ESPECIALIZACIÓN EN CIBERCRIMEN

Trabajo Final

Vulneración del derecho a la intimidad en el análisis forense de dispositivos móviles

Mazur Mansur Nahir Carolina

28.860.936

Legajo ECB000118

Rosario, septiembre 2024

Tabla de contenido

Resumen

El presente trabajo final aborda el análisis forense de dispositivos móviles y su impacto en el derecho a la intimidad. En un contexto donde la eficiencia en la investigación judicial debe equilibrarse con la protección de los derechos fundamentales, el análisis forense de datos recuperados de teléfonos inteligentes y tabletas plantea un desafío significativo. Este trabajo examina el dilema entre la obtención de evidencia digital y la protección del derecho a la privacidad, subrayando que las prácticas actuales pueden vulnerar este derecho fundamental.

La creciente sofisticación de herramientas forenses permite a los peritos acceder y analizar una vasta cantidad de información sensible almacenada en dispositivos móviles. Sin embargo, la obtención y el uso de estos datos deben alinearse con principios de legalidad, limitación de la finalidad, exactitud, seguridad y confidencialidad, respetando tanto a los imputados como a terceros cuyo contenido personal pueda estar involucrado.

La hipótesis central del trabajo es que el análisis forense de datos de dispositivos móviles, utilizando herramientas como UFED, puede comprometer el derecho a la intimidad. Se utilizan argumentos en pos de demostrar que la falta de normativas específicas sobre la recolección y manejo de evidencia digital puede llevar a abusos y vulneraciones de derechos.

El estudio concluye con la necesidad de un marco normativo robusto que contemple la proporcionalidad y la transparencia en el acceso a datos digitales, garantizando así el respeto a la privacidad y la integridad del proceso penal. Además, se resalta la importancia de la capacitación continua para los operadores judiciales y la actualización constante de las normativas.

Palabras claves: evidencia digital. Análisis forense. Dispositivos móviles. Intimidad. Herramientas forenses. Regulación legal.

Abstract

This final work addresses the forensic analysis of mobile devices and its impact on the right to privacy. In a context where efficiency in judicial investigation must be balanced with the protection of fundamental rights, forensic analysis of data recovered from smartphones and tablets poses a significant challenge. This work examines the dilemma between obtaining digital evidence and protecting the right to privacy, highlighting that current practices can violate this fundamental right.

The increasing sophistication of forensic tools allows experts to access and analyze a vast amount of sensitive information stored on mobile devices. However, the obtaining and use of this data must be aligned with principles of legality, limitation of purpose, accuracy, security and confidentiality, respecting both the accused and third parties whose personal content may be involved.

The central hypothesis of the work is that forensic analysis of data from mobile devices, using tools such as UFED, can compromise the right to privacy. Arguments are used to demonstrate that the lack of specific regulations on the collection and handling of digital evidence can lead to abuses and violations of rights.

The study concludes with the need for a robust regulatory framework that contemplates proportionality and transparency in access to digital data, thus guaranteeing respect for privacy and the integrity of the criminal process. In addition, the importance of continuous training for judicial operators and constant updating of regulations is highlighted.

Keywords: digital evidence. Forensic analysis. Mobile devices. Privacy. Forensic tools. Legal regulation.

Introducción

El tema seleccionado para este trabajo final se encuentra dentro de los propuestos en el área "C-Evidencia Digital-Informática Forense-Análisis forense de dispositivos móviles: cómo recuperar datos de teléfonos inteligentes y tabletas para su uso en investigaciones judiciales."

La eficiencia y eficacia en las investigaciones judiciales es un objetivo fundamental para el sistema de justicia. Sin embargo, este objetivo debe ser balanceado cuidadosamente con la protección del derecho fundamental a la intimidad de los ciudadanos. El análisis forense de los datos recuperados de dispositivos móviles plantea un dilema entre estos dos principios que merece un análisis profundo.

El tratamiento y la regulación de la evidencia digital es uno de los mayores desafíos para el derecho penal y procesal penal en la actualidad. Estas técnicas pueden ser cruciales para esclarecer hechos delictivos, pero también conllevan el riesgo de vulnerar el derecho a la privacidad consagrado en la Constitución Nacional y en los Tratados Internacionales de Derechos Humanos. Dentro de la evidencia digital, hay un subtipo de evidencia, y es aquella que surge de los dispositivos móviles. Fotos, videos, contactos, lugares visitados, registro de llamadas, mensajes, incluso borrados, resúmenes bancarios, correos electrónicos, notas personales, contraseñas y aplicaciones de todos los tipos es parte de lo que podemos encontrar en un celular, es decir, concentran una gran cantidad y diversidad de información personal y sensible, incluyendo datos de terceros (amigos, familia, compañeros de trabajo).

Hace tiempo se está desarrollando una industria que vende herramientas para que los/las peritos y auxiliares de la justicia accedan y analicen de forma eficiente la información de los teléfonos móviles. Es por ello que se requiere que estas prácticas mediante las cuales se llevan adelante las tareas de extracción y análisis de datos, así como la normativa que permite incorporarlas en un proceso judicial, sean respetuosas de las garantías de las personas. Tales

prácticas deben adecuarse a principios tales como legalidad, limitación de la finalidad, exactitud y calidad, conservación limitada, seguridad de los datos y confidencialidad. Es importante que estas garantías se apliquen a las personas imputadas y a los terceros cuya información también se encuentra en sus celulares con el fin de que se respete su derecho a la intimidad.

La vulneración del derecho a la intimidad en el análisis forense de dispositivos móviles es un problema serio que plantea preocupaciones legales y éticas. Esto ocurre porque los ciudadanos tienen expectativa razonable de privacidad, los dispositivos móviles contienen una gran cantidad de información sensible, por ello los usuarios generalmente tienen este criterio en relación con sus dispositivos, ya que son considerados extensiones de su vida privada.

Los datos personales no solo de la persona investigada sino también de terceros que pueden no tener ninguna conexión con la actividad criminal investigada. La obtención y retención de esta información puede ser considerada una intromisión innecesaria y desproporcionada en la vida privada de los individuos.

En muchas oportunidades los usuarios de dispositivos móviles no están informados ni han dado su consentimiento para que sus datos sean extraídos y examinados exhaustivamente.

Existe un riesgo inherente de abuso de los datos personales extraídos durante el análisis forense. Si no se maneja adecuadamente, esta información podría ser utilizada indebidamente, vendida o filtrada, lo que podría tener graves consecuencias para la privacidad y seguridad de los individuos afectados.

Algunas técnicas utilizadas en el análisis forense de dispositivos móviles pueden resultar invasivas y violar la intimidad de las personas. Estos métodos pueden incluir la recuperación de datos borrados, la decodificación de contraseñas y el acceso a información encriptada. Si

bien pueden ser justificados en ciertos casos, también plantean preocupaciones sobre los límites y el alcance de la intervención en la privacidad.

Este trabajo se centra en la hipótesis de que el análisis de la información de un dispositivo móvil, extraída mediante herramientas forenses, vulnera el derecho a la intimidad. En línea con esta premisa, el objetivo general es analizar si las investigaciones judiciales llevadas a cabo por el Estado, al emplear herramientas como UFED para el análisis forense de dispositivos móviles, comprometen el derecho a la intimidad.

Para abordar esta problemática, se examinarán los desafíos que presenta la prueba en entornos digitales, desde su recopilación hasta su análisis, explorando los métodos y herramientas utilizados en el análisis forense de dispositivos móviles. Asimismo, se realizará una comparación de los protocolos, normas y jurisprudencia vinculados a esta práctica, con el objetivo de evidenciar la importancia de que dichas actividades respeten las garantías tanto de los imputados como de los usuarios de teléfonos móviles. Además, se subrayará la necesidad urgente de promulgar una legislación que regule de manera exhaustiva la evidencia digital.

La importancia del trabajo planteado radica en que se aborda un tema de gran actualidad y relevancia social. El uso cada vez mayor de dispositivos móviles y la creciente dependencia de los mismos para almacenar información personal hacen que el análisis forense de estos dispositivos sea una práctica cada vez más común para la persecución de delitos y la búsqueda de la justicia.

Es necesario contribuir al conocimiento y debate sobre un tema tan complejo, que carece de regulación específica en nuestro país, ya que si no se aborda de manera adecuada el dilema entre eficiencia investigativa y protección de derechos en el análisis forense de datos de dispositivos móviles, las situaciones a mediano y largo plazo podrían incluir una mayor vulneración de los derechos a la intimidad, un aumento en los abusos de los datos obtenidos,

e incluso planteos por parte de los defensores de los derechos individuales en busca de proteger y garantizar la privacidad de las personas.

El análisis de la evidencia digital y su impacto en la privacidad se articula en varios capítulos que abordan distintos aspectos del tema. En el primer capítulo se proporciona una visión general de la evidencia digital, incluyendo su definición, características y relevancia en el contexto judicial. Se exploran los desafíos técnicos y legales asociados con la autenticidad e integridad de la evidencia digital, así como las herramientas forenses más utilizadas, como el UFED, y los métodos de extracción de datos, como las técnicas física, lógica y chip-off.

En el capitulo dos se examina la intervención estatal y la regulación de la evidencia digital, abordando la evolución del derecho procesal penal y la necesidad de equilibrar la recolección de pruebas digitales con la protección de los derechos fundamentales. Se analiza la normativa internacional, como el Convenio sobre Ciberdelincuencia y la Resolución N° 68/167 de la ONU, también se hace referencia a la regulación de la evidencia digital fragmentada en los distintos códigos procesales penales provinciales y federales de nuestro país.

En el capitulo tres se examina la protección de la privacidad en el contexto de la recolección de datos personales y cómo las normativas internacionales y locales abordan estos desafíos. Se discute la interacción entre la libertad probatoria y la protección de la intimidad, y se analiza cómo se equilibran estos intereses en la práctica judicial.

En el anexo se presentará una revisión de la jurisprudencia relevante en materia de evidencia digital, explorando fallos nacionales e internacionales que reflejan la evolución de la regulación y los desafíos asociados con el acceso a datos digitales.

Para abordar la hipótesis utilicé un enfoque metodológico cualitativo. Se recolectaron datos de fuentes primarias y secundarias mediante una revisión exhaustiva de literatura académica, artículos científicos y publicaciones relevantes en el campo del derecho a la intimidad y el

análisis forense de dispositivos móviles. Se analizaron leyes y protocolos aplicables a la privacidad, la protección de datos y el análisis forense, y se acompañaron fallos judiciales que ilustran los problemas que surgen en torno a la evidencia digital.

La investigación se clasifica como explicativa, y su propósito es demostrar la necesidad de modificar las prácticas de extracción forense en dispositivos móviles para respetar el derecho a la intimidad. Se abordará el problema de la falta de tratamiento doctrinario y precedentes jurisprudenciales específicos en Argentina, y se buscará respaldar la hipótesis con bibliografía relevante, así como con información obtenida de charlas, simposios y congresos especializados en la materia.

La viabilidad de la investigación está garantizada por la disponibilidad de diversas fuentes de información confiables y relevantes, como nuestra Constitución Nacional, tratados internacionales como la Convención Americana sobre Derechos Humanos y la Convención de Cibercriminalidad del Consejo de Europa, proyectos de ley y reformas en materia de protección de datos y evidencia digital, normas técnicas y protocolos de actuación, entre otros.

Capítulo 1: Nociones generales de la evidencia digital

El avance tecnológico ha transformado profundamente la manera en que se desarrollan las investigaciones judiciales, introduciendo la evidencia digital como un componente clave en la búsqueda de justicia. La evidencia digital, que comprende cualquier información de valor probatorio almacenada o transmitida en formato digital, se ha convertido en un elemento esencial en los procesos penales y civiles, siendo utilizada para esclarecer hechos, identificar responsables y fundamentar decisiones judiciales.

Este capítulo se centra en proporcionar una comprensión básica de la evidencia digital, explorando su definición, características y relevancia en el contexto judicial. A través de una

revisión de los principales desafíos asociados con la recopilación y el examen de esta prueba, se destacan los aspectos técnicos y legales que pueden influir en su autenticidad e integridad. Además, se ofrece una descripción detallada de las herramientas forenses más utilizadas en el análisis de dispositivos móviles, como el UFED, y se analizan los métodos empleados para la extracción de datos, como las técnicas física, lógica y chip-off.

La comprensión de estas nociones generales es esencial para situar el uso de la evidencia digital en el contexto jurídico, ya que establece el fundamento para evaluar no solo su valor probatorio, sino también los desafíos y consideraciones legales que surgen en su aplicación en los procesos judiciales.

Definición y características de la evidencia digital

Aún no se ha establecido una definición normativa de evidencia digital en las legislaciones procesales. Sergi (2018) sostiene que este vacío ha sido abordado por diversos organismos que han desarrollado propuestas basadas en las características distintivas de la evidencia digital, la Guía de Prueba Electrónica del Consejo de Europa emplea la definición de que 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 Organización Internacional de Evidencia Computacional -IOCE- la definió en el 2000 como toda información generada, almacenada o transmitida a través de medios electrónicos que puede ser utilizado en una corte judicial, la organización Grupo de Trabajo Científico sobre Evidencia Digital -SWGDE- lo hizo como información de valor probatorio almacenada o transmitida en forma digital.(p.3)

En el ámbito del CommonLaw, Casey (2005), sostuvo que 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. (p.12)

Delbono (2018) considera que una evidencia digital es un elemento almacenado en un medio digital. Sin embargo, una definición más precisa sería cualquier información que, aunque esté sujeta a intervención humana, no ha sido extraída de una computadora. Para que la evidencia digital sea útil, debe ser legible o interpretable por personas expertas, a menudo con la ayuda de un programa de computadora. Las características fundamentales de la evidencia digital incluyen su volatilidad, anonimato, capacidad de duplicación, alterabilidad, modificabilidad y eliminabilidad. Estos aspectos son cruciales en el contexto de un análisis forense.(p.160)

La evidencia digital es, en realidad, un subgrupo de la evidencia electrónica, un concepto más amplio, aunque a menudo se utilizan ambos términos de manera indistinta. La evidencia electrónica abarca datos analógicos, como fotos, audios o videos, que pueden ser digitalizados y convertirse en formatos digitales, aunque originalmente no lo eran.

