XXXI CONGRESO NACIONAL DE DERECHO PROCESAL (MENDOZA)

COMISIÓN 1 (PROC. PENAL): El uso de los medios telemáticos y las audiencias remotas en el proceso penal

TEMA: La búsqueda de evidencia y la producción de la prueba en el proceso penal de la era digital

AUTORA: DANIELA ILEANA MARGARITA PIOMBO (*)

FECHA DE NACIMIENTO: 21/10/1989 (32 AÑOS)

DIRECCIÓN POSTAL: 17 N° 370 LA PLATA

TELÉFONO CELULAR: 221-5450966

CORREO ELECTRÓNICO: DANIELAIMPIOMBO@GMAIL.COM

BREVE SÍNTESIS DE LA PROPUESTA:

El presente trabajo tiene por finalidad reflexionar a la luz de la actual legislación vigente y tratados internacionales los problemas más relevantes en torno a los medios de prueba en la era digital vinculadas a los procesos de investigación y juzgamiento de delitos, como así también respecto a las garantías constitucionales en juego, a efectos de poder proponer las reformas y actualizaciones necesarias que permitan alcanzar investigaciones más eficaces en materia de ilícitos perpetrados mediante tecnologías legales.

**La Autora deja plasmada de su voluntad de postularse para el concurso "Jóvenes Ponentes" organizado por la Fundación de Estudios Superiores e Investigación (FUNDESI) y para el concurso "Premio A.A.D.P". A su vez, deja constancia no hallarse incursa en las exclusiones previstas por los reglamentos.*

LA EVIDENCIA DIGITAL: interrogantes y nuevos desafíos

Por Daniela I. M. Piombo

I.- Introducción

La emergencia sanitaria global causada por el COVID-19, ha provocado en el último tiempo un aumento de las amenazas y delitos cometidos mediante el uso de las nuevas tecnologías, redes sociales y otros medios digitales[1]. Hasta el momento, el ojo siempre estuvo en la necesidad de adaptar el derecho de fondo a las nuevas tecnologías, creando nuevos o reformando tipos legales ya existentes[2]. Sin embargo, el foco de la discusión actual debe girar en torno a otro problema: cómo probarlos.

El trabajo intentará demostrar algunos problemas en el plano procesal derivados de la gran inseguridad jurídica que subsiste, principalmente, como consecuencia de la obsoleta regulación existente en relación a los nuevos medios de prueba tecnológicos. A su vez, la prueba digital plantea una serie de exigencias al momento de su obtención y aportación al proceso que deben tenerse en cuenta a la hora de asegurar su validez y eficacia, como así también requiere de altos niveles de capacitación y cooperación en el plano internacional.

La investigación del entorno digital de una persona puede incrementar la eficacia de la persecución y prueba de actividades en multitud de ámbitos de la actividad humana, pero también, como se analizará, lleva consigo un riesgo potencial de lesividad para los derechos fundamentales de las personas investigadas, especialmente la intimidad, el secreto de comunicaciones y la protección de datos personales.

II.- La evidencia digital y el estado actual de la cuestión

[1] La permanente conexión a través de equipos informáticos y dispositivos electrónicos llevaron a que un gran número de la ciudadanía fuera víctima de técnicas de manipulación informática, tales como *phishing*, sustitución de identidad, extorsión sexual, entre otros.

[2] En los últimos años se presentaron numerosos proyectos de ley destinados a reformar el Código Penal para adaptar los tipos penales a estas nuevas modalidades comisivas. Finalmente, la ley 26.388 incluyó diez tipos penales: 1. El ofrecimiento y distribución de imágenes relacionadas con pornografía infantil (art. 128). 2. Violación de correspondencia electrónica (art. 153). 3. Acceso ilegítimo a un sistema informático (art. 153 bis). 4. Publicación abusiva de correspondencia (art. 155). 5. Revelación de secretos (art. 157 del Cód. Penal). 6. Delitos relacionados con la protección de datos personales (art. 157 bis). 7. Defraudación informática (art. 173, inc. 16). 8. Daño simple y agravado (arts. 183 y 184). 9. Interrupción o entorpecimiento de las comunicaciones (art. 197l). 10. El tipo penal de alteración, sustracción, ocultación, destrucción e inutilización de medios de prueba (art. 255). A este catálogo de delitos, se le sumaría en diciembre del año 2013, a través de la ley 26.904, el tipo penal de *grooming* o ciberacoso sexual a menores, completando así el listado de tipos penales propios de la criminalidad informática en el sistema jurídico argentino.

