de Chubut

Por su parte, el Código Procesal Penal de la provincia de Chubut, prevé en su art. 326 la reproducción de grabaciones y elementos de prueba audiovisuales en la audiencia de juicio. El sistema jurídico de esta provincia también admite el expediente electrónico, la presentación y producción de prueba mediante evidencia digital, y las comunicaciones y notificaciones electrónicas.

Por otro lado, el art. 165 complementa el principio de libertad probatoria, estableciendo que: *"Podrán probarse los hechos y circunstancias de interés para la solución correcta del caso, por cualquier medio de prueba, salvo prohibición expresa de*

la ley. Además de los medios de prueba establecidos en este Código, se podrán utilizar otros siempre que no vulneren garantías constitucionales y no obstaculicen el control de la prueba por los demás intervinientes."

Conclusiones parciales

Siendo la evidencia digital un recurso tan fundamental para acercar a los procesos judiciales a la realidad diaria, resulta lógico que la misma sea necesaria también para la eficacia probatoria en las distintas normas procesales provinciales. Siendo la característica fundamental de este fenómeno el hecho de que trasciende distintos aspectos de la sociedad, y habiendo llegado a la conclusión los distintos Estados parte de la Convención de Budapest de que resultaba necesario realizar una solución integral y completa al problema, resulta evidente que debería existir al menos una regulación general en común para todas las provincias. Sin embargo, la regulación no es la misma para el Código Procesal Penal de la Nación que las previstas para las distintas provincias.

Pese a la carencia de una normativa orgánica a nivel nacional que aborde una regulación uniforme para todas las provincias en lo que respecta a la incorporación de la evidencia electrónica o digital, podemos encontrar algunas normas provinciales de carácter procesal en el campo penal que regulen al respecto, dentro de los 24 códigos procesales penales. Algunos pocos códigos procesales admiten explícitamente el uso de medios de prueba electrónicos. También reconocen la posibilidad de realizar notificaciones, comunicaciones y exhortos en formato electrónico.

En materia procesal penal, en Córdoba, el CPP no regula específicamente sobre la evidencia digital, aunque alguna de sus normas admite el uso de medios digitales para determinadas circunstancias. El principio de libertad probatoria en la investigación penal Art. 192 del CPP admite la posibilidad de su utilización salvo prohibición expresa por la ley y en los casos de exclusión probatoria (Art. 194 CPP). En este supuesto tanto el Fiscal a cargo de la investigación como el Juez tiene permitido la ponderación de otros medios de prueba no contemplados específicamente en la normativa que tratamos, posee la

facultad de admitir, ordenar, valorar e interpretar distintos elementos a fin de lograr su convicción sobre los hechos alegados por las partes

Conclusiones finales

Se hace cada visible que la Evidencia Digital implica un proceso complejo en todo sentido, al punto que no se logra tener una definición acabada de lo que implica, ni una definición especifica. Se debe cambiar la mirada tradicional y entender que la evidencia digital requiere de medios de prueba específicos diferentes de los pensados para las evidencias físicas, la evidencia digital deber ser manejada conforme a procedimientos legales regulados, para asegurar que su obtención esté debidamente documentada, preservada y disponible para su utilización y revisión. Y por supuesto en este proceso de incorporación de las evidencias digitales se hace imperiosa la utilización de expertos, capacitados, para garantizar que la misma se ha realizado con cierta experticia, respetando las buenas prácticas y garantías constitucionales.

En nuestro país como vemos se está avanzando en todo lo relacionado con la tecnología informática, la obtención de evidencias desde fuentes abiertas, o desde la nube. Pero en la medida que las mismas no tengan una regulación es difícil usarlas como medios de pruebas. Se encuentran varias recomendaciones relacionadas con el tratamiento la evidencia digital, generales y específicas como el protocolo de procedimientos para evidencias en teléfonos celulares, la, pero siguen siendo insuficientes, y solo es una recopilación de buenas prácticas, sin fuerza legal. La modificación del CPPN, no trajo mejoras el manejo de la evidencia digital, pero si presenta un escenario más completo para los delitos tecnológicos. Lo esperable sería que, en función de esta modificación en el sistema penal, tenga si correlación en los sistemas procedimentales. A la vez que se logre una mayor unificación a nivel provincial.