Por esta razón, algunos autores prefieren centrarse en el concepto más inclusivo de evidencia electrónica, que comprende tanto los datos analógicos como digitales que adoptan un formato digital. Este enfoque abarca cualquier dato en formato digital que sea creado, manipulado, almacenado o comunicado por dispositivos o sistemas informáticos, o transmitido a través de sistemas de comunicación, y que sea relevante para un proceso judicial. (Salt, 2017)

En nuestro país la distinción entre evidencia tradicional y digital se menciona en los considerandos de la Resolución la 234/16, Protocolo General en la Investigación y proceso de recolección de pruebas en ciberdelitos, 2019

> Que la prueba digital se diferencia de la prueba tradicional por su volatilidad, la capacidad de duplicación de la misma, la facilidad para alterarla y la cantidad de meta-datos que posee.
>
> Que la investigación de la delincuencia informática se dificulta debido a la

intangibilidad y volatilidad de la evidencia digital, por lo que su adecuada preservación es fundamental para que las mismas sean admitidas judicialmente. Que la prueba digital, en su estado natural, no permite entrever qué información es la que contiene en su interior, por lo que resulta para ello ineludible, examinarla a través de instrumentos y procesos forenses específicos.

Que la prueba digital es fundamental para la investigación por la información y datos de valor que pueden extraerse de los distintos dispositivos electrónicos, tanto aquellos aportados por el denunciante como los que se encuentren en el lugar de allanamiento. Que dicha prueba puede ser en ciertos delitos de extrema preponderancia y en algunos casos, la única evidencia que se puede obtener para el esclarecimiento del delito investigado.

Que la adecuada obtención, conservación y tratamiento de la evidencia digital es un elemento clave para asegurar el éxito de las investigaciones.

Que las Fuerzas de Seguridad y Policiales deben estar capacitadas para operar con prueba digital teniendo en cuenta su fragilidad ya que las altas temperaturas, la humedad y cualquier error en su manejo puede acarrear la destrucción de la misma. Que incluso el valor de las pruebas obtenidas con el mayor esmero puede perderse si no se respeta debidamente la cadena de custodia, las precauciones especiales al momento de recolectar, manipular, documentar y examinar la evidencia digital ya que de no hacerlo, podrían generarse nulidades judiciales o resultar imprecisa a efectos de esclarecer el hecho delictivo.

Que es necesario asistir y capacitar a las Fuerzas de Seguridad y Policiales dado que son las encargadas de auxiliar en la investigación de estos delitos, y que dicha investigación requiere de una experiencia, herramientas y actuación distinta que en los

delitos convencionales.

Que es fundamental que las Fuerzas de Seguridad y Policiales sean capaces de reconocer qué tipo de dispositivos pueden contener información vital para la investigación del delito para su posterior secuestro.

Sain (2012) observa que la evidencia digital, al igual que las huellas dactilares y el ADN, se caracteriza por su volatilidad. También resalta la fragilidad de esta evidencia, que puede deteriorarse con el tiempo dependiendo del medio en el que esté almacenada, y que es susceptible a alteraciones, daños, destrucción o eliminación. El autor destaca que, a diferencia de la criminalística tradicional, las investigaciones que involucran computadoras requieren métodos no convencionales de búsqueda (p.110).

Simian (2023) sostiene que Molina Quiroga identifica características similares de la evidencia digital, subrayando que esta puede encontrarse tanto en los medios como en los dispositivos de almacenamiento. Además, el autor destaca que la evidencia digital, a diferencia de la tradicional, contiene una gran cantidad de metadatos. Estos incluyen datos que pueden ser fácilmente obtenidos con herramientas comunes, pero también información adicional, como archivos borrados, renombrados u ocultos, que solo pueden recuperarse mediante el uso de herramientas forenses especializadas. Los procesos de almacenamiento y eliminación de datos, el acceso a internet, la ejecución de impresiones e incluso el sistema operativo de la computadora son fuentes valiosas de metadatos. El autor expone que en la misma línea Sueiro, subraya no solo la importancia de los metadatos en la evidencia digital, sino también el mayor grado de certeza probatoria que esta ofrece. Además, resalta que la evidencia digital es transfronteriza, intangible y latente, ya que requiere de programas específicos para ser interpretada, y que, en comparación con la prueba tradicional, presenta un mayor nivel de fiabilidad. (p.94-95)

Además de las características y diferencias previamente mencionadas, Sergi (2018) menciona que el documento sobre el tratamiento de la evidencia digital del Consejo de Europa también aborda la creciente capacidad de almacenamiento y el bajo costo económico que significa han llevado a un aumento significativo en el volumen de documentos digitales. Aunque existen herramientas informáticas que facilitan la búsqueda automatizada, identificar la evidencia relevante en un dispositivo que puede almacenar millones de documentos sigue siendo un desafío logístico considerable para los investigadores. Además, esto puede afectar las garantías individuales al aumentar el riesgo de encontrar información que no está directamente relacionada con el objeto de prueba que motivó la medida.

La evidencia digital puede ser copiada sin limitaciones, ya que, al realizar la operación de manera correcta y con las herramientas adecuadas, lo que se obtiene no son simples copias, sino clonaciones exactas que conservan todas las características del original. El contenido digital puede ser replicado infinitamente y mantenerse idéntico al original. Este atributo permite crear múltiples copias exactas que pueden ser distribuidas y examinadas por diferentes especialistas simultáneamente (por ejemplo, se puede proporcionar una copia bit a bit a la defensa para su propia pericia). De este modo, una adecuada obtención de la evidencia digital asegura que todas las medidas sean actos de prueba reproducibles desde una perspectiva procesal. (p.4-5)

Dentro de las características de la evidencia digital cabe mencionar que es transversal a todos los delitos, ya que no es patrimonio exclusivo de los delitos informáticos, trasciende los mismos y se extiende hacia cualquier tipo de delito de los ya conocidos por todos. En este sentido, señala González-Cuellar Serrano (2008) que cualquier infracción penal es susceptible de ser investigada y probada gracias a la obtención de información digitalizada. El autor menciona como ejemplo al joven agresivo que registra en video, con su teléfono

móvil, la violenta golpiza que le da a un mendigo. Aunque no es un ciberdelincuente, genera datos digitales que documentan el acto delictivo (p. 151).

La evidencia también puede transmitirse transfronterizamente, de manera veloz y sencilla, tiene la facilidad de ser enviada de un país al otro en cuestión de segundos. Consta de archivos digitales (impulsos eléctricos), puede ser fácilmente duplicada -clonada- y transmitida a la velocidad de la luz por las redes.

Frente a la posibilidad de que la evidencia digital atraviese las fronteras de los países en cuestión de segundos, en esta materia, es fundamental la cooperación internacional entre los Estados. En este sentido, Dupuy (2021) expresa que una importante particularidad del fenómeno digital es la transnacionalidad, la ubicuidad. El autor del hecho puede encontrarse en un lugar, las víctimas distribuidas en diferentes países y la evidencia digital que se necesita para comprobar uno de los aspectos de la teoría del caso de cualquiera de las partes, puede estar alojada en un servidor en otra ciudad, o bien los datos pueden estar fragmentados y ubicados en diferentes servidores en varios Estados. Los límites o fronteras se vuelven difusos entre la comisión del evento delictivo y su resultado, debilitándose el tradicional principio de territorialidad y soberanía nacional. En razón de ello, explica que es fundamental profundizar los mecanismos de cooperación internacional entre los Estados. (p.43)

Proceso del análisis forense: recopilación, análisis, presentación y preservación de la evidencia

Según Semprini (2017) en los últimos años, se han mejorado los procedimientos no solo para el secuestro de dispositivos tecnológicos en la escena del crimen, sino también en las técnicas forenses utilizadas para analizar la evidencia digital. Durante una investigación, es crucial comprender los conceptos y emplear los términos adecuados para determinar el rol que tienen los componentes o sistemas informáticos, lo que influye en el tipo de análisis que se realizará

para obtener indicios y, posteriormente, las pruebas necesarias que respalden las hipótesis del caso. Con este fin, se categorizan las pruebas para distinguir entre el hardware y la información contenida en él, conocida como evidencia electrónica y digital respectivamente. Esta distinción facilita el diseño de metodologías y procedimientos adecuados para manejar y estudiar cada tipo de evidencia, logrando un paralelismo entre el escenario físico y el entorno digital. Es esencial prestar atención a los procedimientos de recopilación y almacenamiento de evidencias en la escena del delito y asegurar la cadena de custodia, aplicando métodos que eviten alteraciones y permitan la reproducción por terceras partes en cualquier momento.

Para lograr esto, los especialistas en informática forense basan sus investigaciones en normas y guías de buenas prácticas, como las RFC (Request for Comments) e ISO (International Organization for Standardization). Las evidencias digitales están surgiendo en nuevos dispositivos tecnológicos que desafían los procedimientos actuales, por lo que los informáticos forenses deben entender y adaptarse a la tecnología para interpretar correctamente la evidencia digital. (p.91)

La RFC 3227 "Guidelines for Evidence Collection and Archiving" es una guía esencial en informática forense que establece recomendaciones para la recolección y preservación de evidencia digital. Publicada por el IETF en 2002. Es uno de los primeros documentos adoptados por la comunidad de informática forense, ofreciendo una serie de buenas prácticas para evaluar la volatilidad de los datos, decidir qué recolectar, cómo realizar la recolección, y cómo almacenar y documentar la información. La RFC 3227 aborda de manera limitada los aspectos legales, ya que estos dependen del marco jurídico específico de cada país. Esta RFC sigue siendo una referencia clave en protocolos forenses modernos.(Di Iorio, 2016).

A principios de 2012, la organización ISO publicó el estándar ISO/IEC 27037:2012 "Guía para la identificación, recolección, adquisición y preservación de evidencias digitales" fue el

primer estándar ISO enfocado exclusivamente en la recolección y resguardo de evidencias digitales, estableciendo normas y buenas prácticas generales. Proporciona directrices para identificar, recopilar y preservar evidencias digitales de dispositivos como teléfonos móviles, tarjetas de memoria, sistemas de navegación GPS, cámaras digitales, redes TCP/IP, entre otros. La norma se centra en tres principios fundamentales de la evidencia digital:

- Relevancia: es una condición técnicamente jurídica. Se refiere a la pertinencia de la evidencia en relación con los hechos investigados, excluyendo lo irrelevante.
- Confiabilidad: asegura que la evidencia pueda ser reproducida y verificada por terceros, garantizando la repetibilidad y auditabilidad del proceso.
- Suficiencia: se relaciona con la completitud de las pruebas recolectadas, asegurando que se tengan suficientes elementos para sustentar las hipótesis del caso investigado.

La norma ISO/IEC 27037:2012 no cubre los procedimientos legales, disciplinarios u otras acciones relacionadas con el manejo inadecuado de la evidencia digital. Su aplicación requiere el cumplimiento de las leyes, normas y reglamentos nacionales vigentes, sin reemplazar las exigencias legales específicas de cada jurisdicción. Sin embargo, puede actuar como una guía práctica para cualquier DEFR o DES durante una investigación. Esta norma no contempla requisitos específicos de cada jurisdicción, como la admisibilidad, la relevancia probatoria, la pertinencia y otras limitaciones sobre el uso de evidencia digital en los tribunales, aunque sí puede facilitar el intercambio de evidencia digital entre jurisdicciones. (Roatta, 2015)

Otros estándares ISO para la informática forense son

- ISO/IEC 27042:2015: Directrices para el análisis e interpretación de evidencia digital.
-ISO/IEC 27043:2015: Principios y procesos para la investigación de incidentes.
-ISO/IEC 27050-1:2019: Conceptos de descubrimiento electrónico, incluyendo

investigación en vivo y en la nube.

En Argentina, el IRAM (Instituto Argentino de Normalización y Certificación) es el encargado de adaptar y normalizar estos estándares. A fines de 2017, se solicitó el estudio y adaptación de estos estándares al contexto local.

Según la "Guía de obtención, preservación y tratamiento de evidencia digital" (2016) aunque puedan existir otros factores que contribuyan al manejo de la evidencia digital, la norma ISO ha establecido que los principios relevancia, confiabilidad y suficiencia son los que definen las condiciones esenciales y suficientes para que los expertos en informática forense puedan recopilar, asegurar y preservar los elementos materiales probatorios en medios digitales. Estos elementos pueden ser revisados y analizados por terceros interesados y sometidos a contradicción según lo establezca el marco jurídico aplicable.

Un pionero en este ámbito fue el Poder Judicial de la provincia de Neuquén, que aprobó en 2012 el Protocolo de Actuación para Pericias Informáticas. Este documento establece los pasos a seguir durante un allanamiento, asegurando una base sólida para el proceso pericial.

Otra guía relevante es la elaborada por el InfoLAB, el grupo de investigación de informática forense de la Universidad de Ingeniería del FASTA de Mar del Plata. La Guía integral de empleo de la informática forense (2016) presenta los elementos esenciales a considerar en la búsqueda, obtención, preservación, examen pericial y presentación de evidencias digitales en el ámbito penal, con el objetivo de asegurar la validez y eficacia probatoria de estas actividades. En términos técnicos, se basa en el Proceso Unificado de Recuperación de Información – PURI, desarrollado por el grupo de investigación en Sistemas Operativos e Informática Forense de la Facultad de Ingeniería de la Universidad FASTA, el mismo integra procesos y guías de buenas prácticas nacionales e internacionales de informática forense, estructurándolas en fases, etapas, tareas, técnicas y herramientas recomendadas. Este

protocolo abarca la planificación previa, identificación, recolección, validación, análisis, interpretación, documentación y presentación de evidencia digital para esclarecer o probar hechos delictivos.

El protocolo ofrece un tratamiento general para los equipos de telefonía celular, sin especificar técnicas ni herramientas detalladas para el análisis pericial.

Asimismo actúa como una herramienta para la planificación y supervisión del proceso de investigación penal. Además, su correcta implementación proporciona un apoyo crucial para la presentación efectiva de pruebas digitales y dictámenes periciales en el ámbito judicial.

Debido al rápido crecimiento y la naturaleza dinámica del ciberdelito, se ha desarrollado un protocolo que exige la actualización de las prácticas de intervención de los cuerpos forenses en su labor pericial. La preservación de la evidencia digital se ha vuelto esencial para que pueda ser utilizada como prueba en un proceso legal, donde se deben emplear técnicas científicas y analíticas especializadas para identificar, preservar, analizar y presentar los datos e información extraídos de los dispositivos examinados.