Los cambios vertiginosos en la informática y las telecomunicaciones han generado un replanteo en la forma de afrontar las investigaciones cuando las conductas ilícitas se cometan por medios informáticos o, cuando para su persecución, sea necesaria la obtención de evidencia digital contenida en dispositivos de comunicaciones.

Puede definirse la evidencia digital como el conjunto de datos e información, relevantes para una investigación, que se encuentran almacenados o transmitidos en un formato digital o a través de un medio informático, que sea útil para acreditar hechos en un proceso[3].

Este tipo de prueba tecnológica aparece como consecuencia de las nuevas modalidades mediante las cuales los seres humanos comenzaron a cometer ilícitos: el cibercrimen, entendiendo esto como cualquier delito que se comete mediante, a través o con la intervención de medios electrónicos[4].

Conforme es señalado la evidencia digital presenta varios caracteres: intangible, replicable, volátil y alterable[5]. Esto conlleva a que la misma, por su propia naturaleza, sea frágil y de fácil modificación o destrucción. Estas notas características de la evidencia digital, hizo que muchos países modificaran su legislación procesal para prever medidas especiales necesarias para la investigación en entornos digitales.

Ya la Convención de Budapest advertía sobre este problema y la necesidad de introducir un conjunto de herramientas procesales especiales tendientes a la obtención de evidencia digital para la investigación no sólo de los denominados delitos informáticos, sino también a los demás delitos cometidos por medios informáticos y la recolección de evidencia digital en la investigación de cualquier delito que así lo requiera. En efecto, sobre este punto impone la adopción de medidas legislativas tendientes a lograr: conservación rápida de datos almacenados (art. 29); revelación rápida de datos de tráfico conservados (art. 30); confiscación, obtención o revelación de datos almacenados (art. 31); acceso transfronterizo sin previo requerimiento estatal, siempre que los datos sean de fuente abierta, o se tenga su acceso mediando el consentimiento de la persona legalmente

[3] DELGADO MARTIN, J., "La prueba digital constituye un reto proceso, en el que hay que tener muy en cuenta los derechos de fundamentales de las personas", Diario La Ley España Ciberderecho, Nº 41,2020, Wolters Kluwer. Definición recogida por el autor de la elaborada por el FBI en el documento: *"Digital Evidence: Information of probative value stored or transmitted in digital form".*

[4] ABDELCADER, Y., "La evidencia digital en el proceso penal", cita online: TR LA LEY AR/DOC/4223/2019.

[5] MAGRO SERVET, V., "Casuística práctica de la prueba digital en el proceso civil y penal", La Ley España Actualidad Civil N°2, 2020, Wolters Kluwer.

autorizada a revelarlos (art. 32); obtención en tiempo real de datos de tráfico (art. 33); e interceptación de datos de contenido (art. 34).

La Argentina mediante la sanción de la ley 27.411 aprobó la mentada convención, lo que implicó una serie de reformas procesales a tal fin, aunque la mayoría de los regímenes continúan hoy aplicando analógicamente las normas existentes para evidencia física a aquellos supuestos de obtención de evidencia digital[6].

En definitiva, nos encontramos ante un escenario donde se carece expresamente de medios procesales para investigar. Como excepción, podemos destacar el denominado nuevo Código Procesal Penal Federal[7] - cuya entrada en vigor se ha dispuesto en forma progresiva - que incluye ciertas nociones relativas a medios de prueba. Así, podemos identificar los arts. 150 y 151[8], los cuales regulan la posibilidad de interceptación de comunicaciones electrónicas y la incautación de datos almacenados en algún medio informático. Resulta interesante el tratamiento que el legislador ha dispuesto en relación a la información no vinculada a la investigación criminal en curso. De esta manera, se trata de los pocos códigos que contiene una normativa reguladora de procedimientos en materia de obtención de evidencia digital, sin necesidad de tener que recurrir a la técnica de la analogía[9], según la cual basta para aplicarlos con asimilarlos a algún medio de prueba ya regulado.

