Artículos

Revista Pensamiento Penal
Sección Medios digitales y delitos informáticos
Vol. 2, núm. 4 – 2025, págs. 16–28
ISSN: 1853 – 4554
DOI: https://doi.org/10.64178/azymfr57

Evidencia digital

Introducción al proceso penal: anomia procesal y garantías constitucionales

Eduardo Daniel Viazzi[1]

Resumen

En la actualidad, la incorporación de evidencia digital al proceso penal se ha vuelto cada vez más frecuente, resultado del uso masivo de herramientas y tecnologías informáticas que atraviesan prácticamente todos los aspectos de la vida cotidiana. Las nuevas formas delictivas —habitualmente denominadas «ciberdelitos»— conviven con los tipos penales tradicionales y, en la mayoría de los casos, las tecnologías digitales inciden en la organización de la conducta, en el *iter criminis* o en las fases posteriores a la comisión del hecho. El propósito de este trabajo es precisar cómo debe recolectarse, tratarse, introducirse e interpretarse la evidencia digital en el marco del proceso penal, considerando que las normas rituales vigentes fueron dictadas en un contexto radicalmente distinto, cuando los medios de prueba distaban mucho de poseer las características actuales. En consecuencia, se impone actualizar el rito penal al entorno informático a fin de prevenir eventuales afectaciones a las garantías constitucionales. Para ello, y dado el escaso tratamiento que la temática ha recibido en nuestro sistema judicial y en la jurisprudencia local, se propone abordar la evidencia digital desde su conceptualización, para luego examinar su incorporación en la fase de investigación y analizar los conceptos y precedentes relevantes tanto a nivel nacional como internacional.

Sumario

Palabras clave

evidencia digital – ciberdelitos – metadatos – investigación forense digital – derecho penal informático

[1] Abogado por la universidad nacional de Río Cuarto. Especialista en derecho penal por la universidad de Belgrano. Correo electrónico: viazzi.estudio@gmail.com

1. Breve introducción

Las nuevas tecnologías han venido a revolucionar el modo de vida de los sujetos a tal punto que prácticamente no existen aspectos de la vida cotidiana en los que no tome intervención un dispositivo electrónico que, como tal, almacena datos e información. Piénsese por ejemplo en el caso de un teléfono celular que almacena, entre otras cuestiones, fechas, agenda, comunicaciones laborales y personales, cuentas bancarias, contraseñas, etc. es decir, un sinnúmero de datos que resultan ser una fiel representación de la vida de una persona.

Ahora bien, en el marco de un proceso penal y, puntualmente, en el afán de recolectar evidencia, esos datos pueden afectar la personalidad del sujeto cuando trascienden esferas de intimidad (por ejemplo, al lesionar la expectativa razonable de privacidad) que el sujeto entiende amparada normativa y socialmente.

Los avances tecnológicos obligan a que el sistema de investigación penal deba aggiornarse al ritmo que lo han hecho las manifestaciones delictivas más actuales identificadas como delitos informáticos. Emerge así el derecho penal informático (*cybercrime*) como una representación de aquellos delitos que se cometen mediante el empleo de terminales electrónicas, independientemente de que el destinatario de la ofensa sea un sujeto determinado o un sistema de información.

La investigación de este tipo de delitos resulta más compleja, en parte por la volatilidad de la llamada evidencia digital que exige una preparación y capacitación particular de las fuerzas de seguridad para garantizar la cadena de custodia de todos los elementos probatorios recolectados.

Ahora bien, el propósito del presente artículo es examinar qué es la evidencia digital, qué abarca el concepto y cómo debemos proceder frente a la misma, esto es, su recolección, análisis, conservación y cadena de custodia. Es decir, cuáles son las «buenas prácticas» para que esta evidencia sea válida en términos procesales.

Teniendo siempre como norte el estudio de las garantías constitucionales en juego se determinará el escenario de anomia normativa que impera en la temática.

2. Conceptualización. ¿Qué es la evidencia digital?

Conceptualizar «evidencia digital» resulta dificultoso toda vez que de la conjugación de ambos términos podemos obtener tantos conceptos como enfoques se realicen sobre los mismos, esto es, no será lo mismo conceptualizar a la evidencia digital desde el punto de vista de la naturaleza de los datos, la fuente de donde provienen los mismos que hacerlo desde el contenido mismo de esos datos que, en ocasiones podrán acreditar la existencia de un hecho ilícito.

Una primera definición que puede servir como puntapié inicial para entender el concepto es aquella que identifica a la evidencia digital como un tipo de evidencia física construida de campos magnéticos y pulsos electrónicos, que por sus características deben ser recolectados y analizados con herramientas y técnicas especiales[2]. El conglomerado de elementos probatorios que engloba dicha definición resulta extenso ya que hace alusión a cualquier registro de datos que se encuentre almacenado en un dispositivo

[2] Casey, E. (2004). *Digital evidence and computer crime: Forensic science, computers, and the Internet*. Academic Press.

electrónico o informático con independencia de si la creación del dato obedece a un factor humano o a la intervención de un dispositivo tecnológico[3].