El “Protocolo para la identificación, recolección, preservación, procesamiento y presentación de evidencia digital” (2023) busca establecer una metodología de intervención adecuada y uniforme en casos que involucren elementos con potencial probatorio digital, complementando el "Protocolo de Actuación para la Investigación Científica en el Lugar del Hecho". Su aplicación es obligatoria en los procedimientos policiales realizados por las Fuerzas Policiales y de Seguridad Federales (Resolución N° 528/21 del Ministerio de Seguridad)

Este protocolo establece las directrices y procedimientos que deben seguir los miembros de las Fuerzas Federales Policiales y de Seguridad durante el proceso de identificación, recolección, preservación, procesamiento y presentación de evidencia digital relacionada con

cualquier delito, especialmente ciberdelitos, incluyendo tanto los ciberasistidos como los ciberdependientes.

Proporciona procedimientos específicos de secuestro para el primer interviniente, clasificados según el tipo de dispositivo electrónico, como celulares, notebooks, equipos de escritorio, servidores, equipos de video, criptoactivos, rigs de minería y redes informáticas.

Incluye flujogramas de los procedimientos de secuestro para facilitar una consulta rápida en el campo. También especifica los lineamientos para la intervención técnico-forense realizada por el personal especializado en el laboratorio.

Este protocolo, en su Capítulo V, aborda los procedimientos específicos según el tipo de dispositivo electrónico. A continuación, se abordará lo relativo a dispositivos móviles, dado que es de particular relevancia para el presente trabajo.

1. Es fundamental aislar el dispositivo de inmediato para impedir su conexión a redes móviles y WiFi, evitando así cualquier posible adulteración o borrado remoto.
2. No se debe interactuar innecesariamente con los dispositivos móviles ni buscar información en ellos, salvo que lo solicite la autoridad judicial. Cualquier interacción debe ser documentada, ya que todos los movimientos quedan registrados en el dispositivo y serán reportados por el equipo especializado durante el análisis en el laboratorio.
3. Si el dispositivo está encendido (CALIENTE-AFU), no se debe apagar. Es necesario seguir los procedimientos recomendados para garantizar la preservación e identificación del equipo, y registrar todo en el acta del procedimiento. Esto incluye:
    a. Retirar la tarjeta SIM para evitar modificaciones remotas a través de la red celular.
    b. Registrar la numeración y el logo visibles en la tarjeta SIM.
    c. Si hay más de un slot de SIM, identificar y registrar la ubicación de cada tarjeta.
    d. Fijar las tarjetas SIM con cinta transparente a la carcasa del equipo.

e. Si es posible, identificar el IMEI del dispositivo y registrarlo. Si no es visible, se debe anotar "IMEI no visible / ilegible". No se debe manipular el equipo para obtener este número.

f. Si es posible, activar el modo avión y desactivar la opción de WiFi.

g. Identificar y registrar cualquier marca o inscripción visible en la carcasa del dispositivo.

h. Identificar y registrar el modelo técnico del dispositivo.

i. Identificar y registrar el número de serie, si es visible. No se debe manipular el equipo para obtener este número.

j. Registrar la existencia de una tarjeta de memoria, su tipo, capacidad e inscripción. Si no existe, registrar "No Posee Tarjeta de Memoria".

k. Evaluar y registrar el estado de conservación del dispositivo (Bueno, Regular, Malo), describiendo cualquier daño visible.

l. Finalmente, colocar el dispositivo en una bolsa Faraday o envolverlo con un método no invasivo que garantice el aislamiento electromagnético (por ejemplo, papel aluminio, utilizando al menos cinco capas).

4. Si la autoridad judicial lo requiere y se dispone de los medios necesarios, mantener el dispositivo encendido conectándolo a un powerbank (batería portátil) mientras se utiliza el aislamiento electromagnético, para su posterior envío a las oficinas especializadas o al laboratorio, evitando que se apague.

5. Si la autoridad judicial solicita un triage de dispositivos móviles, este será realizado por personal especializado y consistirá en un examen manual sin herramientas forenses, utilizando solo las funciones del dispositivo. Todas las interacciones deben ser correctamente documentadas.

6. Si el dispositivo está apagado (FRIO-BFU), debe mantenerse así y seguir estos pasos:

a. Retirar la tarjeta SIM para prevenir accesos remotos.

b. Registrar la numeración y el logo de la tarjeta SIM.

c. Identificar y registrar la ubicación de cada tarjeta SIM si hay más de un slot.

d. Fijar las tarjetas SIM a la carcasa del dispositivo con cinta transparente.

e. Si es posible, identificar y registrar el IMEI.

f. Identificar y registrar cualquier marca o inscripción visible.

g. Identificar y registrar el modelo técnico.

h. Identificar y registrar el número de serie, si es visible.

i. Registrar la existencia y detalles de la tarjeta de memoria, si la tiene.

j. Evaluar y registrar el estado de conservación del dispositivo.

k. Colocar el dispositivo en una bolsa Faraday o envolverlo con papel aluminio para garantizar el aislamiento electromagnético.

7. Para dispositivos encendidos o apagados, cuando sea posible, también se deben secuestrar el cargador y los cables de datos.

8. Si algún usuario, con pleno conocimiento de sus derechos, desea proporcionar voluntariamente las claves del dispositivo durante el secuestro, estas deben ser registradas en el acta y su uso debe ser acordado con la autoridad judicial y documentado.

9. Una vez acondicionado el dispositivo (en bolsa Faraday, papel aluminio, etc.), debe ser preservado individualmente en un contenedor que garantice su seguridad. Es esencial que se coloquen firmas de los intervinientes en los cierres y pliegues del embalaje para evitar dudas sobre un posible acceso no autorizado. Finalmente, se debe confeccionar una planilla de cadena de custodia para cada dispositivo en particular.

El registro de la cadena de custodia consiste en un documento o conjunto de documentos

(como actas de secuestro, actas de entrega y recepción, actas de apertura o desintervención, y formulario de cadena de custodia) que detallan la trazabilidad de los elementos probatorios. Este registro especifica quién fue responsable de custodiar y trasladar los elementos desde su secuestro hasta su disposición final, conforme a lo determinado por la autoridad judicial.

El procesamiento de información se limitará exclusivamente a responder a los requerimientos de pericia o investigación. En cuanto a los dispositivos móviles (como teléfonos y tablets), la extracción y procesamiento de datos se llevará a cabo con software especializado, documentando claramente la versión utilizada. Existen diversas técnicas de extracción según el sistema operativo, componentes electrónicos y medidas de seguridad del dispositivo (como bloqueo de acceso o métodos de root/jailbreak). Se podrán emplear técnicas para obtener datos escalando privilegios del sistema operativo, siempre que estas prácticas sean autorizadas previamente por la autoridad judicial, con una clara explicación de los riesgos y beneficios asociados.

Análisis de la evidencia digital

Según Pina González (2023) el análisis de información o evidencia digital implica llevar a cabo las acciones necesarias para identificar cuáles de los archivos contenidos en los dispositivos incautados son relevantes para la investigación. Los dispositivos móviles almacenan una amplia gama de información de diversa índole, por lo tanto, al realizar el análisis de la información almacenada, es fundamental llevar a cabo la tarea de manera eficiente, evitando al mismo tiempo invadir áreas de privacidad que no están relacionadas con el delito en cuestión.

En esta fase, la elección del método de búsqueda y análisis de la información contenida en el dispositivo es de vital importancia, y en la medida de lo posible, debería estar respaldada por una resolución judicial. Aquí, el perito aplicará técnicas científicas y analíticas a la copia

forense para poder encontrar pruebas de comportamientos específicos. Esto puede incluir la búsqueda de cadenas de texto, acciones concretas realizadas por los usuarios del dispositivo, búsqueda de archivos particulares, recuperación de identificaciones de correos electrónicos, recuperación de los últimos sitios web visitados, entre otros. Sin embargo, los archivos de interés a menudo están dispersos, ocultos en cualquier parte del dispositivo de almacenamiento, o incluso encriptados, lo que complica el análisis de la información y puede llevar al acceso a toda la información almacenada en el dispositivo.

Presentación de los resultados

La misma implica la recopilación de toda la información obtenida durante el análisis. En esta fase, el experto debe elaborar un informe claro y detallado, donde se explique el procedimiento seguido y se expongan las conclusiones alcanzadas. Este informe es fundamental para que las partes involucradas y el juez puedan evaluar correctamente la evidencia presentada.

Preservación de la evidencia digital

Se logra siguiendo meticulosamente las etapas y procedimientos establecidos, lo que garantiza que la información recolectada permanezca inalterada desde su obtención hasta su presentación en juicio. Este proceso incluye la correcta recolección, almacenamiento y custodia de la evidencia, asegurando que cada paso del manejo sea trazable y transparente. Así, se puede demostrar que la prueba presentada es la misma que fue obtenida en la escena del delito, lo que refuerza su fuerza probatoria ante posibles cuestionamientos de la defensa, especialmente respecto a la cadena de custodia. La confiabilidad de los soportes y procedimientos técnicos empleados es crucial para asegurar la integridad y el valor de la evidencia en el proceso judicial.

Valoración de la evidencia digital

Sigue diciendo el autor que la mayoría de los códigos procesales contemporáneos se basan en el sistema de libre convicción razonada o crítica racional para la evaluación de pruebas. La evidencia digital también se ajusta a este método. Sin embargo, debido a su naturaleza técnica e informática, es necesario que las partes cumplan con ciertos requisitos adicionales para asegurar la calidad de la evidencia y su adecuada evaluación por parte del juez. La valoración de la prueba digital es un proceso clave en la administración de justicia que busca garantizar que la evidencia digital presentada en un juicio cumpla con ciertos estándares antes de ser aceptada y utilizada en el proceso judicial. Esta valoración se basa en tres requisitos fundamentales.

1.Licitud: La prueba digital debe haber sido obtenida y presentada de manera legal. Esto significa que el proceso para adquirir la evidencia debe respetar las garantías constitucionales, como el derecho a la intimidad y la inviolabilidad de las comunicaciones. Por ejemplo, acceder a un teléfono móvil sin autorización judicial y extraer información de él sería ilegal, así como también sería inapropiado acceder a la información de un dispositivo sin un permiso adecuado, incluso si el dispositivo fue secuestrado legalmente.

2. Autenticidad: Se debe demostrar que la evidencia digital proviene de la fuente que se dice y que corresponde al autor real del documento o mensaje. Esto puede implicar identificar el dispositivo desde el que se envió la información o verificar la identidad del usuario a través de métodos como la identificación del número de teléfono o el código IMEI. Además, es crucial mostrar que el documento no ha sido alterado desde su creación hasta su presentación en el juicio.

3.Integridad e Inalterabilidad: La prueba digital debe mantenerse intacta y sin modificaciones desde el momento en que se obtuvo hasta que se presenta en el juicio. Es necesario garantizar que el contenido no haya sido editado ni manipulado de manera

fraudulenta. Técnicas de informática forense, como la cadena de custodia y la pericia técnica, juegan un papel crucial para verificar que la evidencia digital no ha sido alterada y para asegurar su autenticidad. (p12-14)

Métodos de extracción de datos: física, lógica y chip-off entre otros.

Según Gómez Palacios (2019) los datos en un dispositivo Android pueden formar parte de investigaciones civiles, penales o internas en empresas corporativas. En tales casos, el perito forense debe estar atento a varios aspectos durante el proceso de extracción. Es crucial determinar si se permite el acceso con privilegios de root (ya sea por consentimiento o autoridad legal) y qué datos se pueden extraer y analizar. Por ejemplo, en una investigación de acoso, el tribunal puede limitar la extracción y análisis a mensajes SMS, registros de llamadas y fotos, lo cual justificaría una captura lógica de estos elementos específicos. Alternativamente, se puede optar por una extracción física completa del dispositivo y luego examinar únicamente las áreas permitidas por el tribunal.

Las técnicas de extracción de datos en un dispositivo Android se dividen en tres categorías.

Extracción manual de datos: Este método implica navegar por el dispositivo de manera similar a como lo haría un usuario, y capturar cualquier información valiosa visible en la interfaz del usuario (IU). Esto incluye registros de llamadas, mensajes de texto y chats de mensajería instantánea como WhatsApp. El contenido de cada pantalla se captura mediante fotografías con herramientas especializadas, y estos datos pueden ser presentados como evidencia. Es fundamental documentar detalladamente el proceso. Sin embargo, la principal limitación de este método es que solo permite el acceso a los archivos visibles a través del sistema operativo y su IU, y la cantidad de información obtenida puede ser insuficiente dado el volumen de datos que un dispositivo puede contener. Además, el examen manual presenta el riesgo de borrar o alterar datos accidentalmente, por lo que debe ser considerado como

último recurso para corroborar hallazgos obtenidos mediante otros métodos.

Extracción lógica de datos: Esta técnica recupera datos accediendo al sistema de archivos y al sistema operativo del dispositivo. Es importante porque proporciona datos valiosos, funciona en la mayoría de los dispositivos y es relativamente fácil de usar. A diferencia de la extracción física, la extracción lógica no requiere acceso con privilegios de root, aunque tener permisos de administrador en un dispositivo permite acceder a todos los archivos, no solo a los visibles o accesibles en un dispositivo no rooteado. Por lo tanto, la calidad y cantidad de datos accesibles mediante extracción lógica pueden mejorar significativamente si el dispositivo tiene acceso root.

El tiempo que insume es menor que en una extracción física, ya que solo se trabajará sobre los archivos que sean necesarios para la investigación y no la totalidad del dispositivo.

Extracción de sistemas de archivos*:* da un volumen intermedio de datos. Extrae los archivos de sistema del dispositivo, los datos del usuario, de aplicaciones y algunos archivos ocultos o protegidos. Los sistemas de archivo pueden contener información que no es visible en una extracción lógica.

Extracción física de datos: Esta técnica implica obtener una imagen exacta, bit a bit, del almacenamiento del dispositivo. Es importante destacar que una imagen bit a bit no es lo mismo que copiar y pegar, que solo copia los archivos visibles y accesibles. En contraste, la extracción física incluye una copia completa de la memoria del dispositivo, abarcando archivos visibles, ocultos, y aquellos asociados con el sistema, así como el espacio libre y no asignado y todas las particiones. Por lo tanto, la extracción física proporciona una vista exhaustiva de toda la información contenida en el dispositivo. Para realizar una extracción física de datos, es necesario contar con un almacenamiento de capacidad igual o superior a la del dispositivo original. Esto se debe a que una copia de este tipo resulta en un archivo (o

varios) que tiene el mismo tamaño que el disco del dispositivo fuente. Además, este proceso puede ser muy lento, dado que implica una copia completa del contenido, lo cual puede requerir varios gigabytes y consumir una cantidad considerable de tiempo. (pp. 63-70).