En este tipo de evidencia, dada las características fundamentales señaladas, deben respetarse una serie de procedimientos para su recogida, etiquetado, almacenamiento y posterior análisis[10]. A continuación, a partir del dictado de la norma ISO/IEC

[6] CAFFERATA NORES, J., *La prueba en el proceso penal*, Ed. De Palma, 1998, p. 21.
[7] Decreto N° 118/2019 B.O. 8/2/2019 por el cual se aprueba el texto ordenado del "Código Procesal Penal Federal", aprobado por la Ley Nº 27.063 con las incorporaciones dispuestas por la Ley Nº 27.272 y las modificaciones introducidas por la Ley Nº 27.482, el que se denominará "Código Procesal Penal Federal" (T.O. 2019).
[8] "Art. 150: Interceptación. Siempre que resulte útil para la comprobación del delito, el juez podrá ordenar, a petición de parte, la interceptación y secuestro de correspondencia postal, telegráfica, electrónica o cualquier otra forma de comunicación o de todo otro efecto remitido por el imputado o destinado a este, aunque sea bajo nombre supuesto. Art. 151: Incautación de datos. El juez podrá ordenar a requerimiento de parte y por auto fundado, el registro de un sistema informático o de una parte de este, 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, bajo las condiciones establecidas en el art. 129".
[9] MOLINAS, J., La obtención de evidencia digital y sus desafíos constitucionales. Una mirada defensista", cita online: TR LA LEY AR/DOC/392/2019.
[10] RUBIO ALAMILLO, J., "Cadena de custodia y análisis forense de smartphones y otros dispositivos móviles en procesos judiciales", La Ley España Ciberderecho, Nº 22, 2018, Wolters Kluwer.

27037/:2012[11], el documento aprobado por la Procuración General de la Nación[12] y la reciente Res. 528/2021 del Ministerio de Seguridad de la Nación[13], se intentarán brindar una serie de reglas que deben ser tenidas en cuenta por los operadores del sistema a la hora de dar tratamiento a la evidencia digital:

— Asegurar el lugar mediante la documentación de cualquier tipo de actividad que esté teniendo lugar en la computadora, componentes externos y/o dispositivos de almacenamiento. Todos los dispositivos deben ser correctamente fotografiados, filmados, etiquetados y embalados en bolsas[14].

—La intervención de un especialista en informática forense que reúna los conocimientos técnicos esenciales en la materia[15].

—La obtención de una copia o imagen exacta de la información digital contenida en el soporte electrónico original (copia *bit* a *bit*) mediante *softwares* autorizados al efecto[16]. Resulta recomendable el empleo para esta operación de un bloqueador de escritura (*write blocker*) ya que de este modo se asegura que no se modifique absolutamente la más mínima información (únicamente permite la mera lectura y copiado de los archivos) y la presencia de testigos que permitan otorgar transparencia al acto.

—La generación de un código *hash*[17], de manera que permita garantizar la "mismidad" de la evidencia informática, de tal suerte que, cualquier manipulación - por más mínima que sea - que se realice sobre un archivo del que se ha calculado su código, arrojará un nuevo algoritmo totalmente diferente para dicho conjunto de datos.

[11] La ISO (*International Standarization Organization*) es la entidad internacional encargada de favorecer normas de fabricación, comercio y comunicación en todo el mundo, brindando estándares internacionales. Puede visualizarse parte del documento "Guía para la identificación, recolección, adquisición y preservación de la evidencia digital", disponible en https://www.iso.org/obp/ui/#iso:std:iso-iec:27037:ed-1:v1:en

[12] "Guía de obtención, preservación y tratamiento de evidencia digital", Res. PGN Nro. 756/16, 31 de marzo de 2016. Se trata de una guía que contiene protocolos de actuación para la recolección de evidencia digital.