En lo que nos concierne, la evidencia digital puede ser abordada desde dos enfoques que resultan prácticos, esto es, en primer lugar, desde un enfoque que puntualiza en la cualificación de la modalidad de prueba lo que abarca a aquella información cuya fuente es el ámbito digital (soportes electromagnéticos, computadoras en donde la información se genera por reacción electrónica del dispositivo o plataformas para la gestión de información inteligente; o por empleo de gestiones humanas). En segundo lugar, el enfoque será aquel en que la categoría probatoria se basa en el hecho mismo que surge o está almacenado en la fuente digital; en este caso se pueden probar hechos de relevancia jurídica que impliquen un reproche por comportamientos delictivos[4].

De lo expuesto surge entonces que toda información almacenada en un soporte magnético o electrónico podrá ser considerada evidencia digital. La valoración de este tipo de evidencia, así como su recolección, custodia, introducción al proceso y almacenamiento obligan a un tratamiento especial por el tipo de información que suele manejarse, como así también por la propia naturaleza de la misma.

3. ¿Cómo debe tratarse este tipo de evidencia? Protocolo de actuación

La evidencia digital supone un tratamiento especial por las características propias que posee este tipo de prueba. Las particularidades que caracterizan a la evidencia digital, conforme lo analiza Sosa[5], suponen a la misma:

- Una evidencia *volátil*, es decir, puede ser fácilmente eliminada o extraviada si falla el proceso de recolección;
- Una evidencia *duplicable*, esto es, por su esencia el material es fácilmente duplicable, al punto tal de que sea dificultoso reconocer cuál es el original;
- Una evidencia *alterable*, factible de ser alterada o eliminada sin que consten registros de estas acciones;
- Una evidencia *anónima*, en ocasiones no puede determinarse quien o quienes son los autores de este tipo de evidencia.

Estas características que no son únicas pero que son las más destacadas de este tipo de evidencia implican que, recopilar y preservar la evidencia digital sea un proceso complejo que necesariamente debe ser realizado por quien posee conocimientos y comprensión de la tecnología y los sistemas informáticos.

Ahora bien, debemos entender que dicho proceso en la manipulación de la evidencia digital debe también realizarse respetando las garantías constitucionales de todo proceso penal, por ende, el proceso de recopilación, preservación, identificación, custodia, adquisición y presentación de la evidencia debe ser realizado de modo tal que se

[3] Ministerio Público Fiscal & Ministerio de Seguridad. (2023). *Protocolo para la identificación, recolección, preservación, procesamiento y presentación de evidencia digital*. https://www.fiscales.gob.ar

[4] Bujosa Vadell, L. M., Bustamante Rúa, M. M., & Toro Garzón, L. O. (2021). La prueba digital producto de la vigilancia secreta: Obtención, admisibilidad y valoración en el proceso penal en España y Colombia. *Revista Brasileira de Direito Processual Penal*, 7(2), 1347–1384.

[5] Sosa, M. E. (2023). *Evidencia digital: Su importancia en la investigación*. Revista Pensamiento Penal, (466)

garanticen la integridad y la confiabilidad de la fuente en las investigaciones judiciales y forenses.

El adecuado tratamiento de este tipo de evidencia garantizará su admisibilidad en el proceso, siempre que cumpla con ciertos requisitos. Siguiendo a Devis Echandía, la evidencia será admitida por el Juez siempre que se ponderen una serie de requisitos indispensables, como los define el autos intrínsecos y extrínsecos:

> los primeros (intrínsecos) atañen al medio mismo utilizado en cada caso incluyendo su objeto y los segundos se refieren a circunstancias que existen separadas de ese medio o, pero que se relacionan con él y lo complementan. Son requisitos intrínsecos: a) La conducencia del medio; b) la pertinencia o relevancia del hecho objeto de la prueba; c) la utilidad del medio; d) la ausencia de prohibición legal de investigar el hecho. Son requisitos extrínsecos: a) La oportunidad procesal o ausencia de preclusión; b) las formalidades procesales; c) la legitimación y postulación para la prueba de quien la pide o la presenta y la legitimación del juez que la decreta; d) la competencia del juez o de su comisionado; e) la capacidad general del juez o funcionario comisionado y de los órganos de la prueba (testigos, peritos, interpretes, partes cuando confiesan) y la ausencia de impedimentos legales en aquellos y estos.[6]

Tal como afirma Sueiro[7] la prueba electrónica distingue de la prueba física por su naturaleza particular que la caracteriza por ser intangible, latente, volátil, frágil y sensible en su integridad e inalterabilidad. Resulta intangible por el hecho de estar almacenada en códigos y diversos niveles de lenguaje lo que implica una evidencia que no es corpórea, material o física.