La investigación de los delitos y preconstitución de la evidencia digital requiere de conocimientos específicos además requiere de capacitaciones de los operadores y constate actualización. Los expertos deben reconocer y ser conscientes que una correcta utilización de las buenas prácticas que nos guían como peritos o sin el respaldo legal que englobe todas estas acciones, se puede dar lugar a que se cometan errores que vicien de nulidad algo que a posteriori puede ser utilizado como prueba.

Partiendo desde mi hipótesis tentativa, *que la obtención e incorporación de evidencia digital como prueba en juicio, requiere su validación por peritos informáticos, garantizando que la misma, se obtuvo sin violar el derecho a la privacidad e intimidad de las personas;* y por todo lo expuesto a lo largo de este trabajo, la misma se confirma.

En cuanto a la propuesta de mejora, como siempre la capacitación debería estar en primer lugar, la capacitación en todos los ámbitos operadores judiciales e incluir a nivel curricular la evidencia digital como materia especifica. Hoy se presentan problemas en conseguir gente capacitada en las distintas áreas de forensia. La titulación no tiene carrera universitaria, lo que muestra una veta para poder avanzar y ser pioneros en esta área, construir laboratorios para el tratamiento, exploración y almacenaje de las evidencias digitales, en otros países la Universidades son referentes o consultores obligados, en nuestro país se está empezando a capacitar a las fuerzas policiales y ya tiene equipos especializados, para dar las primeras respuestas, en los lugares del delito, pero el tratamiento posterior es derivado, creo que este sería el punto en donde generar experticia en el manejo de equipos específicos.

El estado necesita estar a la altura de los retos que vienen de la mano de esta revolución digital (inteligencia artificial, biotecnología, nanotecnología, robótica). Este profundo cambio vino para quedarse e impactar en forma constante en todos los ámbitos privados y públicos, en este último surge la creciente necesidad de adaptarse en el marco institucional para integrarse y funcionar.

Parafraseando a un profesor… *"la tecnología, de por sí, no transforma la justicia, pues es el factor humano el que propondrá un sentido (al litigar) y valorará (al juzgar) esta clase de pruebas"*. Nos queda mucho camino por descubrir todavía en materia de prueba digital, pero cada vez somos más conscientes de su importancia.

Referencias bibliográficas

Bruzzone, G. y Bertolino, P. (Comps.) (2005). *Estudios en homenaje al Dr. Francisco J. D'Albora*. Buenos Aires: Ed. Abeledo Perrot.

Bruzzone, G, (2000). *La Nulla Coactio Sine Lege como pauta de trabajo en materia de medidas de coerción en el proceso penal*. Buenos Aires: Di Plácido.

Cafferata Nores, J (1998). *La prueba en el proceso penal*. Buenos Aires: Depalma.

Cafferata Nores, J., Montero, J., Vélez, V., Ferrer, C., Novillo Corvalán, M., Balcarce, F.; Hairabedián, M., Frascaroli, M., Arocena, G. (2012). *Manual de derecho procesal penal.* (3ª edición actualizada). Córdoba: Advocatus.

Cafferata Nores, J. y Arocena, J. (2001). *Temas de derecho procesal penal (Contemporáneos).* Córdoba: Mediterránea.

Cario, A (1994). *Garantías constitucionales en el proceso penal.* Buenos Aires: Hammurabi.

Casey, E. (2011). *Digital Evidence and Computer Crime*. London: Academic Press.

Consejo de Europa, Data Protection and Cybercrime Division (2013). *Guía de Prueba Electrónica. Guía básica para Fuerzas y Cuerpos de Seguridad, Jueces y Fiscales*, Estrasburgo, Francia.

Delgado Martín, J (2016). *Investigación tecnológica y prueba digital en todas las jurisdicciones*. Madrid: La Ley.

Diaz Cantón, F (2010). La relación entre la Prueba y la Coerción Penal. *Revista de Derecho Procesal Penal, 2006 1*, 1-15.

Garibaldi, G (2010). *Las Modernas Tecnologías de Control y de Investigación del Delito.*

Buenos Aires: Ad. Hoc.