Dentro de los métodos más invasivos se encuentran: ***Chip-off:*** Este método implica la extracción física de los chips de memoria del teléfono. Una vez extraídos, se utiliza un lector especializado para acceder a la información y obtener una copia exacta, bit a bit, de la memoria. Este procedimiento es altamente complejo, y cualquier error durante el proceso podría resultar en la pérdida irreversible de los datos. Algunas de las herramientas utilizadas para este tipo de extracción incluyen MD Reader de Hancom, microscopios y dispositivos como Riff Box.

Micro Read: Este método se basa en la interpretación directa de los datos almacenados en el chip de memoria. Se requiere un microscopio de alta potencia para examinar y analizar las puertas físicas del chip, leer las puertas binarias y convertir esta información en formato ASCII. Este procedimiento es costoso y consume mucho tiempo. (Núñez Soto, 2020)

A pesar de la diversidad de metodologías y herramientas disponibles para la adquisición de datos, es innegable que los dispositivos móviles se han convertido en elementos fundamentales en las investigaciones debido a su capacidad para almacenar vastas cantidades de información y su versatilidad en el uso cotidiano. No obstante, el verdadero desafío que enfrentan las organizaciones no radica solo en extraer esta información, sino en hacerlo de manera que se respete y proteja la privacidad del usuario. Lograr este equilibrio es una tarea compleja que deberá abordarse con urgencia en un futuro cercano.

UFED y otras herramientas forenses utilizadas para extracción de información

Las herramientas de extracción forense de dispositivos móviles son instrumentos tecnológicos especializados diseñados para recuperar información de dispositivos móviles de

manera que esta pueda ser utilizada legalmente en procesos judiciales. Estas herramientas permiten acceder a datos como mensajes, registros de llamadas, ubicaciones GPS, y otro tipo de información almacenada en dispositivos como smartphones, tarjetas SIM, y dispositivos de almacenamiento externo. Su uso es fundamental en investigaciones penales, donde la precisión y la fiabilidad de los datos extraídos pueden ser cruciales para el desarrollo de un caso.

Según Kiguel (2021) en Argentina, estas herramientas son empleadas principalmente por peritos informáticos que operan en laboratorios forenses dependientes de las fuerzas de seguridad y de la ley tanto a nivel nacional como provincial. Entre las entidades que utilizan estas tecnologías se incluyen la Gendarmería Nacional Argentina, la Policía Federal Argentina, la Policía de Seguridad Aeroportuaria, y diversas fiscalías provinciales, como las de Salta, Córdoba, Santa Fe y Buenos Aires, entre otras.

Diversas compañías privadas suministran estas herramientas a las fuerzas de seguridad. Entre las más destacadas se encuentran.

Cellebrite y su UFED (Universal Forensic Extraction Device)

Cellebrite, una compañía israelí, es reconocida mundialmente por su suite de herramientas de extracción forense. Su dispositivo UFED permite realizar extracciones físicas, lógicas y de sistema de archivos de una amplia variedad de dispositivos móviles (más de 31.000), incluidos teléfonos con Android y iOS, drones, y dispositivos GPS. En Argentina, Cellebrite ha consolidado su posición como líder en el mercado, con múltiples licencias activas en diversas agencias gubernamentales. La herramienta UFED es considerada una de las más fiables para acceder a dispositivos bloqueados y extraer información que pueda ser utilizada como evidencia en procedimientos judiciales. Se vende como un software para ser instalado en cualquier PC o en su versión UFED Touch2, que incluye una tablet portátil y accesorios

que permiten realizar la extracción en cualquier lugar.

MSAB y XRY

MSAB es otra compañía destacada en el ámbito de la extracción forense. Su producto XRY Logical permite realizar extracción lógica del archivo y acceder a recuperar cualquier sistema de archivo del dispositivo en tiempo real. El XRY Physycal permite extracción física, y se distingue por su capacidad para eludir sistemas operativos y acceder a datos eliminados y en algunos casos vulnera el cifrado si el dispositivo se encuentra bloqueado. Incluso posee herramienta de extracción que permite recuperad datos en la nube, información de Facebook, Google, Icloud sin necesidad de introducir datos de usuario y contraseña.

Aunque su presencia es más fuerte en Europa, en Argentina también ha sido adoptada por varias fuerzas de seguridad, incluyendo el Ministerio Público Fiscal de la Nación y otros cuerpos provinciales.

Magnet AXIOM

Magnet Forensics, una empresa canadiense, ofrece el software Magnet AXIOM, que se utiliza para la extracción y análisis de datos de dispositivos móviles, computadoras y servicios en la nube. En Argentina, varias fiscalías, como las de la Ciudad Autónoma de Buenos Aires y Santa Fe, utilizan este software para investigaciones digitales.

Oxygen Forensic

Que a diferencia de las herramientas previamente citadas, Oxygen Forensic Detective es más económico y ofrece suites personalizadas adaptadas a los teléfonos más utilizados en distintas regiones. Esto significa que adquirir Oxygen Forensic Detective en Latinoamérica, Asia, Medio Oriente o Europa implica tener acceso a bases de datos específicas para cada área geográfica, ajustadas a los modelos de teléfonos predominantes en cada región.

Uno de los problemas más críticos en el uso de estas herramientas radica en la falta de

transparencia sobre cómo operan. Dado que la mayoría de estas herramientas son de software comercial, sus códigos fuente están protegidos bajo leyes de propiedad intelectual, lo que impide que los peritos y las partes involucradas en un proceso judicial comprendan completamente cómo se obtuvieron y procesaron los datos extraídos. Esto plantea interrogantes sobre la confiabilidad de la prueba, especialmente en lo que respecta al derecho del acusado a conocer y desafiar la evidencia en su contra, tal como lo establece el artículo 18 de la Constitución Nacional Argentina.

En este contexto, es importante subrayar que el secreto comercial es un interés legítimo y protegido por el derecho. No obstante, este no puede ser invocado en situaciones que pongan en riesgo derechos fundamentales, como el derecho de defensa antes mencionado. La admisibilidad de estas herramientas en un proceso judicial debe estar supeditada a que se garantice, mediante cualquier medio disponible, que la herramienta emplea una metodología confiable y que los resultados obtenidos no han sido manipulados. Por ello, es esencial fomentar la transparencia y el control sobre el funcionamiento de estas herramientas, lo que resulta indispensable para supervisar adecuadamente los dispositivos y detectar posibles defectos que puedan comprometer la confiabilidad de la prueba producida.

Un caso que ilustra la vulnerabilidad de estas herramientas ocurrió en abril de 2021, cuando el CEO de Signal, una popular aplicación de mensajería, descubrió fallas en la seguridad del UFED de Cellebrite. Estos hallazgos subrayan la necesidad de un escrutinio riguroso y continuo de las herramientas forenses utilizadas en el ámbito judicial. (pp. 9-19)

Espejo Chubut: El programa "Espejo Chubut" fue diseñado para agilizar y asegurar la recolección de evidencia digital para víctimas y denunciantes, permitiendo incorporar contenido como chats o audios de redes sociales en procesos penales sin necesidad de confiscar el dispositivo móvil.

Este software captura imágenes o videos en tiempo real de la pantalla de dispositivos Android conectados vía USB, sin crear archivos adicionales ni modificar el dispositivo, ya que solo refleja lo que se muestra en pantalla. De esta manera, genera una "copia" del contenido del dispositivo que es admisible en un proceso judicial, preservando la cadena de custodia mediante un registro completo de conexión, grabación y extracción. Esto garantiza que la evidencia se mantenga intacta y permite un proceso ágil y eficiente, liberando a los peritos de trabajo adicional y evitando la exposición de otros datos personales de la víctima que no son relevantes para la investigación.

Además, el programa guarda y documenta información crucial del dispositivo, como la marca, el modelo, el número de serie y el IMEI, ofreciendo un registro detallado. Una vez que se ingresan los datos iniciales, el dispositivo se configura de manera sencilla para conectarse a una computadora, lo que permite al fiscal acceder y extraer la información necesaria para la investigación.

Entre las ventajas del sistema se destacan la eliminación de la necesidad de secuestrar el dispositivo móvil de la víctima, garantizando la integridad de la evidencia, la aceleración de los procedimientos judiciales, la reducción de la carga de trabajo para los peritos, la capacidad de extraer solo la información relevante para el caso, y la facilidad de implementación en cualquier dependencia policial o repartición oficial. Y a se utiliza en la mayoría de las provincias de nuestro país. (Torres, 2023)

Capítulo 2: La intervención estatal y la regulación de la evidencia digital

La intervención estatal y la regulación de la evidencia digital han sido temas centrales en la evolución del derecho procesal penal. A medida que el siglo XX avanzó, se destacó la necesidad de reformar los sistemas judiciales para garantizar derechos fundamentales en un contexto de creciente violencia estatal. El modelo acusatorio, que enfatiza la igualdad de las

partes y la imparcialidad del tribunal, ha sido un pilar en esta transformación, asegurando que la carga probatoria recae en el Estado y protegiendo los derechos del imputado.

Internacionalmente, el Convenio sobre Ciberdelincuencia y la Resolución N° 68/167 de la ONU han establecido estándares para equilibrar la recolección de pruebas digitales con la protección de derechos fundamentales como la privacidad. Estas normativas reflejan un esfuerzo global por adaptar la legislación a los desafíos de la era digital.

En Argentina, la regulación de la evidencia digital ha sido abordada de manera fragmentada en los distintos códigos procesales penales provinciales y federales. Aunque existen disposiciones que permiten el secuestro y análisis de datos informáticos, la falta de un marco unificado y detallado genera desafíos significativos. En este capítulo, exploraremos cómo los códigos procesales penales en Argentina regulan la intervención estatal en la obtención de evidencia digital, destacando las variaciones y limitaciones de las normativas actuales, y abordaremos las deficiencias y necesidades en la legislación para proteger adecuadamente los derechos de privacidad.

La falta de normas específicas para la evidencia digital subraya la necesidad de actualizar la legislación para alinearla con los estándares internacionales y proteger adecuadamente los derechos de privacidad.

Este capítulo explora la evolución de la intervención estatal y la regulación de la evidencia digital, destacando la importancia de equilibrar la eficacia del poder punitivo con la protección de los derechos fundamentales en el contexto de la justicia penal.

La evolución del derecho procesal penal y el modelo acusatorio

Durante el siglo XX, se discutieron ampliamente las reformas necesarias para los sistemas de administración de justicia, aunque se mantuvieron las bases inquisitivas. En respuesta a la violencia estatal en Europa y Latinoamérica, surgió una normativa humanitaria internacional

para proteger los derechos humanos básicos, que hasta entonces habían sido vulnerados en los procesos penales estatales.

Según Maier (2016), hubo un incremento en los esfuerzos político-criminales dirigidos a racionalizar el poder penal estatal, regulando la persecución penal. Una característica clave del modelo acusatorio es la separación de las funciones de acusación y decisión dentro del sistema judicial. En este modelo, el acusador lidera la investigación desde el inicio, buscando la verdad material basada en evidencias. Este rol, ya sea en solitario o junto a la parte querellante, ejerce la acción penal y enfrenta a su adversario bajo la vigilancia de la defensa y el tribunal. (p.347)

Jauchen (2013) sostiene en lo que respecta al ejercicio de la acción, que el fiscal actúa de manera oficial y oficiosa (p.76) en relación con los delitos de acción pública, tal como se establece en el artículo 71 del Código Penal. Además, el Código Procesal Penal de Santa Fe regula este procedimiento en el artículo 16, indicando que el fiscal puede actuar de oficio, siempre y cuando no dependa de una instancia privada. La promoción de la acción penal es obligatoria en relación con los hechos punibles de los que el fiscal tenga conocimiento y existan indicios de su existencia.

Baclini y Schiappa Pietra (2017) explican que este artículo refleja lo que se denomina el principio de legalidad procesal, que es el principio fundamental en la regulación de la acción penal pública. Según este principio, se obliga al órgano encargado de la persecución penal a iniciar la acción penal. A su vez, se otorga una facultad en el ejercicio de la acción, permitiendo la aplicación de criterios de oportunidad, siempre que se respeten los marcos de legalidad establecidos por la norma como principio rector.En cuanto a la carga probatoria, señalan que recae sobre el Estado. (pp. 73-74)

En el sistema acusatorio, corresponde al fiscal la responsabilidad de aportar pruebas, por lo

que su labor consiste en investigar y recopilar la mayor cantidad de evidencias posibles. Esto es necesario para refutar el estado de inocencia del que goza cualquier persona acusada y establecer su culpabilidad, con el objetivo de lograr una sentencia condenatoria.

La antinomia fundamental, según Binder (2013), es una herramienta crucial para entender los conflictos de intereses opuestos presentes tanto en el núcleo del derecho procesal penal como en todas sus instituciones. Esta antinomia se refiere a la tensión esencial entre la necesidad de eficiencia del poder punitivo del Estado y las limitaciones impuestas para proteger las libertades individuales. El enfrentamiento de estas fuerzas se manifiesta como una contradicción fundamental, característica de los sistemas adversariales, en los que hay conflictos entre el interés de sancionar y reprimir los delitos y el de protegerse contra acusaciones injustificadas y persecuciones infundadas. El autor sugiere que los distintos mecanismos procesales establecidos en la legislación deben ser analizados a la luz de estas tensiones. Una norma podría permitir una determinada medida investigativa siempre que se respeten ciertos límites y restricciones formales, que no pueden ser superados sin vulnerar los derechos de los afectados. Es responsabilidad del tribunal correspondiente evaluar cada caso, decidiendo en función del contexto y las particularidades del asunto. La existencia de esta contradicción de fuerzas es esencial, ya que el proceso penal es el medio inevitable para la aplicación de una pena.