Estos rasgos distintivos implican que su tratamiento (en la adquisición, recolección, peritaje y conservación) sea muy distinto del que se le otorga a la evidencia física.

Entonces, podemos afirmar sin lugar a dudas que, respecto a la evidencia digital, el tratamiento es distinto y por ende existen principios específicos que lo gobiernan tales como la relevancia, la suficiencia y la confiabilidad[8].

La relevancia se identifica como un concepto netamente técnico jurídico y refiere a la pertinencia de la información en relación al hecho que se investiga. Su finalidad es dar firmeza (sea como prueba de cargo o de descargo) a la hipótesis que se intenta acreditar.

Por otro lado, la suficiencia que implica que la información aportada por el medio probatorio sea completa, de modo tal que podamos sustentar y verificar los elementos puestos en la investigación.

Finalmente, la tercera característica que gobierna a este tipo de evidencia es la confiabilidad entendida como validar la repetibilidad y auditabilidad del proceso aplicado para la obtención de la evidencia digital. Implica que la evidencia que se extraiga a través de un proceso pueda ser extraída en iguales condiciones y con el mismo alcance, si un tercero aplica el mismo proceso.

En esta línea, ha tenido amplia difusión y adhesión por parte de los organismos judiciales el manual de buenas prácticas forenses, más conocido como normas ISO/IEC 27037:2012 que, en concreto, establece el conjunto de reglas que deben ser cumplidas en

---

[6] Devis Echandía, H. (1972). *Teoría general de la prueba judicial* (T. 1). Zavalía.

[7] Sueiro, C. C. (2019). La obtención de prueba digital de la computación de la nube. En H. R. Granero (Ed.), *E-mails, chats, WhatsApp, SMS, Facebook, filmaciones con teléfonos móviles y otras tecnologías* (2.ª ed., pp. 390–391). Albremática (elDial.com).

[8] Procuración General de la Nación. (2016). *Guía de obtención, preservación y tratamiento de evidencia digital* (Res. PGN 756/2016).

el marco de la investigación forense digital para que el tratamiento de la evidencia digital sea apropiado y la misma admisible en el proceso judicial cumpliendo las características ya enunciadas previamente.

Las reglas a las que refiere la norma ISO/IEC 27037:2012 pueden simplificarse en cuatro, a saber:

1. Mínima manipulación de ejemplares originales evitando así la adulteración, modificación o contaminación de la evidencia remitida a estudio;
2. Reportar cada cambio, ante una manipulación de la evidencia inevitable (por ejemplo, al encender un teléfono celular) dicha actividad debe ser documentada indicando el agente que intevino, las razones que motivaron la manipulación y el alcance o extensión del procedimiento empleado;
3. Cumplir con las reglas del tratamiento de evidencia digital, las cuales se han descripto en párrafos anteriores;
4. Finalmente, no exceder el conocimiento propio, esto es, ante un tratamiento de evidencia que excede la capacidad de conocimiento del investigador, solicitar la cooperación de terceros con mayor experiencia o conocimiento en la temática.

Surge de lo estudiado que el tratamiento de la evidencia digital difiere notoriamente del tratamiento de cualquier otro tipo de prueba. Las características particulares del tratamiento al que debe ser sometida la misma no ofrece mayor complejidad e implica que quien la manipula debe hacerlo con especial responsabilidad, un error –que luego mutará a una cadena de errores- puede derivar en la inadmisibilidad probatoria y, con ello, en la falta de sustento a la hipótesis que intentemos acreditar en el proceso.

Expresamente las reglas de buenas prácticas forenses para el tratamiento de la evidencia digital prevén protocolos de actuación para que dicha evidencia sea admitida formalmente y que de este modo se evite la introducción de componentes adicionales en el marco de la investigación que tornen «poco confiable» a la evidencia introducida.

Como consecuencia lógica, la introducción de evidencia poco confiable (sin respetar protocolos de actuación) derivará en una lesión a la garantía del juicio previo y derecho de defensa, toda vez que el imputado en el marco de un proceso penal tiene la facultad de *controlar la prueba de cargo que podrá ser utilizada válidamente en la sentencia.*[9] El fundamento de una sentencia por medios poco confiables o que no se ajusten a técnicas protocolares ni a buenas prácticas, podrá derivar en un pronunciamiento arbitrario con la consecuente condena de un inocente por lo que, el derecho de defensa implica la posibilidad de revisar que la metodología empleada en la producción probatoria sea acorde a la disciplina a la que pertenece la evidencia en estudio.

a. El proceso penal informático ¿Existe anomia procesal respecto a los medios de investigación?