Ferreyra de la Rua, A y Gonzalez de la Vega, C. (2011). (4ta ed.). *Código de Procedimiento Civil y Comercial de la Provincia de Córdoba.* Córdoba: La ley

Koops, B & Goodwin, M (2014). *Cyberspace, the cloud, and cross-border criminal investigation.* Tilburg: The Netherlands. Universidad de Tilburg. TILT - Instituto de Derecho, Tecnología y Sociedad de Tilburg.

Lloveras de Resk (1992*). Los Documentos Electrónicos: Concepto y valor probatorio.* Córdoba: Advocatus.

Palazzi, P. (2009). *Los delitos informáticos en el Código Penal. Análisis de la Ley 26.388*. Buenos Aires: Abeledo Perrot.

Sueiro, C.C. (2015). *Criminalidad informática: la eficacia político-criminal de la reforma al Código Penal en materia de delitos informáticos.* Buenos Aires: Ad-Hoc.

Sueiro, C.C. (2016). *La prueba digital en la criminalidad informática*. Buenos Aires: Facultad de Derecho (UBA), Departamento Penal.

Maier, J (2004). *Derecho Procesal Penal. I. Fundamentos.* (2da. Ed.). Editorial; Buenos Aires: Del Puerto.

Maier, J. (2011). *Derecho Procesal Penal. III. Actos Procesales*. Editores; Buenos Aires: Del Puerto.

Petrone, D (2014). *Prueba Informática*. Buenos Aires: Didot.

Ponencias

Rivolta, M (2007, agosto). *Medios de prueba Electrónicos: Estado de avance en la legislación argentina.* Ponencia presentada en el IV Congreso Argentino de

Administración Pública, organizado por Cuerpo de Administradores Gubernamentales – Jefatura de Gabinete de Ministros. Buenos Aires, Argentina.

Delgado Martín, J., Agustinoy Guilayn, A., Lopez Gutierrez, J. (2017, abril). *La Prueba Digital*. Ponencia presentada en el II Congreso de la Abogacía madrileña. Madrid, España.

Bes, E. (2017, noviembre). *Prueba digital y su inclusión en el procedimiento laboral*. Ponencia presentada en el VI Congreso de Derecho Laboral y Relaciones del Trabajo – XII Congreso Nacional de la SADL, VIII Congreso Internacional de ARTRA-, organizado por la Sociedad Argentina de Derecho Laboral (SADL), la Maestría en Derecho del Trabajo y Relaciones Laborales Internacionales de la Universidad Nacional de Tres de Febrero (UNTREF) y la Asociación de Relaciones del Trabajo de la República Argentina (ARTRA). Mar del Plata, Argentina.

Aciarri, H., Alvarez, H., Bouhadana, I., Cevasco, J., Corvalán, D., Del Campo, A., Dupuy, D., Gilles, W., Manes, F., Pastor, D., Tolosa, P. y Tomeo, F. (2017, noviembre) *Gobernanza Inteligente e innovación inclusiva. Desafíos y oportunidades para promover la efectividad de los derechos en la cuarta revolución industrial.* Ponencias presentadas en Congreso Internacional que se llevó a cabo en la Universidad de Buenos Aires.

Buriticá Tobón, G. (2003, octubre). *Como obtener y presentar evidencia Digital*. Ponencia presentada en el III Congreso Mundial de Derecho e Informática que se llevó a cabo en la Universidad Nacional de Colombia.

Legislación

a) Nacional

Constitución Nacional Argentina

Decreto N° 2628/2002. Reglamentario de Ley de Firma Digital. (2002)

Ley N° 25.506. Firma digital. (2001)

Ley N° 26.388. Modificación del Código Penal, que penaliza delitos informáticos. (2008)

Ley N° 27.063. Aprueba la reforma del CPPN. (2014)

Ley N° 26.904. Ley del Grooming. (2018)
Ley N° 26.685. Expedientes Digitales. (2011)
Ley N°2.303. Código Procesal Penal CABA. (2017)
Ley N° 10.317. Código Procesal Penal Entre Ríos. (2014)
Ley N° 5.478. Código Procesal Penal Chubut. (2006)
Ley N° 8123. Código Procesal Penal Córdoba. (1995)

b) Extranjera

Convención de Budapest (2001). Ratificada por Argentina noviembre 2017.
Ley 25/2007 de conservación de datos de las comunicaciones electrónicas, accesibles previa autorización judicial y con los requisitos legales, octubre 2007. Madrid.
Decreto-Ley núm. 78/87, de 17 de febrero de 1987, por el que se dicta el Código Procesal Penal (actualizado hasta el Decreto-Ley núm. 324/2003, de 27 de diciembre de 2003). Portugal
Decreto-Ley núm. 400/82 de 23 de septiembre, por el que se dicta el Código Penal. Portugal.
Ley N° 527/1999. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. Colombia.