[13] Mediante la cual se aprobó el "Protocolo de actuación para la investigación científica en el lugar del hecho y sus anexos, 25/11/2021. El mismo puede consultarse a través de la página oficial del Boletín Oficial (https://www.boletinoficial.gob.ar).

[14] Para ello se sugiere utilizar las denominadas "jaulas de aislación Faraday" que permiten mantener los equipos electrónicos bloqueados de cualquier transmisión de datos con el exterior.

[15] Los dispositivos deben manipularse por un experto en informática, ya que de efectuarse por una persona sin los conocimientos y herramientas específicos podría afectarse la prueba recolectada, alterando su contenido original, o bien perjudicando las copias, las cuales podrían no ser iguales a la evidencia.

[16] El art. 148 del reciente Código Procesal Penal Federal recepta esta posibilidad: "Podrá disponerse la obtención de copias, reproducciones o imágenes de los objetos cuando resulte más conveniente para la investigación".

[17] Algoritmo matemático que se realiza sobre el conjunto de los datos contenidos en un concreto dispositivo o soporte digital, de 32 o más dígitos. Su aplicación permite acreditar la autenticidad y la preservación de integridad de los datos (asegura que la información no ha sido alterada por personas no autorizadas hasta que sea presentada al tribunal).

El aseguramiento de estos mínimos pasos garantiza la máxima transparencia a la hora de proceder a la recolección de evidencias digitales y permite, a la vez, la verificación a *posteriori* de la integridad de la evidencia mediante la comprobación de la huella digital.

Como indicamos la mayoría de los códigos procesales vigentes en nuestro país aún no cuentan con una regulación específica. Por ello, en la práctica resulta esencial la urgente reforma o, al menos, la elaboración en todas aquellas jurisdicciones territoriales de protocolos de actuación que homogenicen dichas actuaciones. Sobre la primera solución, Perez Barberá pone de resalto la paradoja que representa tener regulado en nuestros códigos la prueba testimonial o pericial y ningún medio de prueba basado en las nuevas tecnologías con el altísimo potencial vulnerante de la privacidad que aquellas conllevan[18]. No parece, pues, dejar librado a cada juez que determine en cada caso concreto si el empleo de la tecnología ha sido lícito o no.

Otro aspecto sustancial, que debe garantizarse es la cadena de custodia tanto de los originales como de las imágenes forenses realizadas. Por tal, se entiende al conjunto de actos que tienen por objeto la recogida, el traslado y la conservación de los indicios o vestigios obtenidos en el curso de una investigación criminal, actos que deben cumplimentar una serie de requisitos con el fin de asegurar la autenticidad, inalterabilidad e indemnidad de las fuentes de prueba.

Por último, el órgano jurisdiccional valorará la autenticidad e integridad de la prueba conforme las reglas de la sana crítica, de acuerdo con criterios como la seriedad de los argumentos y otros medios de prueba y dictámenes periciales y argumentales propuestos por las partes, destinados a acreditar las condiciones de autenticidad e integridad de la prueba electrónica.

III.- Algunos problemas vinculados a la prueba informática

Si bien es cierto que en el proceso penal rige el principio de libertad probatoria, la falta de una moderna legislación procesal respecto a la evidencia digital genera un elenco de inconvenientes que deben afrontarse adecuadamente, de lo contrario esto podría conspirar contra el buen éxito de las investigaciones.

[18] PEREZ BARBERÁ, G. "Nuevas tecnologías y libertad probatoria en el proceso penal" ponencia presentada en el VI Encuentro Nacional de Profesores de Derecho Procesal Penal realizado en la ciudad de Salta, mayo de 2009.

1.Limitaciones constitucionales: La obtención de la prueba digital puede afectar una serie de derechos fundamentales (como la intimidad personal, el secreto de las comunicaciones, la protección de datos personales, libertad de expresión, etc.) cuya vulneración podría dar lugar a nulidades que pongan en jaque las actuaciones. En el plano internacional los estados nacionales y, en particular, Argentina se han comprometido a garantizar el respeto a la privacidad de las personas como forma de desarrollo humano.