Ahora bien, teniendo en cuenta lo relatado hasta este punto, surge claro un interrogante y es: en el marco de la investigación penal informática, ¿existe, a nivel nacional, un conjunto de normas que regulen el procedimiento de obtención de evidencia digital acorde a las garantías constitucionales y que sea efectivo frente a la prevención del delito informático? La respuesta, entiendo, se inclina por la negativa. Independientemente de los manuales de buenas prácticas, adhesiones protocolares y

[9] Maier, J. B. (2004). *Derecho procesal penal: Fundamentos* (T. I, 2.ª ed.). Editores del Puerto.

resoluciones ministeriales, no contamos con un sistema normativo que regule la investigación en el proceso penal informático y que permita el empleo de programas –aún malicioso - con la finalidad de prevenir y sancionar el delito.

Lo antedicho genera lógica preocupación dado que los inminentes avances tecnológicos a los que nos exponemos como sociedad terminan colisionando con un sistema que podríamos caracterizar como «vetusto» en lo que refiere a recolección y tratamiento de evidencia digital.

Si a lo anterior le adicionamos que las nuevas estructuras delictivas por lo general se desarrollan en un marco en donde se emplean cada vez con mayor regularidad medios digitales para la organización y comisión de los delitos, la investigación penal por parte de los agentes de prevención necesariamente debe modernizarse hacia el empleo de nuevas tecnologías que permitan investigar sin perforar esa barrera que forma el llamado derecho a la intimidad. Piénsese, por ejemplo, en el empleo de programas que permiten simular una IP o incluso ocultarla de los investigadores (por ejemplo, navegador *Tor*[10]), o en aquellos dispositivos que eliminan o bloquean la inform0ación ante reiterados intentos de acceso indebido, o en los diversos algoritmos que simulan actividad distinta a la que en realidad se ejecuta, las probabilidades y situaciones son inimaginables e inagotables.

Pues bien, en el contexto detallado podemos entonces suponer que la inexistencia de normas que regulen este tipo de investigación podría derivar en un serio problema constitucional. Esto es, nuestra constitución nacional en su art. 18 establece los alcances de las garantías constitucionales y los principios que deben regir el proceso entre los que se encuentra el principio de legalidad. Dicho plexo normativo, en el art. 28 indica que «los principios, garantías y derechos reconocidos en los anteriores artículos, no podrán ser alterados por leyes que reglamenten su ejercicio».

Del simple razonamiento deductivo entonces podemos arriesgarnos a suponer que, si las normas vigentes regulan procesos de investigación para épocas en donde los avances tecnológicos no eran tan masivos como los actuales y en donde las tecnologías empleadas no gozaban de la inmediatez y el alcance que tienen hoy, por ejemplo, los teléfonos celulares; ¿qué alternativa –que no atente con aquellos principios, derechos y garantías constitucionales- le queda a un investigador que tiene que valerse de programas o protocolos que no tienen una finalidad preventiva sino, a nuestro modo de ver, que sirven para la etapa ex post, es decir meramente punitiva? El ejercicio de la defensa eficaz en un proceso de recolección de evidencia digital que no sea confiable o empleando métodos poco claros, conforme lo hemos relatado con anterioridad, se vería seriamente afectado.

En esta exposición de interrogantes toman relevancia dos aspectos, por un lado, la confiabilidad de la información obtenida a través de programas determinados y, por el otro, de tratamiento obligado en esta temática, el empleo de malware por parte de los agentes de investigación.

Lo planteado en el párrafo anterior ha sido objeto de tratamiento por la jurisprudencia norteamericana en dos precedentes que, entiendo, resultan de interés para terminar de comprender cómo una regulación normativa en este tema resulta útil y necesaria de cara al proceso penal informático:

[10] Según se indica en el sitio oficial del proyecto Tor, el navegador Tor permite acceder a Internet mediante un sistema de «capas» que garantiza la privacidad del usuario. Este diseño posibilita la navegación sin que la actividad sea monitoreada y sin que queden rastros identificables.

b. United States v. Ocasio (2013)[11]

En el caso el señor Angel Ocasio fue acusado de poseer pornografía infantil en su computadora. Dicho hallazgo se produjo mediante el uso de un programa denominado CPS (*Child Pornography System*, por sus siglas en inglés). El funcionamiento de dicho programa consiste en ubicar material (archivos) relacionado con pornografía infantil en diversas redes e internet.

Haciendo uso del derecho que le confiere la cuarta enmienda, el señor Ocasio solicitó judicialmente que la empresa fabricante del software indicara cómo funcionaba el mismo, ya que los archivos se encontraban en carpetas privadas para las cuales no había otorgado autorización de acceso, violando de este modo los principios de la constitución americana.

La empresa fabricante planteó que no se encontraba obligada a proporcionar dicha información argumentando que se encontraba amparada por el secreto empresarial.