Otros

ACD (2017). "*Evidencia digital, Investigación de cibercrimen y Garantías del Proceso Penal"*. Disponible en https://adcdigital.org.ar/wp-content/uploads/2017/12/ADC-Evidencia-Digital-Investigacion-Cibercrimen.pdf

Canal AR (2016). *Aseguran que hay más de un 55% de argentinos con Smartphone*. Disponible en http://www.canal-ar.com.ar/24791-Aseguran-que-hay-un-55-por-ciento-mas-de-argentinos-con-smartphone.html.

IOCE (2000). International Organization on Computer Evidence. *Evidencia digital*. Disponible en http://www.ioce.org/.

Palazzi, Pablo "*La controversia sobre la retención de datos de tráfico en internet*". La Ley 25873. Disponible en http://www.habeasdata.org/wp/2005/06/01/DatosTrafico/

Piccirilli, D.A. (2013). *La forensia como herramienta en la pericia informática.* Disponible en http://sistemas.unla.edu.ar/sistemas/redisla/ReLAIS/relais-v1-n6-237-240.pdf

Sergi, Natalia. (2018). *Análisis jurídico de la situación de la evidencia digital en el proceso penal en Argentina*. Disponible en https://adcdigital.org.ar/wp-content/uploads/2018/04/Analisi-juridico-evidencia-digital-proceso-penal.pdf.

Salt, Marcos (2017). *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.

Viegener, Francisco (2018); "*El Derecho a la Intimidad y los Límites a la Injerencia Estatal*". Disponible en www.alfa-redi.org.

Association of Chief Police Officers, A. (2003). *Good Practice Guide for Computer-Based Electronic Evidence*:
Disponible en: ww.cps.gov.uk/legal/assets/uploads/files/ACPO_guidelines_computer_evidence.pdf
Protocolo unificado de los ministerios públicos de la República Argentina – *Guía para el levantamiento y conservación de la evidencia.* Disponible en: www.jus.gob.ar/media/3262247/Protocolo%20unificado.pdf

Neuquén, P. J. (05 de 07 de 2013). *Pericias Informáticas. Protocolo de Actuación para Pericias Informáticas*. Disponible en: http://periciasinformaticas.sytes.net/index.php?option=com_docman&task=cat_view&gid=39&Itemid=59

Gómez, L. (2008) Buenas Prácticas para el secuestro de evidencia digital. Disponible en: http://es.slideshare.net/cxocommunity/buenas-prcticas-para-el-secuestro-de-evidencia-digital-sebastiangomez.

Gómez, L. (2013) Pericias informáticas sobre telefonía celular. Disponible en: http://www.jusneuquen.gov.ar/images2/Biblioteca/ProtocoloPericiasTelefoniaCelular.pdf.

Parlamento Europeo. Comisión de Libertades Civiles, Justicia y Asuntos de Interior. *Segundo Documento de trabajo sobre la propuesta de Reglamento sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal* (2018/0108 (COD)). Disponible en: http://www.europarl.europa.eu/committees/es/working-documents.html?action=1

Jurisprudencia

Suprema Corte de los Estados Unidos, County of Monroe, *People v. Emerson*. 766 N.Y.S.2d 482 (2003). Debido Proceso. Privacidad. Exceso de búsqueda. Plain View.

Suprema Corte de los Estados Unidos. District of Connecticut, *United States of America v. Aleksey Vladimirovich Ivanov*.175 F. Supp. 2d 36 (2001).

Suprema Corte de los Estados Unidos, *United States v. Antoine Jones*. 565 U.S. 400 (2012). Debido proceso. Proceso Penal. Admisibilidad de las pruebas. Allanamiento. Derecho a la intimidad.

Corte de Apelaciones de Estados Unidos, Noveno Circuito. *Estados Unidos v. Raymond Wong*. 334 F.3d 831 (2003). Registro domicilio. Causa desaparición. Pornografía en dispositivo de tercero. Teoría del árbol envenenado.