El registro de dispositivos informáticos personales supone un nivel de intrusión mayor al ámbito de privacidad e intimidad individual, motivo por el cual las órdenes libradas al efecto deberán ser fundadas y expedidas por autoridad judicial competente, en la que se acredite la necesidad, idoneidad y proporcionalidad de la medida dispuesta[19]. Algunos autores cuestionan su utilización en caso de investigación de delitos castigados con penas leves; pero lo cierto es que el empleo de tecnologías de telecomunicación genera una difusión rápida, trasnacional, masiva, anónima que permite, en muchos casos, fundar estos extremos[20].

Actualmente, el Cód. Proc. Penal de la Nación concede amplias facultades al investigador al no restringir el objeto de búsqueda, permitiéndole acceder a la totalidad de los datos de cualquier dispositivo informático, lo que genera un gran menoscabo a la privacidad de los individuos (art. 224).

Una buena alternativa, sería la extensión de órdenes detalladas y no generales e imprecisas, como así también la implementación de protocolos de búsqueda de datos mediante “palabras clave”, a partir de las cuales se identifiquen y extraigan las imágenes forenses ubicadas en dichos ficheros. De esta manera, es posible identificar, seleccionar y recortar aquella parte de la información que cumpla con el patrón y descartar el resto de documentación que pueda contener información de carácter personal[21]. En caso de producirse “hallazgos casuales” que tengan que ver respecto de otros hechos o

[19] El art. 18 dispone la inviolabilidad del domicilio, la correspondencia epistolar y los papeles privados. La jurisprudencia viene reconociendo que dentro de esa enunciación quedan comprendidas también las comunicaciones realizadas mediante correos electrónicos, llamados telefónicos o mensajes de texto, entre otros.
[20] VELASCO NUÑEZ, E., “Diligencias de investigación penal”, La Ley España, junio, 2010.
[21] En el caso "*United States v. Carey*" (1999) la policía copió archivos con nombres que sugerían contenido sexual y extensión jpg. de una de las computadoras incriminadas, a pesar de que la orden era detallada y autorizaba a buscar “nombres, números de teléfono, anotaciones, direcciones vinculadas a la distribución de sustancias estupefacientes. La justicia entendió que se excedieron los límites de la orden de registro al revisar archivos de imagen y por lo tanto invalidó el secuestro realizado relativo a pornografía infantil.

conductas que pueden llegar a ser delictivas por parte de los investigadores, deberá gestionarse ante la autoridad competente la ampliación de la orden de registro y secuestro a fin de evitar futuras nulidades[22].

Otra cuestión fundamental, es limitar el registro y secuestro de evidencia digital a un rango temporal determinado, principalmente, porque los soportes pueden contener datos informáticos almacenados de vieja data. A diferencia del registro y búsqueda de un elemento físico, en los dispositivos electrónicos se podrá encontrar todo lo que esté alojado digitalmente en ese momento, lo de hace un mes o, incluso, años atrás.

Respecto al tratamiento de los archivos eliminados, podrían surgir diversas controversias, las que deberán resolverse en cada caso particular respecto a la configuración de la conducta investigada, debido a que podrían tratarse de elementos que permitan acreditar la consumación del delito, o un grado de ejecución incompleta (tentativa) pero también constituir un desistimiento activo voluntario o quedar en meros actos preparatorios impunes.

En definitiva, el desafío consiste en que el diseño del procedimiento elegido sea capaz de conjugar las garantías constitucionales y procesales de defensa en juicio, debido proceso, legalidad, con las demás exigencias propias de estos medios de investigación.

2. Conflictos de competencia: Como se afirmaba, la propia naturaleza de los hechos bajo análisis ha generado ciertos problemas relativos a la competencia territorial de los jueces en razón de su interjurisdiccionalidad[23].

Nuestro país, a la hora de aplicar su ley penal, privilegia el principio de territorialidad (se aplica la ley penal argentina para el juzgamiento de los delitos cometidos en el territorio de la Nación y en los lugares sometidos a su jurisdicción)[24]. Esto significa que tiene valor sólo en los límites del territorio que la sancionó, principio que domina la aplicación de la ley penal en el espacio, de manera que el lugar de comisión del hecho (*forum delicti commissi,* art. 118 CN) determina la ley penal aplicable[25].