En síntesis, el fallo obligó a la empresa a facilitar dicha información respecto del código fuente del programa bajo protecciones legales que permitan impedir que sea perjudicada comercialmente y amparando el derecho de Ocasio a que se revelen dichos datos a fin de cotejar que el método empleado no implicaba atentar contra sus derechos constitucionales.

La importancia del caso resulta en facilitar –en el marco de la investigación penal informática- datos que permitan identificar si el método de recolección de información resulta confiable y, por otro lado, si ese método lesiona garantías constitucionales.

c. «*Playpen*»[12]. La reforma a la «Regla 41» y el empleo de malware en el acceso transfronterizo de datos.

En lo que es conocido como uno de los casos más relevantes en materia de investigación penal informática, «*Playpen*» viene a sentar precedentes sobre el uso de «malware» por parte de las fuerzas de seguridad quienes, a través del empleo de este tipo de programas maliciosos logran acceder a información que permite identificar a los ciberdelincuentes.

Si bien las autoridades lograban interceptar el intercambio de datos prohibidos, el problema aparecía al momento de identificar el origen de dicha difusión. Por este motivo, lograron –a través de una orden judicial emanada por un Juez del Estado de Virginia- emplear el programa denominado *network investigative technique* (NIT) que permitía identificar el origen del material de difusión.

En cuanto a la modalidad de funcionamiento, el programa permite el ingreso en el dispositivo (sin autorización) de quien se sospecha, con la posibilidad de administrar

[11] *United States v. Ocasio* (No. EP-11-CR-2728-KC, W.D. Tex., 6 de junio de 2013), la Corte del Distrito Oeste de Texas —División El Paso— analizó diversos aspectos vinculados a la investigación de delitos cometidos en entornos digitale.

[12] «Playpen» era una plataforma ubicada en la denominada «deep web» o «dark web», utilizada por redes dedicadas a la producción, distribución y consumo de material de explotación sexual infantil. A partir de su descubrimiento se inició una de las investigaciones más extensas contra estructuras internacionales de pedofilia y tráfico de pornografía infantil. Los hechos relevantes del caso se encuentran detallados en Aboso (2022, pp. 335–336).

todos los sitios y funciones. De este modo, se puede acceder a la totalidad de información de quien consume el material, como de quien lo difunde.

En el caso de marras, las fuerzas de seguridad administraron durante un tiempo considerable la web logrando identificar a una gran cantidad de usuarios (con sus direcciones de IP incluidas). Esto permitió formular cargos criminales contra al menos doscientos usuarios cuyos domicilios escapaban a la jurisdicción del juez que emitió la orden autorizando el uso del «malware», siendo ésta una de las principales aristas del caso y dando lugar a la reforma de la denominada «regla 41»[13].

La «regla 41» permite entonces que un Juez, independientemente del distrito en donde se encuentre, secuestre datos de un dispositivo electrónico sin que las autoridades lo tengan en su poder o en el lugar en que se encuentran. El empleo del malware para acceder de manera remota permitía a los investigadores identificar la IP desde la que se conectaba el usuario y de ese modo, allanando la morada, lograr su aprehensión. El empleo del NIT como plataforma para acceder al sitio e identificar las IP y las órdenes judiciales emanadas en consecuencia fueron objeto de numerosas impugnaciones por parte de los usuarios, las que se concentran en tres: a) falta de jurisdicción del juez federal para emitir la orden que autorizaba el empleo del malware; b) falta de motivación de la medida judicial y c) actuación de buena fe por parte de la autoridad al momento de ejecutar la medida.

Sobre el primer agravio se argumentó que, dado que los usuarios se conectaban desde lugares que no estaban en la jurisdicción del juez de Virginia, la medida carecía de validez, toda vez que la misma FRCP establecía la limitación a la procedencia de órdenes de allanamiento y registro fuera de la propia jurisdicción del magistrado. La respuesta fue una interpretación flexible de la jurisprudencia de la corte americana en el sentido de que la jurisdicción era válida toda vez que lo determinante es el lugar en donde se halla el servidor al cual se conecta el usuario y no el lugar o locación en la que se halla el usuario al momento de conectarse.

En relación al segundo agravio, se argumentó que el criterio de la locación del servidor no siempre se ha utilizado en el caso de los ciberdelitos como los de abuso sexual infantil o distribución de pornografía infantil. El criterio rector en estos casos ha sido el contrario (locación de la conexión de la dirección de IP)

En cuanto al último argumento, los tribunales fundamentaron la validez del procedimiento en el hecho de que la autoridad no actuó de manera deliberada, sino que actuó de buena fe. Se amparó en esto casos en que el agraviado no especificó cuál fue el perjuicio sufrido, y que en el caso no aplicaba la expectativa razonable de privacidad, toda vez que al acceder al intercambio de información con el servidor que proporciona los datos, dicha expectativa se torna difusa. En definitiva, el objetivo de la defensa era lograr la exclusión probatoria argumentando que el empleo de este tipo de programas resultaba en una actuación deliberada por parte de la autoridad y, por ende, la obtención de prueba en este sentido era ilegal.