Corte Suprema de los Estados Unidos, *Horton v. California*, 496 US 128 (1990). Plain View. Exceso de búsqueda autorizada.

Corte Suprema de los Estados Unidos, *Katz v. Estados Unidos,* 389 US 347 (1967). Derecho a la privacidad. Comunicaciones basadas como llamadas telefónicas.

Corte Suprema de los Estados Unidos, Carpenter v. United States, No. 16-402, 585 US (2018). Derecho a la privacidad. IV Enmienda. Trazabilidad de la ubicación por telefonos celulares.

Corte Suprema de los Estados Unidos, *United States v. White*. 401 US 745 (1971), conversaciones usando transmisores de radio ocultos, por informantes no viola la protección de la Cuarta Enmienda contra búsquedas y confiscaciones no razonables, y por lo tanto no requiere una orden judicial.

Corte de Apelaciones de Estados Unidos, Noveno Circuito, *Cobbler Nevada, LLC v. Gonzalez.* No. 17-35041 (2018). Estable que una dirección de Protocolo de Internet asociada con una actividad infractora no es suficiente para declarar una reclamación por infracción directa o contributiva.

Poder Ejecutivo Nacional, "Halabi, Ernesto c/ P.E.N. - ley 25.873 - dto. 1563/04 s/ amparo ley 16.986". Fallo 332:111. 24/02/2009. Derechos de incidencia colectiva, proceso colectivo y garantías
Constitucionales.

Cámara Federal de Casación Penal, Sala IV "Merida, Maximiliano s/elevación a juicio". Causa Nº 29815/III. 03/12/2015. Plain View.

Cámara de Apelaciones en lo Civil, Comercial, Minas, de Paz y Tributario, Sala de Acuerdo "Llopart Ricardo Jose c/Lombardich Luis y Otros p/Cobro de Pesos". Expte. 52190. 01/06/2017. Apreciación de la prueba. Admisión WhatsApp.

Tribunal de Impugnación de Salta, Sala IV. S/ delitos de grooming y abuso sexual con acceso carnal en concurso real en perjuicio de D.M.Y". Causa N° JUI 125162/16. 01/06/2017. Delito de grooming.

Cámara de Apelaciones en lo Criminal y Correccional Federal, Sala I. "Fiscal". Causa N°46.744. Reg. Nº 458. 24/5/2012.Prueba. Informe pericial. Notificación. Derecho de defensa. Cadena de custodia. Nulidad.

Cámara de Apelaciones en lo Criminal y Correccional Federal, Sala II. "Ilic Dragosla v y otros". Causa Nº 25062. 5/6/2007. Correo electrónico. Pruebas. Querella.

Cámara Nacional de Apelaciones en lo Comercial, Sala D. "Bunker Diseños S.A. c/IBM Argentina S.A.". Expte. Nº 29.958/2004. 2/3/2010.Prueba documental. Correo electrónico. Firma. Instrumentos privados.

Cámara Nacional de Apelaciones en lo Comercial, Sala D. "Henry Hirschen y Cia. S.A. c/Easy Argentina S.R.L.". Expte. Nº 48061. 16/2/2007.Correo electrónico. Prueba. Firma. Facturas.

Cámara de Apelaciones en lo Civil y Comercial de Córdoba, Sala primera. "Pisanu Juan Mauro c/ Carteluz S.R.L.". Expte. Nº 1642556/36. 22/5/2014.Prueba documental. Correo electrónico. Firma. Informe pericial.

Cámara Nacional de Apelaciones en lo Criminal y Correccional, Sala VII. "Pucill, Hernán C.". Causa Nº 27.462/14. 25/11/2015.Prueba digital. Correo electrónico. Violación de correspondencia. Nulidad parcial.

Cámara Nacional de Apelaciones en lo Criminal y Correccional, Sala IV. "R., J. C.". Expte. Nº 39989/2012/CA1. 8/7/2013.Mensajes de texto. Telefonía celular. Red social. Facebook. Pruebas.

Cámara Nacional de Apelaciones en lo Penal Económico, Sala A. "Steinhaus, Raquel y otros ". Causa Nº 48760. 13/9/2002.Garantías constitucionales. Correo electrónico. Derecho a la privacidad.