---

[22] DÍAZ KINDSVATER, J., "Evidencia digital y *plain view*: recaudos para evitar planteos de invalidación procesal", cita online: TR LA LEY AR/DOC/40/2021. La doctrina de la "plena vista" supone la posibilidad de incautar evidencia descubierta durante un registro válido si la naturaleza incriminatoria del elemento que hay que incautar, suficiente para crear una causa probable de que este constituye una prueba, es inmediatamente aparente.

[23] ROSENDE, E., "Ejercicio de la acción y la competencia en los delitos informáticos", cita online: LA LEY AR/DOC/3820/2012

[24] FREELAND, A., "Internet y Derecho Penal", cita online: TR LA LEY 0003/007609.

[25] SALT, M., "Nuevos desafíos de la evidencia digital. El acceso transfronterizo de datos en los países de América Latina", cita online: TR LA LEY AR/DOC/5459/2013.

Pero, ¿qué ocurre cuando la conducta antijurídica tiene lugar en un territorio y el resultado se produce en otro? La necesidad de hacer frente de manera eficiente a la persecución de los modernos fenómenos de la criminalidad organizada trasnacional, ha hecho replantearse el principio de territorialidad y la necesidad de implementar sistemas de cooperación eficaces, como se verá en el apartado siguiente, de modo tal que las fronteras físicas no actúen como límites.

Por ello, cuando se cometen delitos informáticos cobra especial relevancia la "teoría de la ubicuidad"[26] como excepción al principio de territorialidad, según la cual el delito se comete tanto en el lugar en donde se desarrolla la acción como donde se produce el resultado[27], con lo cual quedan cubiertas ambas alternativas y se desvanece la posibilidad de impunidad. Es importante, a la hora de elegir el órgano competente para llevar adelante la investigación, lo sea el que en mejores condiciones se encuentre, en base a los distintos criterios relacionados con la cantidad de medios y recursos existentes, mejor defensa y respeto de las garantías del imputado, la facilidad y proximidad en la recolección de las pruebas, entre otros posibles[28].

3. Cooperación internacional: La obtención de evidencia digital, ya sea para la persecución de los denominados delitos informáticos como para las investigaciones de cualquier delito cuya prueba se encuentre almacenada en entornos digitales, puede hallarse muchas veces en el exterior, por ejemplo, cuando una empresa proveedora de servicios de internet tenga sus servidores en un país distinto al lugar donde se investiga la comisión del delito.

Esta circunstancia se trata de un obstáculo de difícil solución para los organismos de persecución penal estatal. Cabe destacar que, el Convenio de Budapest, al que Argentina adhirió, establece diversos mecanismos de cooperación internacional entre los Estados parte para compartir y obtener información de manera "reforzada, rápida y eficaz" mediante las vías formales, aunque también establece canales para el acceso de datos transfronterizos almacenados sin necesidad de requerir la autorización del otro Estado, de manera que el intercambio de datos puede generarse de manera rápida y sin

[26] Este principio ha sido receptado por la jurisprudencia de la CSJN en diversos fallos 271:396; 316:2373; 294:257, entre otros.
[27] El delito se reporta cometido en todas las jurisdicciones en las que se haya realizado algún elemento del tipo.
[28] FREELAND, A., "Internet y Derecho Penal", cita online: TR LA LEY 0003/007609.

participación de las autoridades estatales, sino directamente entre el Estado requirente y la empresa privada, en aquellos supuestos en que: a) éstos sean de acceso público; b) se obtenga el consentimiento lícito y voluntario de la persona legalmente autorizada a revelarlos. Este punto, plantea algunos interrogantes respecto a la interpretación sobre quién es la persona autorizada y sobre la posible afectación del principio de territorialidad y soberanía al no existir ninguna intervención del Estado nacional en el que se encuentra el servidor alojado.

Asimismo, propone la creación de una red 24/7, es decir que cada Estado establecerá un punto de contacto las 24 horas, los 7 días de la semana con el objetivo "de garantizar una asistencia inmediata para investigaciones relativas a delitos vinculados a sistemas y datos informáticos, o para obtener las pruebas en formato electrónico de un delito" (art. 35).