Sin embargo, tal como refiriera al comienzo del párrafo anterior, los tribunales entendieron que el uso del NIT por parte de las fuerzas de seguridad no quebrantaba la

[13] La «Regla 41» integra el compendio de las reglas federales del procedimiento penal de los Estados Unidos (*Federal Rules of Criminal Procedure*, FRCP). Entre otros aspectos, habilita a los jueces federales a emitir órdenes que permiten a las fuerzas de seguridad acceder de manera remota a equipos informáticos, con prescindencia del lugar físico donde se encuentren.

tutela a garantías judiciales reconocidas por la Cuarta Enmienda, toda vez que las autoridades habrían justificado una causa probable de comisión de delitos y, a través de este tipo de medidas y el empleo de este tipo de programas descubrieron lugares y efectos para secuestrar.

El uso del malware se justificaba porque, tal como lo hemos referido al inicio de este acápite, los ciberdelincuentes hacen uso de herramientas que permiten disuadir a los investigadores y son éstos quienes deben valerse de herramientas similares (muchas de ellas catalogadas como «malware») con la finalidad de prevenir y sancionar la comisión de este tipo de hechos. El uso de estos «programas electrónicos de rastreo facilita la búsqueda y asegura en gran medida la posibilidad de identificar al cibernauta»[14]

De lo estudiado hasta aquí podemos advertir que, si bien no se encuentra exenta de críticas el compendio de reglas federales del procedimiento penal se encarga de reglamentar cómo debe procederse en investigaciones vinculadas con evidencia digital, amoldándose así a los avances tecnológicos sin dejar de lado la tutela a garantías constitucionales reconocidas por la cuarta enmienda. Con similar criterio y un carácter funcional, entiendo que resulta prioritario contar con una regulación procesal que permita tratar el uso de este tipo de programas en el proceso penal con el alcance suficiente para que su empleo no implique una lesión a principios constitucionales.

También comprendemos que no todo es válido (ni siquiera la buena fe del funcionario) en el marco de una investigación judicial, y si bien producto de ello podría obtenerse evidencia que resulte en el descubrimiento de la comisión de un hecho delictivo, sea de manera preventiva o con el fin de iniciar un proceso penal, la norma está escrita y forma parte de nuestro Estado; no podemos so pretexto de prevenir el delito, actuar sin miramientos de la norma constitucional, por ello es necesaria una regulación clara y contundente para que el «debido proceso» como garantía no se vea alterado por la finalidades indicadas.

4. Metadatos e información asociada: conceptualización, criterios para su incorporación al proceso penal y exigencia de orden judicial previa conforme al Código Procesal Penal Federal

Al momento de definir qué entendemos por «metadatos» o «información asociada», no podemos pasar por alto el contexto en el que nos encontramos. Tal como hemos venido remarcando a lo largo de este trabajo, la era digital ampliamente caracterizada por el gran cúmulo de información que se almacena en los dispositivos electrónicos, forma parte fundamental de la vida cotidiana.

En este escenario, cada vez más influenciado por tecnologías (en uso y nuevas) resulta interesante ingresar en el estudio de cómo se procesa esa información y cómo la misma puede incluirse en la investigación penal informática. Ello es así porque las nuevas tecnologías implican, a la vez que mayores comodidades para los quehaceres cotidianos –sean personales, laborales o financieros- la aparición de nuevas formas de delito.

[14] Aboso, G. E. (2023). *Evidencia digital en el proceso penal: La investigación forense en el entorno digital y la validez de las garantías constitucionales*. Euros Editores SRL.

Los metadatos o información asociada vienen a formar parte de la información que se «asocia» a un elemento determinado, de allí el término «información asociada» o «datos asociados». En este sentido son variadas y numerosas las definiciones sobre metadatos que, por lo general, se resumen en el adagio «datos sobre datos»; aunque la definición resulta más amplia y variada, tal como afirma Mayernik[15]:

> […] se ofrece un puñado de definiciones de metadatos que ilustran como pueden ser desde muy específicas hasta muy genéricas: Greenberg (2003, p. 1876): «datos estructurados sobre un objeto que posibilitan funciones asociadas al objeto designado». Greenberg (2005, p. 20): «atributos de datos que describen, aportan contexto, indican la calidad, o documentan características de otro objeto (o dato)». Smiraglia (2005, p. 2): «descripciones estructuradas de recursos de información, diseñadas para potenciar la recuperación de información». Gilliland (2008, n.p.): «la suma total de lo que se puede decir de cualquier objeto informativo a cualquier nivel de agregación». Pomerantz (2015, p. 26): «Los metadatos son declaraciones sobre un objeto potencialmente informativo».