Binder señala que la eficacia del poder punitivo estatal se centra en su capacidad para llevar a cabo su misión de controlar la criminalidad, evitar la impunidad y mantener la paz social mediante la aplicación de la ley penal. Este poder es ejecutado principalmente por el ministerio público acusador, el cual actúa de manera autónoma y en colaboración con otras autoridades estatales para imponer sanciones a quienes infringen la ley. Sin embargo, este poder no es ilimitado; está restringido por un conjunto de garantías diseñadas para proteger

los derechos de los ciudadanos en un Estado Constitucional de Derecho. Estas garantías funcionan como un escudo protector contra posibles abusos del poder penal, asegurando que cualquier intervención estatal en contra de un individuo esté justificada y fundamentada en la ley. Estas protecciones están recogidas en la Constitución Nacional, en tratados internacionales de derechos humanos, y en legislaciones y códigos procesales provinciales. (pp.99-105)

El sistema penal busca mantener un equilibrio entre la eficacia del poder punitivo del Estado y las garantías de los derechos de los ciudadanos, especialmente el derecho a la intimidad. Este equilibrio es dinámico y puede variar en cada caso, dependiendo de los intereses en juego. Los tribunales tienen la responsabilidad de decidir sobre la procedencia de medidas investigativas, como la interceptación de comunicaciones o la exclusión de ciertos puntos de pericia informática, basándose en los argumentos presentados y siempre dentro del marco de la legalidad.

El tribunal actúa como un dinamizador de las disputas que surgen entre las partes involucradas. Según Maier (2016), esto se entiende dentro del contexto de las medidas coercitivas que el Estado puede aplicar durante una investigación. Destaca que el derecho a la intimidad está protegido por la Constitución, que la protección de la privacidad asegura la exclusión de terceros de ciertos ámbitos privados, estableciendo una barrera contra la intervención del Estado, salvo en situaciones específicas que cumplan con estrictas formalidades legales. Esta protección se extiende a las comunicaciones privadas, ya que las nuevas tecnologías de comunicación están incluidas en el derecho a la intimidad (p.143).

Si se incumplen las formalidades legales requeridas para proteger estos derechos, como la autorización judicial, la presencia de testigos, la documentación adecuada, el mantenimiento de la cadena de custodia entre otros, las pruebas obtenidas de forma irregular pueden ser

rechazadas. Incluso si se aceptan, es posible que no sean consideradas por el tribunal al dictar una resolución, en línea con el principio de que el fin de obtener la verdad no puede justificar el uso de métodos prohibidos.

Regulación internacional y derechos humanos en la era digital

En 2001, el Consejo de Europa en Budapest adoptó el Convenio sobre Ciberdelincuencia. En el preámbulo del Convenio se subrayó la importancia de respetar los derechos humanos reconocidos en diversos tratados internacionales, incluyendo explícitamente la privacidad y la protección de datos personales y comunicaciones. Se estableció la necesidad de un "equilibrio adecuado" entre estos derechos. El capítulo II requiere que las partes adopten medidas legislativas y procesales para la recolección de pruebas informáticas durante las investigaciones criminales (art. 14), garantizando su aplicación más amplia posible. Asimismo, se estipula que el uso de estas facultades no debe perjudicar la protección de los derechos humanos y libertades de los ciudadanos. Por lo tanto, las medidas y procedimientos deben contar con autorización judicial, ser motivados y estar limitados en alcance y duración, evaluando el impacto en los derechos legítimos de terceros. Esto implica que la intromisión estatal en los derechos y libertades solo es válida si existe un interés concreto y razonable.

En el ámbito del proceso penal, la pertinencia de la prueba con respecto al hecho es un criterio clave. Dado que muchas evidencias informáticas pueden afectar profundamente la privacidad, deben ser autorizadas solo cuando se justifique dicha intromisión.

En Argentina, la Ley 27.411 ratificó el Convenio e hizo reservas sobre ciertas cláusulas relacionadas con delitos informáticos y cuestiones de jurisdicción, entre otras.

En el 2013, la Asamblea General de Naciones Unidas adoptó la Resolución N° 68/167 sobre el derecho a la privacidad en la era digital. Esta resolución destaca que nadie debe ser objeto de injerencias arbitrarias e ilícitas en su privacidad. Reconoce que Internet tiene una

naturaleza global y abierta, que el avance de las TIC ha tenido un impacto positivo en el desarrollo, y afirma que los derechos de las personas también deben estar protegidos en Internet. Esta regulación ofrece especificaciones más claras que permiten al Estado llevar a cabo su tarea dentro de un marco legal que protege los derechos ciudadanos.

En cuanto a regulaciones específicas europeas en España, la Ley de Enjuiciamiento Criminal proporciona un tratamiento detallado para las evidencias informáticas: 1) interceptación de comunicaciones telefónicas y telemáticas para delitos graves en contextos de organizaciones criminales o terrorismo, 2) captación y grabación de comunicaciones orales mediante dispositivos electrónicos, 3) uso de dispositivos de seguimiento y localización, 4) registro de dispositivos de almacenamiento de información, y 5) registro remoto de equipos informáticos. Además, establece principios rectores para la validez de estas medidas: deben estar relacionadas con un delito específico (especialidad), limitadas a un ámbito objetivo y subjetivo y tener una duración preestablecida (idoneidad); ser necesarias, ya que no existen medidas menos gravosas (excepcionalidad y necesidad). También regula el descubrimiento casual y la orden de borrado y eliminación de registros una vez finalizado el procedimiento, garantizando que la información extraída de pericias informáticas o interceptaciones será eliminada y no podrá ser utilizada en otro momento.

Relata Bernard (2022) que en Alemania, el Tribunal Constitucional Federal introdujo el concepto de derecho a la autodeterminación informativa, como una extensión del derecho a la intimidad. Este derecho asegura que el desarrollo libre de la personalidad requiere protección frente a la recolección, archivo, uso y retransmisión ilimitada de datos personales. Sin embargo, este derecho a la autodeterminación de la información no es absoluto. El individuo debe admitir ciertas restricciones a su derecho a la autodeterminación de la información, principalmente en aras del interés general preponderante. (p.43)

Como conclusión de lo expuesto, el avance internacional en la materia estudiada indica un camino hacia una regulación exhaustiva y detallada que pretende llenar los vacíos legislativos y evitar las intromisiones indebidas en la privacidad de las comunicaciones a través de medios informáticos. Esto evidencia, por un lado, la complejidad en la obtención de evidencia digital, lo que requiere actualizaciones constantes en los sistemas de administración de justicia para mantenerse al ritmo de las modificaciones tecnológicas. En este contexto, es importante destacar la relación entre el derecho a la información almacenada en soportes tecnológicos, que es de acceso privado, y las medidas investigativas emprendidas por los órganos de persecución en el marco de la aplicación del derecho penal en casos específicos, y los límites impuestos por el respeto a la dignidad humana.

Como señala Aboso (2014), los datos almacenados en medios tecnológicos están protegidos por la tutela constitucional del derecho a la intimidad y la expectativa de privacidad de los ciudadanos, lo que implica que cualquier intrusión arbitraria por parte de las autoridades públicas podría resultar en la nulidad de cualquier fuente o evidencia utilizada en contra del afectado. En estos casos, es imperativo contar con la autorización judicial. Es decir, cualquier medida que pueda afectar la intimidad del acusado requiere la aprobación judicial, así como una evaluación del caso específico a la luz del principio de razonabilidad, pertinencia y necesidad. Según el autor el derecho a la privacidad personal impone un deber doble al Estado: por un lado, abstenerse de realizar cualquier injerencia arbitraria en el ámbito de la vida personal de los ciudadanos; por otro, debe actuar de modo proactivo para asegurar el ejercicio razonable de ese derecho. (p.68)

La evidencia digital en códigos procesales penales argentinos

En Argentina, los distintos códigos procesales penales han adoptado un esquema similar, con algunas variaciones menores, para las medidas de coerción probatorias. Estos códigos regulan

procedimientos como el allanamiento, la requisa, la intercepción de correspondencia y la intervención de las comunicaciones.

El Código Procesal Penal de la Provincia de Neuquén establece disposiciones para la autorización del registro y secuestro de datos en dispositivos informáticos hallados durante un allanamiento. Además, permite los registros remotos sin imponer condiciones ni requisitos adicionales.

> Artículo 153º Información digital. Cuando se hallaren dispositivos de almacenamiento de datos informáticos que por las circunstancias del caso hicieran presumir que contienen información útil a la investigación, se procederá a su secuestro, y de no ser posible, se obtendrá una copia. O podrá ordenarse la conservación de los datos contenidos en los mismos, por un plazo que no podrá superar los noventa (90) días. Quien deba cumplir esta orden deberá adoptar las medidas necesarias para mantenerla en secreto. También podrá disponerse el registro del dispositivo por medios técnicos y en forma remota….

Sergi (2018) expresa que Salt critica que la normativa no establece un sistema de garantías apropiado para regular este mecanismo intrusivo. Según el texto de la norma, los requisitos parecen ser los mismos que los establecidos para el allanamiento. Aunque la medida está legalmente autorizada bajo autorización judicial, la falta de claridad sobre los casos en que puede aplicarse y el riesgo de vulnerar el principio de proporcionalidad generan dudas sobre su legitimidad constitucional. (p.98)

El Código Procesal Penal Federal regula en el articulo 151 la 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 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, bajo las condiciones establecidas en el artículo 136.

Regirán las mismas limitaciones dispuestas para el secuestro de documentos.

El examen de los objetos, documentos o el resultado de la interceptación de comunicaciones, se hará bajo la responsabilidad de la parte que lo solicitó.

Una vez secuestrados los componentes del sistema, u obtenida la copia de los datos, se aplicarán las reglas de apertura y examen de correspondencia.

Se dispondrá la devolución de los componentes que no tuvieran relación con el proceso y se procederá a la destrucción de las copias de los datos. El interesado podrá recurrir al juez para obtener la devolución de los componentes o la destrucción de los datos.

La reciente reforma del Código Procesal Penal de Salta, Ley 7.690, introduce varias modificaciones significativas en relación con la gestión y obtención de pruebas informáticas. Los cambios se reflejan en los siguientes aspectos clave:

1. Principios generales y autorización judicial. Se modifica el Artículo 309 para establecer que la realización de medidas relacionadas con pruebas informáticas debe ser ordenada por el Juez de Garantías, o, en ciertos casos, dispuesta por el fiscal sin necesidad de autorización judicial. La medida debe definir claramente su alcance y duración, buscando siempre la menor afectación posible a los derechos de los investigados.

2.Aseguramiento de datos: el nuevo Artículo 309 bis permite al fiscal ordenar el aseguramiento de datos informáticos específicos que están en riesgo de ser alterados o eliminados. La orden debe detallar los datos a asegurar, la técnica de conservación y tiene una duración máxima de noventa días, prorrogables si es necesario. El requerido debe preservar la integridad de los datos y mantener la medida en secreto.

3.Orden de presentación de datos: el Artículo 309 ter otorga al fiscal la facultad de ordenar a organismos públicos o privados la presentación de datos almacenados en sistemas informáticos. Esta medida también se extiende a proveedores de servicios que operen fuera de la provincia pero que brinden servicios dentro de Salta.

4.Obtención de datos informáticos: según el Artículo 309 quater, el Juez de Garantías puede ordenar el registro y secuestro de sistemas informáticos o medios de almacenamiento de datos. La orden puede incluir la copia de datos, su preservación y la remoción de datos para garantizar la cadena de custodia. También se permite la extensión del registro a otros dispositivos relacionados y se deben tomar medidas para asegurar que los datos obtenidos no sean alterados.

5.Investigación encubierta en entornos digitales: el Artículo 309 quinquies introduce la posibilidad de realizar investigaciones encubiertas en entornos digitales como redes sociales y sitios de comercio electrónico. Estas investigaciones pueden incluir la utilización de identidades digitales falsas y la realización de actividades encubiertas para identificar y detener a los responsables de delitos graves.

6. Obtención remota de datos: el Artículo 309 sexies permite al Juez de Garantías ordenar la obtención remota de datos informáticos mediante programas tecnológicos, siempre que se justifique la necesidad y proporcionalidad de la medida. La orden debe detallar el objetivo, los datos a obtener y el plazo para la ejecución, y se deben implementar controles para evitar la recolección de datos en exceso.

7. Interceptación de comunicaciones: se modifica el Artículo 316 para permitir la intervención de comunicaciones telefónicas y electrónicas bajo circunstancias específicas. La intervención se ordenará por períodos de hasta 30 días y podrá ser renovada. Además, se prohíbe la intervención de comunicaciones de defensores y otros letrados implicados en

la causa, bajo sanción de nulidad y responsabilidades penales.

Esta reforma busca modernizar la regulación de las pruebas digitales y mejorar la protección de los derechos fundamentales durante el proceso penal, equilibrando la eficacia investigativa con las garantías procesales.

En Santa Fe, no existe una legislación que aborde de manera completa las medidas investigativas en entornos digitales. Aunque sería altamente beneficioso contar con una regulación actualizada que se adapte a los avances tecnológicos en este ámbito, es crucial reconocer que el ritmo de desarrollo de las tecnologías supera con creces el de la legislación. Según Bernard (2022) las lagunas en la normativa podrían resultar, en algunos casos, en una vulneración de los derechos a la intimidad y la privacidad de los ciudadanos, especialmente cuando se implementan nuevas medidas no reguladas de forma indiscriminada. Ferrajoli, citado por Binder, destaca esta preocupación al afirmar que

> las deficiencias del derecho positivo (lagunas) o de justiciabilidad (debilidad del poder judicial) son defectos del sistema político constitucional que deben ser solucionados mediante la obligación constitucional de los órganos pertinentes de proporcionar a estos derechos la plenitud de sus garantías primarias y secundarias.

Para evitar que la falta de normas específicas conduzca a una disminución de las garantías, es recomendable recurrir a la normativa genérica vigente, a los principios generales de prueba y al análisis jurisprudencial en casos concretos. El artículo 159 del Código Procesal Penal de Santa Fe establece el principio de libertad probatoria, permitiendo cualquier medio de prueba que se relacione directa o indirectamente con el objeto de la investigación. (pp.44-45)

En este sentido, Baclini y Schiappa Pietra afirman que “el principio de libertad probatoria permite recurrir a la legislación aplicable para medios probatorios análogos cuando el medio que se pretende utilizar no esté expresamente regulado por la ley”(p.328)

Cuando se trata de evidencia digital, a menudo se aplican las normas que regulan la evidencia física mediante una interpretación amplia de estas. Sin embargo, es necesario reconocer que la evidencia digital tiene características específicas que requieren un tratamiento especial. La única medida legislada en cumplimiento del mandato constitucional es la interceptación de correspondencia y la intervención de comunicaciones (art. 171), la cual debe solicitarse al tribunal para obtener su autorización.

De acuerdo con la mencionada amplitud probatoria, medidas como la conservación de datos informáticos y la extracción de datos de servidores podrían realizarse mediante una solicitud al tribunal, que a su vez ordenaría al prestador de servicios de telecomunicaciones, proporcionando la información completa y suficiente para su procedencia. Este enfoque se ajustaría a la exigencia constitucional de la "orden de autoridad competente".