Por regla general, en los casos que las evidencias se encuentren en un país extranjero, los Estados deberán requerirlas mediante los mecanismos de cooperación internacional que rijan la relación entre ambos países.

A diferencia de la ley penal, la ley procesal penal rige el principio de *lex fori*. En otras palabras, existe aplicación extraterritorial de la ley procesal para la realización de las medidas solicitadas a extrañas jurisdicciones. Este principio expresa que el tribunal competente para instruir el procedimiento aplica la ley procesal sancionada por el poder soberano que creó el tribunal[29].

De modo cada vez más evidente, surge la necesaria suscripción a nivel internacional como regional de instrumentos de cooperación internacional para combatir en forma efectiva el fenómeno de la cibercriminalidad y evitar que los hechos delictivos queden impunes.

4. Capacitación: Los operadores del sistema judicial deben capacitarse en las posibilidades que ofrecen las diferentes herramientas forenses[30]. Es necesario que los fiscales y jueces entiendan de tecnología y empiecen a familiarizarse con términos,

[29] SALT, M., "Nuevos desafíos de la evidencia digital. El acceso transfronterizo de datos en los países de América Latina", cita online: TR LA LEY AR/DOC/5459/2013.

[30] Ta como fuera puesto de manifiesto en las conclusiones del XXX Congreso Nacional de Derecho Procesal en la Comisión N° 1 de Derecho Procesal Penal, las nuevas tecnologías exigen una debida capacitación de todos los operadores del sistema, a la hora de la obtención, preservación, elaboración de la cadena de custodia, determinación de los puntos de pericia y redacción de pedidos de informes a empresas de servicios digitales.

conceptos y procedimientos que no integran el campo de sus incumbencias específicas. Por ello, resulta imperioso el dictado de cursos de actualización y capacitación de manera periódica y obligatoria para los representantes del Poder Judicial.

IV.- Conclusiones finales

A lo largo de este trabajo hemos podido apreciar como el desarrollo de nuevas tecnologías obliga a pensar la urgente introducción de normas procesales y herramientas informáticas en ocasión de futuras reformas que permitan la obtención y conservación de la evidencia digital en el proceso penal[31].

Del análisis de las dificultades vinculadas a la aparición de nuevas tecnologías en el marco de las investigaciones criminales, pueden extraerse las siguientes conclusiones: 1) Adaptación legislativa a los requerimientos del "Convenio sobre Cibercriminalidad" de Budapest, tanto respecto del derecho penal sustantivo (sección I) como del derecho procesal (sección II). Sobre este punto, corresponde que el legislador regule los modernos medios de prueba en la ley procesal, teniendo presente los principios de legalidad, proporcionalidad y gravedad 2) La confección de guías prácticas por parte de los cuerpos periciales y de seguridad en todos los ámbitos jurisdiccionales con el objeto de estandarizar los procedimientos de recolección y tratamiento de la evidencia digital 3) Las órdenes de registro de evidencia digital deberán estar debidamente fundadas y restringidas al objeto de búsqueda a fin de no lesionar otros derechos y garantías 4) Recepcionar en materia de competencia el principio de ubicuidad 5) Avanzar en la suscripción de instrumentos de cooperación tanto a nivel internacional como regional que autorice la práctica de medidas investigativas y el acceso transfronterizo de datos de manera rápida y eficaz 6) Capacitación periódica y obligatoria del personal de los órganos de justicia y fuerzas de seguridad para que tomen conocimiento de las nuevas herramientas forenses[32].

[31] SALT, M., "Nuevos desafíos de la evidencia digital. El acceso transfronterizo de datos en los países de América Latina", cita online: TR LA LEY AR/DOC/5459/2013.
[32] PICCIRILLI, M., "Ausencia de regulación procesal penal aplicable a la evidencia digital y su correlación con los delitos informáticos. Legislación vigente, anteproyectos y convenio de Budapest", cita online: TR LA LEY AR/DOC/509/2020.

Las siguientes recomendaciones, en caso de ser adoptadas y aplicadas por quienes tengan la responsabilidad y competencia para hacerlo, permitirán amalgamar los fines del proceso con el debido respeto de derechos y garantías constitucionales.