De lo expuesto entonces concluimos que pese a ser variadas las definiciones los metadatos o información asociada o datos asociados son aquellos elementos que aportan información sobre un contenido (objeto) informativo. También surge que las definiciones son infinitas y no es objeto de este trabajo el ingresar en conceptualizaciones sumamente científicas o específicamente destinadas a áreas puntuales, sino brindar una aproximación a qué debemos entender cuando nos referimos a metadatos o datos asociados.

Pues bien, a modo de ejemplo podríamos decir que, respecto de una llamada telefónica el objeto o contenido propiamente dicho será la comunicación entre los interlocutores y, los datos asociados o información asociada serán los datos aportados por la prestadora de servicios de telefonía que permitan identificar los abonados, fecha, hora y duración de la llamada y hasta la ubicación de cada abonado; lo mismo ocurrirá, por ejemplo, en el caso de direcciones de IP para conexiones a determinados sitios de la web, en donde la dirección de IP contendrá, como dato asociado, domicilio, ubicación, tiempo de conexión, entre otros, del usuario.

Entonces, para recapitular, ¿cómo debe o puede incorporarse esa información al proceso penal informático a fin de evitar el quebrantamiento de garantías como la inviolabilidad de las comunicaciones, el derecho a la privacidad, entre otras? ¿Es necesario contar con una orden determinada?

En nuestro país, tal como se afirmado en puntos anteriores, no contamos con una norma específica que establezca cuál es el modo en que deben o pueden obtenerse los metadatos; la denominada anomia procesal afecta en este punto a la investigación penal y termina por limitar el contenido de la información que puede obtenerse al registro de comunicaciones telefónicas en una norma cuanto menos cuestionable[16].

En efecto, la norma procesal nada dice respecto a la obtención de datos asociados a dichas comunicaciones ni cuál es el alcance de las facultades de la acusación en este punto. Lo hemos expuesto ya, la doctrina entiende que la información contenida en dichas

[15] Mayernik, M. (2020). *Metadata*. In B. Hjørland & C. Gnoli (Eds.), *Encyclopedia of Knowledge Organization* (Version 1.0, published 2020-03-16; last edited 2020-12-23). ISKO. https://www.isko.org/cyclo/metadata

[16] El artículo 236 del Código Procesal Penal de la Nación (Ley 23.984) autoriza al juez, mediante auto fundado, a disponer la intervención de las comunicaciones telefónicas del imputado «para impedirlas o conocerlas». Asimismo, faculta al Ministerio Público Fiscal a adoptar la misma medida en casos de urgencia, con la sola obligación de comunicar su realización al magistrado instructor.

comunicaciones goza de protección constitucional, ergo, toda intervención de dicha información debe ser sustentada en una orden judicial emanada de autoridad competente, en este caso, el magistrado instructor.

Ahora bien, la doctrina (y jurisprudencia) no son uniformes en cuanto a la protección que debe brindarse a la información asociada y, por ende, cómo debe introducirse al proceso penal.

En el caso *Mitchell*, la Cámara Federal de Casación Penal entendió que los datos asociados a las comunicaciones telefónicas realizadas por el imputado gozan de protección constitucional ya que el derecho a la intimidad no se limita sólo al contenido *per se* de la comunicación, sino también a los datos asociados a la misma.

Entendemos que en el caso *Halabi*, está la respuesta sobre el alcance constitucional que debe otorgarse a los metadatos y radica en la fuente de la norma que es de carácter constitucional y por tal motivo el proceso penal no puede apartarse de dicha protección.

Si consideramos lo previsto en el código procesal penal federal (ley 27.063 y sus modificatorias) el panorama resulta tajante. En una concepción que interpreto más antropocéntrica la intimidad, así como la privacidad del individuo sólo pueden verse afectadas en el marco de un proceso penal cuando medie orden judicial.

En su art. 13 el CPPF determina que

> Se debe respetar el derecho a la intimidad y a la privacidad del imputado y de cualquier otra persona, en especial la libertad de conciencia, el domicilio, la correspondencia, los papeles privados y las comunicaciones de toda índole. Sólo con autorización del juez y de conformidad con las disposiciones de este Código podrán afectarse estos derechos.