Considero que el dictado de una legislación adecuada no solo llenaría el vacío existente, sino que también fortalecería la confianza en el sistema de justicia al proporcionar un marco claro para la obtención y uso de evidencia digital. Es imperativo que esta regulación se alinee con los estándares internacionales y las mejores prácticas en el ámbito de la protección de datos y derechos fundamentales, garantizando así un equilibrio adecuado entre la eficacia de las investigaciones y la protección de la privacidad individual.

Evidencia obtenida de dispositivos móviles

La evidencia se define como cualquier dato o elemento recopilado durante la fase de investigación que permita probar las afirmaciones fácticas en la teoría del caso relacionada con el delito en cuestión. Esta evidencia puede ser física o intangible y se utiliza para fundamentar una imputación de delito y, eventualmente, para llevar el caso a juicio. La evidencia digital tiene características distintivas: es intangible (carece de consistencia física, y su obtención, análisis, visualización y reproducción requieren un soporte electrónico); su

contenido está compuesto por diversos códigos que facilitan su identificación y validación en el entorno digital (como el código hash); es relativamente más susceptible a daños (requiere técnicas especiales para su preservación y protección hasta su extracción); y está constituida por los datos e información almacenados, transmitidos o recibidos en un dispositivo informático.

Entre las medidas que utilizan los organismos estatales para realizar investigaciones se puede mencionar obtención de direcciones IP, dispositivos para geolocalizar personas y comunicaciones, videovigilancia electrónica, reconocimiento facial, allanamiento remoto, agente encubierto digital, redes sociales. Para el presente trabajo, la medida más relevante es la realización de pericias de dispositivos electrónicos.

Estas pericias implican la búsqueda, recolección, extracción y análisis de datos informáticos almacenados en dispositivos electrónicos físicos. En cuanto a la recolección de información, la normativa procesal local establece ciertos requisitos de procedencia: debe basarse en la evidencia que se pretende obtener, especificar los puntos de pericia y el contenido a buscar. Desde el momento en que se incauta el dispositivo informático, el procedimiento debe ser documentado para garantizar su auditabilidad y verificación, y para su presentación en juicio en caso de que sea necesario demostrar el contenido de la pericia.

Según Darahuge y Arellano González (2012) los informes de pericia informática, derivados de la información obtenida de dispositivos, presentan características únicas en comparación con la evidencia documental tradicional, debido a su naturaleza digital., estas características distintivas incluyen: 1) un principio de identidad atípico, ya que una copia digital de un archivo no puede distinguirse del original; 2) la posibilidad de modificación, ya sea local o remota; 3) la divisibilidad del documento; y 4) la necesidad de una prueba pericial informática forense adicional. Frecuentemente, esta prueba requiere ser corroborada mediante

un informe solicitado al proveedor de servicios de Internet correspondiente. (pp.19-20)

Conforme lo señala Bernard (2022) la preservación de los medios debe realizarse siguiendo una cadena de custodia, conjunto de medidas que deben adoptarse a fin de preservar la identidad e integridad de objetos o muestras que pueden ser fuente de prueba de hechos criminales, para su eficacia procesal.

La información accesible puede ser diversa e incluye, entre otros, el historial de ubicaciones y direcciones, marcadores y el historial completo de navegación en Internet, configuraciones de usuario, contenidos multimedia como fotografías con sus ubicaciones y metadatos, correos electrónicos, caché o cookies, contraseñas, aplicaciones o programas descargados, redes Wi-Fi a las que se ha conectado, contactos, y notas, ya sean existentes o eliminadas, tanto en la memoria interna del dispositivo como en tarjetas de memoria o micro SD. (p.50.51)

Capitulo 3: Extracción de información, su impacto en la intimidad y privacidad

En el marco de la creciente digitalización y el avance de las tecnologías de la información, el manejo y la regulación de la evidencia digital se han convertido en temas cruciales tanto a nivel nacional como internacional. La recolección de datos personales y la protección de la privacidad se sitúan en el centro de estos debates, ya que la intervención estatal en la esfera digital plantea serias cuestiones sobre el equilibrio entre la seguridad pública y los derechos fundamentales. En Argentina, la protección de la intimidad está garantizada por diversas normativas, como el Código Procesal Penal Federal, que establece parámetros para la recolección y el análisis de datos personales. A nivel global, los tratados y convenciones internacionales proporcionan un marco para la regulación de la evidencia digital y el respeto a los derechos humanos en el contexto de la justicia penal. Este capítulo examina el contexto histórico y actual del derecho procesal penal, las regulaciones internacionales pertinentes y la forma en que estas normas se integran en el ámbito local para garantizar la privacidad y el

debido proceso. La libertad probatoria y su interacción con la protección de la intimidad serán analizadas para comprender cómo se equilibran estas dos dimensiones en el contexto de la investigación y la justicia.

Regulación en la recolección de datos personales

No todos los datos personales son igualmente sensibles, y no todas las solicitudes de información infringen garantías constitucionales. Existen distintos niveles de afectación, que varían desde una intromisión mínima hasta una invasión más profunda, y cada nivel requiere el cumplimiento de condiciones específicas. Dado que los derechos no son absolutos, es posible avanzar en la recolección de datos sin violar otros intereses, siempre que se respete la intervención de un juez para definir hasta dónde se puede entrar en la esfera privada del individuo.

Datos de abonado: El Convenio de Cibercrimen define estos datos como la información básica que un proveedor de servicios posee sobre sus suscriptores, como el tipo de servicio utilizado, la identidad del cliente, dirección, número de teléfono, datos de facturación y la ubicación de los equipos de comunicación. También incluye datos de redes sociales y páginas comerciales necesarios para la registración. Este nivel de datos es menos intrusivo en términos de privacidad, y la solicitud de esta información a empresas de servicios puede hacerse sin el consentimiento previo del usuario, ya que se encuentra dentro de las facultades investigativas del Estado.

Datos de tráfico: Los datos de tráfico, también conocidos como metadatos, se refieren a la información generada en el contexto de una comunicación a través de sistemas informáticos o electrónicos, pero que no forma parte del mensaje mismo. Según Fernández Rodríguez (2016), “los datos de tráfico, o metadatos, en una comunicación son los datos que rodean el mensaje que se transmite, pero que no forman parte de dicho mensaje.”(p.96) Estos datos

permiten ubicar a alguien en un tiempo y lugar específicos, así como conocer el intercambio de comunicaciones y los interlocutores. Aunque no revelan el contenido de las comunicaciones, su recopilación implica una mayor intromisión en la esfera íntima de una persona. La Ley de Telecomunicaciones 25.873 obliga a las empresas a registrar y conservar estos datos por diez años, lo que puede llevar a un uso indiscriminado de la información por parte de los organismos estatales. Este tipo de datos a menudo se solicita sin autorización judicial, lo que podría permitir un uso excesivo de las facultades estatales.

Datos de contenido: Se refieren al mensaje en sí mismo, ya sea un correo electrónico, un mensaje de WhatsApp o cualquier otra comunicación. Jauchen (2013) señala que el artículo 18 de la Constitución Nacional no menciona específicamente las comunicaciones telefónicas o por otros medios puesto que no existían, la norma está diseñada para proteger y asegurar el derecho a la intimidad de las personas, independientemente del medio que utilicen para comunicarse. La idea subyacente es que los intercambios de diálogos o mensajes solo deberían ser conocidos por las partes involucradas en esa comunicación, sin estar expuestos a su divulgación o a ser escuchados involuntariamente por terceros. Este principio es lo que fundamenta la confianza de los ciudadanos en la confidencialidad de sus comunicaciones, permitiéndoles mantener una “razonable expectativa de privacidad”(p 247) en el desarrollo de su vida .La Corte Suprema de Justicia de la Nación, en su Acordada 17/2019, ha indicado que

> el balance entre el derecho de toda persona a no sufrir invasiones a su privacidad y el interés estatal en la persecución penal de un posible delito, debe incluir una necesaria ponderación de los instrumentos escogidos y los fines hacia los que se dirige la específica herramienta investigativa dispuesta en la causa.

La obtención de datos de contenido representa la forma más grave de intromisión en la

privacidad y debe ser considerada como una medida excepcional. Debe ser fundamentada, restringida en el tiempo y utilizada únicamente para el esclarecimiento de delitos y la administración de justicia.

Según Lega (2014) una idea propia del sistema inquisitivo es la que entiende que el fin justifica los medios, lo que implica que se pueden transgredir garantías y derechos de los acusados con tal de demostrar la existencia de un delito y restablecer el orden social alterado por su comisión. Sin embargo, la búsqueda de información no puede ser arbitraria y debe estar directamente relacionada con lo que se pretende probar. (p.23)

Un problema recurrente en las investigaciones penales es que la información obtenida de diversas fuentes, como dispositivos electrónicos o redes sociales, queda bajo el criterio del personal encargado de las diligencias, lo cual podría dar lugar a intrusiones indebidas. Aboso (2019) sostiene que

> No cabe duda de que la erosión de la expectativa razonable de privacidad en el uso de estos servicios telemáticos traería como lógica consecuencia la falta de confianza del público sobre el resguardo de sus derechos personalísimos, al permitir o autorizar el registro y tratamiento de datos por parte de las autoridades públicas, lo que sellaría el destino de esta moderna forma de comunicación. (p.61)

Esta práctica conlleva riesgos significativos, ya que podría ocasionar daños graves a los derechos de las personas afectadas si se accede a información que no guarda relación con una investigación específica. Una analogía adecuada sería con los allanamientos, procedimientos altamente intrusivos en la privacidad de un domicilio, que para ser legales deben contar con una orden judicial detallada, especificando los puntos autorizados, el momento de ejecución y el alcance de la medida. De igual forma, al recopilar evidencias digitales, no se debe permitir un acceso indiscriminado a la información contenida en computadoras o teléfonos móviles, a

menos que esté vinculada a una investigación concreta, bajo la justificación de motivos de prevención o seguridad pública.

En este contexto, el Tribunal Supremo Español, en la sentencia N° 204/1660, señaló que

> dado que la multifuncionalidad de los datos que se albergan en estos dispositivos provoca una extrema debilidad de la tutela jurisdiccional del derecho del investigado a la reserva de su propio entorno virtual, pues una vez realizado el acceso al dispositivo, superando la barrera de la contraseña, todos los datos, incluidos los relacionados con el secreto de las comunicaciones están al libre alcance del investigador.

Es en este ámbito donde surgen mayores interrogantes sobre la legitimidad de las medidas de recolección de evidencia, ya que para que la información encontrada fuera del ámbito autorizado judicialmente sea utilizada de manera legítima, debe demostrarse cómo se obtuvo sin que se hayan vulnerado las garantías constitucionales.

El derecho a la privacidad y su marco legal internacional y nacional

Según la Comunicación conjunta de la Asociación por los Derechos Civiles y Privacy International, la privacidad es un derecho fundamental respaldado por diversos tratados de derechos humanos. Este derecho es esencial para salvaguardar la dignidad humana y constituye un pilar de cualquier sociedad democrática. Además, la privacidad refuerza y protege otros derechos, como la libertad de expresión, de información y de asociación. Actividades que limitan el derecho a la privacidad, como la vigilancia y la censura, solo pueden justificarse si están estipuladas por ley, son necesarias para alcanzar un objetivo legítimo y son proporcionales al propósito buscado. Con el avance de las tecnologías de la información, que han permitido nuevas formas de recopilación, almacenamiento y transmisión de datos personales, el derecho a la privacidad ha evolucionado para incluir las obligaciones del Estado en relación con la protección de los datos personales. Existen varios

instrumentos internacionales que contienen principios de protección de datos, los cuales han sido incorporados en las legislaciones nacionales de numerosos países. (pp.2-3)

En cuanto a la regulación de la obtención de pruebas, existen una variedad de normas que, desde los inicios del constitucionalismo, han otorgado prioridad a la privacidad de los ciudadanos y su entorno sobre la obligación estatal de perseguir delitos. En los casos donde se permite la intervención estatal en la intimidad de las personas (allanamientos, requisas personales, secuestros o interceptación de comunicaciones), se han establecido disposiciones específicas y se requiere cumplir con ciertos requisitos para justificar tal intromisión en la privacidad del individuo sospechoso. Corresponde al juez la responsabilidad de garantizar que se cumplan las normas constitucionales y convencionales en estos procedimientos. (Mera, s.f., p.8)

En la cúspide de la jerarquía normativa se encuentran los artículos 18 y 19 de la Constitución Nacional. Si bien la Constitución Argentina no menciona la palabra “privacidad,” sí se refiere a “acciones privadas” en su artículo 19, el cual ha sido interpretado por la Corte Suprema de Argentina como consagrando el derecho a la privacidad. El artículo dice “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.”

Además, el artículo 18 de la Constitución dice “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.”

Según Sergi (2018) el texto constitucional de 1853 establece las garantías de intimidad y privacidad en los artículos 18 y 19. Aunque ambos términos se refieren a derechos

fundamentales, la doctrina distingue entre ellos: la privacidad es un concepto amplio que abarca todas las acciones que no afectan a terceros, mientras que la intimidad se refiere a una esfera personal que queda excluida del conocimiento de otros. Estos derechos no se superponen, sino que se complementan. Específicamente, el artículo 19 protege las comunicaciones privadas que no perjudiquen a terceros, otorgándoles una protección absoluta. Si estas comunicaciones fueran descubiertas por el Estado, se requeriría restaurar la situación de intimidad previa, por ejemplo, eliminando los registros. Sin embargo, si afectan a terceros, pueden perder su inmunidad total, aunque todavía están protegidas contra injerencias arbitrarias del Estado.

El artículo 19 consagra el derecho a la privacidad en sentido amplio, esto crea un ámbito de inmunidad frente a intervenciones estatales en la autonomía personal, asegurando la libre elección de un plan de vida sin interferencias estatales, salvo cuando haya impacto en terceros. Algunos autores consideran que esta protección de la privacidad justifica también el resguardo de la intimidad, especialmente en contextos donde la divulgación de ciertos datos podría afectar la autonomía individual. Esta idea es crucial en el análisis de la protección de los ciudadanos frente a la intromisión estatal en sistemas informáticos.

La protección del art. 18 incluye no solo documentos físicos, sino también comunicaciones electrónicas modernas, como correos electrónicos y llamadas por voz. Ignorar estos medios significaría dejar sin resguardo constitucional elementos esenciales para la intimidad de los ciudadanos. Sostiene que Carrió propone una interpretación amplia de la CN que protege la intimidad y la privacidad para garantizar el libre desarrollo de la personalidad, sostiene esta protección deriva del derecho a la defensa en juicio y del reconocimiento constitucional de derechos no enumerados (CN, arts. 18 y 33), extendiéndose a ámbitos donde las personas tienen una expectativa razonable de privacidad compatible con intereses estatales. (pp.69-70)

A diferencia de la privacidad en el artículo 19, la garantía de intimidad en el artículo 18 no es absoluta. Este artículo permite injerencias estatales en circunstancias específicas reguladas por la ley, tema tratado en los códigos procesales penales.

El artículo 13.8 de la Constitución de la Ciudad Autónoma de Buenos Aires establece que la privacidad abarca tanto las interceptaciones telefónicas como la "información personal almacenada". Además, este artículo estipula de manera explícita la necesidad de contar con una orden judicial para llevar a cabo acciones que impliquen una intromisión estatal en estos ámbitos protegidos.

Desde la reforma constitucional de 1994, conforme al artículo 75 inciso 22 de la CN, la protección de la intimidad no solo tiene un estatus constitucional, sino también convencional, al incorporarse los Tratados Internacionales de Derechos Humanos ratificados por el país. Por ejemplo, el artículo 12 de la Declaración Universal de Derechos Humanos aborda este tema, al igual que el artículo 17.1 del Pacto Internacional de Derechos Civiles y Políticos al establecer que “nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación”. El Comité de Derechos Humanos ha señalado que los Estados partes en el PIDCP tienen la obligación positiva de “adoptar medidas legislativas y de otra índole para dar efecto a la prohibición de tales interferencias y ataques, así como a la protección de este derecho privacidad.

En el ámbito regional, la Convención Americana sobre Derechos Humanos (CADH), en el artículo 11.2. establece que “nadie puede ser objeto de injerencia 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.”

La protección de la intimidad en el Código Procesal Penal Federal

Mera (s.f.) relata que estas disposiciones constitucionales se reflejan en los artículos 4 y 13 del nuevo Código Procesal Penal Federal (CPPF). El primero prácticamente reproduce la norma constitucional, garantizando que las declaraciones del imputado se realicen de manera libre. El segundo artículo protege la intimidad y las comunicaciones, las cuales pueden ser vulneradas solo mediante una orden judicial. No hay duda de que una interpretación flexible e integral de la Constitución abarca todo tipo de comunicaciones, ya sean correos electrónicos, llamadas telefónicas o mensajes de texto. Todo lo relacionado con la privacidad permanece fuera del alcance de las autoridades, salvo que exista una orden judicial. Sin embargo, no cualquier legislación es aceptable, solo aquellas que impongan restricciones razonables, conforme al artículo 28 de la CN.

El artículo 10 del CPPF establece que la validez de la prueba depende de su obtención e incorporación conforme a las previsiones constitucionales, internacionales y las disposiciones del propio código.

Las normas del procedimiento penal, que reglamentan las garantías constitucionales previamente mencionadas, junto con otras como el juez natural y el principio de legalidad, constituyen lo que se conoce genéricamente como debido proceso. Esto lleva al análisis de las prohibiciones de valoración probatoria o reglas de exclusión probatoria. De manera lógica, para dictar una condena, el Estado debe asegurar que las pruebas obtenidas en el proceso penal respeten las garantías constitucionales del ciudadano. De lo contrario, la solución es declarar la nulidad de la prueba, lo que conlleva la invalidez de la sentencia que se basa en ella. Por lo tanto, la decisión sobre los métodos que utiliza el Estado para descubrir la verdad implica que las autoridades encargadas de esta tarea deben cumplir con las normas que regulan la obtención de pruebas. (pp.8-10)

Guariglia (2005) señala que el legislador crea un mecanismo específico para afectar un

derecho, con el fin de adquirir una prueba tendiente a lograr la verdad, y si el órgano encargado de aplicar la norma la infringe, la consecuencia debe ser la invalidez del acto y la invalorabilidad de la prueba (p. 35).

Otra consecuencia que atribuye es la prohibición de valorar cualquier otra prueba que se derive de la obtenida ilícitamente, conocido como “teoría del fruto del árbol venenoso”. El fundamento para el autor es que el derecho procesal penal cumple una función protectora del imputado, y secundariamente de terceros. Agrega que la afectación de los derechos solo puede ser autorizada cuando el legislador lo establece, lo cual llama principio de reserva de ley (p. 198).

El artículo 3 del CPPF, al regular el principio de presunción de inocencia, establece que una sentencia de culpabilidad debe basarse en pruebas obtenidas legítimamente. Por lo tanto, se regulan de manera taxativa las intervenciones sobre el imputado que permiten que ceda la protección de su intimidad, garantizada por la inviolabilidad del domicilio, los documentos privados y las comunicaciones. Además, el CPPF regula detalladamente el acto de intimación de hechos y otras diligencias probatorias en las que el imputado participa. Ejemplos de regulaciones específicas se pueden encontrar en el artículo 150 del CPPF (interceptación y secuestro de comunicaciones), así como en el artículo 151, que regula la incautación de datos informáticos. El examen de los datos se encuentra regulado en el artículo 152 del CPPF.

Según Polansky (2023) la ley 27.063, que establece el Código Procesal Penal Federal, no contiene disposiciones específicas que regulen la extracción de información digital de dispositivos móviles ni la obtención de imágenes forenses de manera explícita. No obstante, este código permite el secuestro de dispositivos de almacenamiento digital, tratándolos en su artículo 151 como "componentes de un sistema informático" que pueden ser incautados en el marco de una medida investigativa, tal como un registro o una requisa.

No distingue entre datos digitales y otros tipos de evidencia que puedan ser secuestrados, aplicando el mismo requisito general: la presencia de testigos durante la incautación. Este requerimiento de testigos se aplica tanto al secuestro de dispositivos de almacenamiento digital como a la incautación de datos in situ. La normativa exige que los testigos sean ajenos a la fuerza de seguridad que realiza la medida, pero no especifica que deban tener conocimientos en informática, lo que refleja un enfoque similar al secuestro de objetos físicos más tradicionales.

La ausencia de peritos designados por los propietarios de la información digital, que podría mejorar significativamente el control de medidas que requieren conocimientos técnicos especializados, se debe a que estas acciones suelen llevarse a cabo de manera sorpresiva. Esto se hace, precisamente, para evitar la destrucción o el ocultamiento de la evidencia. Como resultado, el titular de los datos no tiene la posibilidad de convocar a expertos de su confianza con antelación para supervisar el procedimiento, ya que, en el mejor de los casos, recién se entera de la medida cuando esta se está ejecutando.

Aunque las mejores prácticas forenses sugieren que un experto en informática debería estar a cargo de la incautación de datos digitales in situ debido a la complejidad y especialización requeridas para manejar evidencia digital de manera segura, la ley 27.063 no establece explícitamente tal requisito. Este tipo de medidas se consideran como secuestros de elementos físicos, no como peritajes, lo que implica que no se requiere la intervención de peritos informáticos en el lugar de los hechos.

La normativa no aborda la denominada "instancia intermedia", es decir, no regula de manera detallada las etapas posteriores al secuestro inicial de dispositivos, como la extracción y análisis de los datos digitales contenidos en ellos. En cambio, se enfoca en asegurar un mínimo de control durante la incautación mediante la presencia de testigos, a pesar de la

volatilidad y fragilidad inherente a la evidencia digital, así como el riesgo de alteraciones maliciosas. Este enfoque de la ley busca proporcionar una salvaguarda básica para proteger la integridad de la prueba obtenida en el proceso penal. (pp.115-118)

La necesidad de regulación específica para la evidencia digital: Un enfoque hacia la protección de la privacidad.

En las situaciones no reguladas explícitamente por la ley, se recurre a la "libertad probatoria", la cual permite la obtención de pruebas mediante diversos métodos, siempre que no se vulneren los derechos constitucionales. Esta práctica está respaldada por el artículo 134 del Código Procesal Penal Federal (CPPF).

> Libertad probatoria. Podrán probarse los hechos y circunstancias de interés para la solución correcta 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.

El principio de libertad probatoria que rige el derecho procesal penal, en materia de admisibilidad de las medidas de coerción, se encuentra regido por limitaciones referidas a la necesidad, razonabilidad y proporcionalidad presentes en el articulo 16 del CPPF

> Restricción de derechos fundamentales. Las facultades que este Código reconoce para restringir o limitar el goce de derechos reconocidos por la Constitución Nacional o por los instrumentos internacionales de Derechos Humanos deben ejercerse de conformidad con los principios de idoneidad, razonabilidad, proporcionalidad y necesariedad

Sin embargo la aplicación de este principio es cuestionada por Pérez Barberá (2009), quien

sostiene que en materia procesal penal también debe regir la protección constitucional amplia de prohibición de analogía de la ley *in malam parte*, ya que incluir por analogía normas procesales que no han sido expresamente previstas genera un perjuicio a la posición del imputado en el proceso. (p.365)

La falta de regulaciones procesales específicas para distintos tipos de evidencia digital ha llevado a compensar esta carencia mediante el principio de libertad probatoria. El problema es que, en la mayoría de los casos, esto se realiza sin un análisis adecuado de las restricciones constitucionales ni de cómo debe aplicarse este principio.

Según argumenta Sergi (2018) el principio nulla coactio sine lege establece que todos los métodos de investigación, procedimientos probatorios o medios de prueba que supongan algún grado de injerencia (o uso de coerción) en el ámbito de los derechos fundamentales reconocidos por la Constitución Nacional o por los Pactos Internacionales de Derechos Humanos con jerarquía constitucional (artículo 75, inciso 22 de la CN), deben estar específicamente previstos en leyes, que deben cumplir con los requisitos establecidos por la reglamentación constitucional. Esta reglamentación garantiza que la ley no altere ni sustituya el principio constitucional que regula (artículos 14, 19 segunda parte y 28 de la CN, y de manera expresa, el artículo 30 de la Convención Americana de Derechos Humanos)

De acuerdo con este principio, también vinculado al principio de legalidad o de reserva (distinto del principio con la misma denominación que rige la actividad penal – nullum crimen sine lege), todas las actividades del Estado, incluyendo la actividad probatoria en los procesos penales, que interfieran en los derechos fundamentales de los ciudadanos, requieren una autorización legal previa como condición de validez. (p.65)

En relación específica con la cuestión de la evidencia digital, Salt (2017) argumenta que el principio de libertad probatoria entra en conflicto con el principio de nulla coactio sine lege,

que establece que todos los medios de prueba que involucren algún nivel de intervención en los derechos fundamentales, o que utilicen la coerción, deben estar obligatoriamente previstos en la legislación y alinearse con los estándares constitucionales en cuanto a la regulación de derechos. (p.106)

Respecto al fundamento de este principio, se puede afirmar que su establecimiento busca imponer límites al ejercicio de la autoridad estatal, para evitar que las intervenciones en los derechos fundamentales de las personas, en este contexto, se vuelvan abusivas o arbitrarias. Aunque los derechos fundamentales pueden estar sujetos a limitaciones o restricciones, estas deben siempre cumplir con ciertos requisitos especificados en el artículo 30 de la CADH, los cuales actúan como límites al poder estatal, este articulo dispone el principio de reserva legal de la siguiente manera

> Alcance de las restricciones: Las restricciones permitidas, de acuerdo con esta Convención, al goce y ejercicio de los derechos y libertades reconocidas en la misma, no pueden ser aplicadas sino conforme a leyes que se dictaren por razones de interés general y con el propósito para el cual han sido establecidas.

Bruzzone (2005) siguiendo la línea de pensamiento de Maier, profundiza en la necesidad de desarrollar una teoría general de las medidas de coerción que establezca bases jurídicas más sólidas para evaluar la pertinencia y proporcionalidad de las medidas, sugiere que la imposición de una medida de coerción debería seguir un proceso similar al utilizado para la imposición de penas, considerando la existencia de una “tipicidad procesal” que defina claramente los tipos de medidas de coerción. Advierte que es crucial diferenciar entre medios de prueba y medidas de coerción, ya que, mientras el sistema argentino permite una amplia libertad probatoria, las medidas de coerción que obtienen pruebas deben estar claramente delimitadas para evitar confusiones y garantizar la protección de los derechos del ciudadano.

(pp.241-253)

Según Sergi (2018) en Argentina, la aplicación del principio de libertad probatoria en el contexto de la evidencia digital presenta varios desafíos que pueden afectar la protección del derecho a la intimidad.

A pesar de que esta problemática ha sido objeto de discusión durante años, el sistema judicial no ha identificado correctamente los problemas jurídicos subyacentes, tales como la invasión de ciertos ámbitos de privacidad que quedan desprotegidos y la falta de certeza respecto a la validez de elementos probatorios obtenidos de manera ilegítima. Con frecuencia, se confunde la validez de las garantías constitucionales con la certeza de la prueba presentada, cuestiones que son claramente diferentes. No obstante, esto no implica que toda aplicación analógica deba ser considerada inconstitucional. No es evidente que el acceso a ciertos ámbitos protegidos a través de medios tecnológicos, informáticos o electrónicos no esté previsto en la ley. Lo relevante no es el medio utilizado, sino los requisitos legales necesarios para el acceso a esa información. En este contexto, se puede argumentar, aunque no sin controversia, que el legislador ha permitido tales intrusiones. El desafío radica en cómo implementarlas correctamente.

El acceso a sistemas informáticos, por su naturaleza coercitiva, debe ser ordenado por un juez y cumplir con los requisitos formales establecidos para la intrusión en ámbitos privados. Esto incluye una justificación adecuada que explique la necesidad de dicha intrusión, criterios de proporcionalidad y la minimización de posibles daños a la intimidad. La legitimidad de estas medidas depende del grado de intrusión y de los requisitos específicos que deben cumplir, teniendo en cuenta la extensión y gravedad de la misma.

No se puede sostener de manera seria que todas las medidas sobre sistemas informáticos estén prohibidas por falta de regulación específica, ya que lo fundamental es el grado de

afectación al derecho a la intimidad y no el medio utilizado. La legitimidad de una medida dependerá de las circunstancias específicas de cada caso y del nivel de intromisión involucrado. En algunos casos, cumplir con los requisitos para órdenes de allanamiento, intervención de correspondencia o comunicaciones puede ser necesario, no solo en la emisión de la orden, sino también en su ejecución, y puede implicar la delimitación temporal de la medida.