Entiendo necesario detenernos en la frase «comunicaciones de toda índole» ya que abarca no solo comunicaciones telefónicas, sino a aquellas de cualquier tipo que, jurisprudencialmente son asimiladas a la protección prevista en art. 19 de nuestra carta magna en tanto «nadie puede ser objeto de injerencias arbitrarias en su vida privada, ni la de su familia, en su domicilio o su correspondencia»[17]

Una interpretación global de la norma analizada en conjunto con principios rectores del proceso penal constitucional, nos permiten concluir en que la expectativa razonable de privacidad, así como el principio de autodeterminación de los individuos, limitan la injerencia del estado en las comunicaciones de los individuos y ello no se cierne únicamente a las comunicaciones de índole telefónica, sino a todo tipo de actividad sobre la que el individuo posea una expectativa razonable de privacidad. Será el Estado en conjunto con las empresas prestatarias de estos servicios quienes deberán arbitrar los medios para que la proporción de información asociada sea efectuada respetando estandartes locales y supranacionales

5. Conclusiones

La evidencia digital ha tomado una enorme trascendencia en el marco del proceso penal informático, aunque no sólo ajustada a delitos cibernéticos o «ciberdelitos». En los tiempos actuales el empleo de dispositivos electrónicos de almacenamiento de datos es prácticamente unánime y se aplica a todos los aspectos de la vida cotidiana por lo que,

[17] Corte Suprema de Justicia de la Nación. (2010). *Quaranta, José Carlos s/ infracción Ley 23.737* (Fallos 333:1674).

podemos afirmar sin lugar a dudas que la vida de la persona –inclusive las relaciones intersubjetivas- se ve atravesada y reflejada por los datos que se almacenan en dichos dispositivos.

A lo largo del artículo hemos brindado una pequeña introducción a un tema que trasciende fronteras y que posee múltiples aristas pero que, sobretodo, se caracteriza por su actualidad.

En este escenario, no podemos desentendernos de la complejidad que reviste la evidencia digital y cómo resulta imperioso dotar de integridad y autenticidad a la misma a lo largo del proceso penal, lo que se traducirá en el respeto a garantías constitucionales y a un ejercicio óptimo de la judicatura. Sin embargo, carecemos actualmente de un plexo normativo ritual que regule específicamente el derecho penal informático y cómo el Estado debe gestionar este tipo de evidencia. Escuchas, imágenes de video, fotografías, movimientos bancarios, correspondencia electrónica, datos de navegación, entre miles de otras pruebas carecen de un andamiaje normativo acorde, actualizado a los tiempos que corren quedando prácticamente desprotegidos en un claro «atentado» contra la ritualidad y seriedad que caracteriza al proceso penal, pero también contra el imputado y con la sociedad toda que delega en manos del Poder Judicial la tutela de los derechos y garantías consagrados.

Es este el gran dilema del derecho penal contemporáneo al que la legislación y el servicio de justicia deben enfrentarse con el fin de resultar funcionales a la sociedad sobre la que rigen.

6. Bibliografía

Aboso, G. E. (2023). *Evidencia digital en el proceso penal: La investigación forense en el entorno digital y la validez de las garantías constitucionales*. Euros Editores SRL.

Bujosa Vadell, L. M., Bustamante Rúa, M. M., & Toro Garzón, L. O. (2021). La prueba digital producto de la vigilancia secreta: Obtención, admisibilidad y valoración en el proceso penal en España y Colombia. *Revista Brasileira de Direito Processual Penal*, 7(2), 1347–1384.

Casey, E. (2004). *Digital evidence and computer crime: Forensic science, computers, and the Internet*. Academic Press.

Código Procesal Penal de la Nación (Ley 23.984).

Código Procesal Penal Federal (Ley 27.063 y mod.).

Corte Suprema de Justicia de la Nación. (2010). *Quaranta, José Carlos s/ infracción Ley 23.737, causa N.º 763* (Fallos 333:1674).

Devis Echandía, H. (1972). *Teoría general de la prueba judicial* (T. 1). Zavalía.

Maier, J. B. (2004). *Derecho procesal penal: Fundamentos* (T. I, 2.ª ed.). Editores del Puerto

Ministerio Público Fiscal & Ministerio de Seguridad. (2023). *Protocolo para la identificación, recolección, preservación, procesamiento y presentación de evidencia digital*. https://www.fiscales.gob.ar

Mayernik, M. (2020). Metadata. *Knowledge Organization*, 47(8), 696–713. https://doi.org/10.5771/0943-7444-2020-8-696

Mayernik, M. (2023). *Metadatos* (S. S. Miralles, Trad.). *Anales de Documentación*, 26. Universidad de Murcia. (Traducción de la entrada publicada en la Encyclopedia of Knowledge Organization.)

Procuración General de la Nación. (2016). *Guía de obtención, preservación y tratamiento de evidencia digital* (Res. PGN 756/2016).

Sosa, M. E. (2023). *Evidencia digital: Su importancia en la investigación*. Revista Pensamiento Penal, (466), 1

Sueiro, C. C. (2019). La obtención de prueba digital de la computación de la nube. En H. R. Granero (Ed.), *E-mails, chats, WhatsApp, SMS, Facebook, filmaciones con teléfonos móviles y otras tecnologías* (2.ª ed., pp. 390–391). Albremática (elDial.com).

United States v. Ocasio, No. EP-11-CR-2728-KC (W.D. Tex. June 6, 2013).