El tratamiento uniforme de la evidencia digital por parte del sistema judicial, simplificando las soluciones y unificando las circunstancias, constituye un error que puede poner en riesgo la validez de las medidas adoptadas. Aunque no siempre es obligatorio desde el punto de vista constitucional, puede ser adecuado como política criminal que el legislador regule explícitamente estas cuestiones. Sin embargo, esta no es la única solución; también es crucial mejorar la formación de los operadores del sistema y fortalecer los equipos técnicos especializados en informática.

La intervención tecnológica en la privacidad de los ciudadanos requiere una regulación rigurosa y detallada cuando sea necesaria, para proteger adecuadamente los derechos fundamentales. Esta regulación debe ser lo suficientemente general como para adaptarse a los constantes avances tecnológicos, estableciendo limitaciones legales, temporales y requisitos específicos que brinden certeza a los elementos probatorios, permitiendo al sistema de justicia penal adaptarse a nuevos medios y tecnologías emergentes. (pp.97-98)

Consideraciones para la protección de la privacidad en la investigación judicial y la extracción de información de teléfonos celulares.

Para concluir este trabajo, en que se ha evidenciado importantes lagunas legislativas en referencia a la evidencia digital, se sugieren y recomiendan medidas clave para mejorar la protección de la privacidad durante las investigaciones judiciales.

- Asegurar que todas las actividades de vigilancia se ajusten al artículo 17 del Pacto Internacional de Derechos Civiles y Políticos (PIDCP). Esto implica adoptar medidas que garanticen que cualquier interferencia con el derecho a la privacidad cumpla con los principios de legalidad, proporcionalidad y necesidad, sin importar la nacionalidad o ubicación de los individuos cuya información se vigila.

- Garantizar que cualquier reforma del Código Procesal Penal respete las obligaciones nacionales e internacionales en materia de derechos humanos, con un enfoque particular en el derecho a la privacidad.

- Incluir disposiciones específicas sobre la protección de datos y la privacidad durante el proceso judicial.

- Aunque las herramientas forenses están protegidas por el secreto comercial, es crucial proporcionar al menos una información básica sobre su funcionamiento. Debe encontrarse un equilibrio entre mantener el secreto comercial y asegurar que se respete el derecho de defensa y la privacidad de las personas afectadas por la información extraída. La admisibilidad de estas herramientas en los procesos judiciales debe depender de que se garantice una metodología confiable y que los resultados obtenidos no hayan sido manipulados. Para lograr esto, es esencial promover la transparencia y el control sobre el funcionamiento de estas herramientas, considerando estos principios como prioritarios sobre la protección del secreto comercial.

- Las autoridades que emplean estas herramientas deben tener una normativa de acceso público específica que asegure el debido proceso y el derecho de defensa en su uso. Aunque el Ministerio Público Fiscal de la Nación ha proporcionado información sobre los protocolos generales para la extracción de pruebas, incluidos los digitales, no se detallan estándares específicos para las herramientas forenses utilizadas en teléfonos celulares.Es

esencial que existan normas claras para garantizar un control adecuado de las pruebas por parte de los afectados y permitirles impugnar cualquier manipulación incorrecta o ilegal durante el proceso de extracción. Además, la selección de proveedores de estas herramientas debe cumplir con criterios de confiabilidad verificables, de acuerdo con lo estipulado en la normativa correspondiente.

- Legislación sobre el análisis de información. Debido a la gran cantidad de datos personales y de terceros almacenados en los teléfonos celulares, la extracción de información debe restringirse únicamente al caso específico y al propósito concreto que se persigue, minimizando el impacto sobre la privacidad de terceros. La recolección de pruebas en un proceso penal debe ajustarse estrictamente a lo necesario para el caso y no debe extenderse más allá de los datos pertinentes.

- Legislación sobre el almacenamiento de la información extraída. Una cuestión clave es la falta de claridad sobre cómo se almacena la información obtenida mediante estas herramientas. Es necesario definir si esta información se guarda en servidores de la institución que realiza la pericia o en los servidores de la empresa proveedora del software.La institución encargada del almacenamiento debería implementar medidas de seguridad adecuadas para asegurar la integridad y protección de la información, garantizando tanto el derecho al debido proceso como la privacidad de las personas implicadas.

- Legislación sobre la eliminación de la información extraída y no relevante. La información obtenida mediante herramientas forenses de teléfonos celulares no debe ser retenida más allá del tiempo necesario para la investigación en curso. Es fundamental establecer directrices claras que estipulen la eliminación definitiva de la información una vez transcurrido un período específico. Además, es crucial subrayar que cualquier

información extraída del teléfono que no sea relevante para el caso en cuestión debe ser eliminada de inmediato, especialmente si dicha información pertenece a terceros.

- Sería aconsejable que, al utilizar herramientas de extracción forense para dispositivos móviles, los informes incluyan un porcentaje que refleje el margen de error de estas tecnologías. Incluir esta información es fundamental, ya que facilita a la defensa la impugnación y cuestionamiento de la validez de la prueba, y garantiza que los jueces y juezas puedan hacer una evaluación precisa y fundamentada de las evidencias presentadas.

- Capacitar a los operadores judiciales en el uso de tecnologías de extracción forense, ya que la investigación revela que existe un conocimiento insuficiente tanto sobre el funcionamiento de estas herramientas como sobre su rol procesal. Esta falta de entendimiento afecta directamente el desarrollo del proceso judicial y las garantías legales involucradas. La formación adecuada permitirá a los operadores judiciales valorar correctamente las pruebas obtenidas y asegurar que su uso se ajuste al debido proceso y al derecho de defensa, protegiendo así los derechos de las personas implicadas.

-A medida que las tecnologías reemplazan a los técnicos y peritos forenses, es esencial asegurar una participación significativa de seres humanos en el proceso. Esta intervención debe ser realmente sustantiva y no limitarse a tareas básicas como conectar o manejar el software o hardware. La intervención humana debe involucrar una supervisión directa y activa en el uso y los resultados de estas herramientas, para evitar que las decisiones sean tomadas de manera arbitraria por las tecnologías.

Conclusión

El análisis de la vulneración del derecho a la intimidad en el contexto del análisis forense de dispositivos móviles revela una problemática compleja y multifacética que afecta tanto a la

integridad del proceso penal como a la protección de los derechos fundamentales. La rápida evolución de la tecnología y la proliferación de dispositivos móviles han cambiado drásticamente el panorama de la evidencia digital, poniendo de relieve la insuficiencia de las normativas actuales para abordar estos nuevos desafíos.

A lo largo de este trabajo se han examinado las implicancias legales, éticas y prácticas del uso de tecnologías avanzadas para la extracción y análisis de datos, destacando las carencias en la regulación actual y proponiendo la necesidad de reformas profundas y específicas.

Los dispositivos móviles contienen una gran cantidad de información personal y sensible, lo que los convierte en una fuente de evidencia potencialmente valiosa, pero también en un punto crítico de vulneración de la privacidad. El derecho a la intimidad, protegido por la Constitución Nacional y diversos tratados internacionales de derechos humanos, exige que cualquier injerencia en la esfera privada de un individuo sea estrictamente necesaria, proporcionada y respaldada por una orden judicial. Sin embargo, en la práctica, la utilización de herramientas forenses a menudo permiten el acceso masivo a datos almacenados en estos dispositivos sin un control judicial adecuado ni protocolos claros que garanticen la protección de la intimidad. Esta situación genera una tensión directa con los principios fundamentales de la legalidad y el debido proceso. La ausencia de normativas claras que distingan entre los diferentes tipos de datos que se pueden extraer y los niveles de sensibilidad de la información obtenida aumenta el riesgo de abusos.

El vacío normativo en torno a la regulación de la evidencia digital, particularmente en jurisdicciones como la provincia de Santa Fe, contrasta con los avances legislativos en otras regiones, como Salta, que ha incluido la evidencia digital en investigaciones judiciales, procurando siempre la menor afectación posible a los derechos de las personas investigadas conforme a las necesidades de la investigación Esta disparidad regional subraya la necesidad

de un enfoque uniforme y coherente a nivel nacional que brinde claridad sobre las condiciones bajo las cuales se puede acceder a la información almacenada en dispositivos móviles.

Uno de los problemas centrales radica en la ambigüedad sobre el carácter judicial de la extracción de información de dispositivos móviles. La ausencia de una definición clara sobre si tales extracciones deben considerarse pericias o secuestros de información, y si requieren una orden judicial específica y notificación a la defensa, resalta la falta de normas precisas que protejan adecuadamente los derechos de los imputados. Esta indefinición genera incertidumbre jurídica y coloca a los operadores judiciales en una posición en la que deben interpretar las categorías jurídicas sin una guía clara, lo que puede resultar en prácticas inconsistentes y potencialmente injustas.

Además, la confiabilidad de las herramientas de extracción forense y su margen de error son aspectos fundamentales que aún no están debidamente establecidos. La falta de estándares claros para la evaluación de estos elementos pone en riesgo la integridad de la evidencia digital y, por ende, la validez de los procesos judiciales basados en dicha evidencia. La jurisprudencia actual (véase Anexo), a menudo carente de un enfoque sólido sobre la evidencia digital, refleja una comprensión insuficiente de la materia por parte de los operadores judiciales.

La doctrina y jurisprudencia, como señala el Dr. Marcos Salt, han destacado la importancia de establecer criterios claros para la autorización judicial, la notificación a las partes y el uso de tecnologías de extracción de datos para proteger los derechos fundamentales.

Este enfoque debe incluir una distinción clara entre las medidas que pueden considerarse invasivas de la privacidad (como el acceso a comunicaciones privadas) y aquellas que son menos intrusivas.

En el ámbito comparativo, países como España y Alemania han adoptado enfoques legislativos que buscan equilibrar la lucha contra el crimen con la protección de los derechos individuales. Estos modelos ofrecen valiosas lecciones para el desarrollo de una legislación argentina que respete el derecho a la intimidad mientras se permite el uso legítimo de la evidencia digital en procesos judiciales. La implementación de estándares internacionales y las mejores prácticas en la recolección y análisis de datos digitales contribuirían a reducir las posibilidades de abuso y a fortalecer la confianza en el sistema judicial.

La aplicación del principio de "libertad probatoria" sin tener en cuenta las características particulares de la tecnología moderna ha resultado en la incorporación inadecuada de evidencia digital bajo normas pensadas para pruebas físicas. Esta flexibilidad, si no se ajusta adecuadamente, puede llevar a medidas desproporcionadas que afectan los derechos de los ciudadanos. La analogía con prácticas anteriores no siempre protege de manera efectiva la intimidad, por ello, es crucial que las decisiones judiciales tomen en cuenta el grado de intromisión en la vida privada y cumplan con los requisitos legales específicos de cada caso.

En Argentina, la adaptación del sistema a estos desafíos ha sido insuficiente. Aunque el país ha ratificado la Convención de Budapest, que busca unificar normas a nivel internacional, esta ratificación no ha resuelto los problemas procesales internos. La especialización en delitos informáticos ha llevado a una fragmentación que no aborda la problemática de manera integral. Es crucial que la regulación se enfoque no solo en aspectos técnicos, sino también en el desarrollo de estándares jurídicos que aseguren la protección adecuada de los derechos de los ciudadanos.

En conclusión, el acceso a sistemas informáticos debe considerarse una medida coercitiva que requiere autorización judicial, y debe cumplir con los requisitos formales establecidos para intervenir en esferas de intimidad. La autorización debe estar debidamente motivada,

justificar claramente la necesidad del grado de intrusión, y aplicar criterios de proporcionalidad para minimizar el impacto sobre la intimidad. La legitimidad de la medida dependerá de una evaluación cuidadosa del nivel y la gravedad de la intrusión.

Por ello el uso de herramientas forenses para la extracción y análisis de datos en dispositivos móviles presenta un desafío significativo para la protección del derecho a la intimidad. La necesidad de regulaciones específicas y detalladas es imperativa para evitar abusos y garantizar que las investigaciones judiciales se realicen en un marco de respeto a los derechos fundamentales. La adopción de un marco normativo claro, basado en los principios de necesidad, proporcionalidad y transparencia, será crucial para proteger la privacidad de los individuos y para asegurar que el proceso penal no se vea comprometido por prácticas invasivas y carentes de control adecuado.

Además, es fundamental que este esfuerzo incluya la formación y capacitación continua de los operadores del sistema judicial, la actualización constante de las normativas y la creación de mecanismos efectivos de supervisión y control para el uso de tecnologías forenses. Solo mediante estas acciones se podrá proteger adecuadamente la privacidad de los individuos y asegurar la efectividad y justicia del proceso penal en el contexto de la evidencia digital.

Anexo

Jurisprudencia nacional e internacional

Validez de allanamiento, secuestro de teléfonos celulares y calificación legal.

"Osuna, Claudio Alberto s/ Recurso de casación"Causa n°: 13994. Tribunal: Cámara Nacional de Casación Penal - Sala II .Fecha de Resolución: 09/03/2011.

La orden de allanamiento fue emitida tras recibir una denuncia anónima que señalaba que Osuna podría tener en su posesión un FAL similar a uno de los sustraídos en el hecho investigado. El Tribunal consideró que la denuncia anónima, corroborada con los datos verificables sobre el lugar y las personas involucradas, justificaba la medida de allanamiento. La orden fue considerada motivada y legalmente válida.

El Tribunal determinó que el peritaje sobre los teléfonos celulares, secuestrados durante el allanamiento, no vulneró el derecho a la intimidad, dado que la invasión del ámbito privado ya había sido autorizada y realizada con base en la orden judicial.

Se validó la calificación legal que consideró a la privación ilegítima de libertad y el robo como delitos independientes. El Tribunal señaló que la privación de libertad no se consumió con el robo, ya que se trató de una circunstancia que prolongó el delito o buscó asegurar la impunidad del robo. Los hechos se consideraron independientes tanto material como jurídicamente.

Dado que no se probó la aptitud para el disparo de las armas involucradas, el Tribunal aplicó el principio in dubio pro reo para recalificar el hecho bajo el artículo 166, inciso 2° in fine del Código Penal, ajustando la calificación según la falta de prueba sobre la capacidad operativa de las armas.

Los disidentes (Dres. Yacobucci, García y Mitchell) argumentaron que la orden de allanamiento no cumplía con las garantías constitucionales establecidas en los artículos 18 y 19 de la Constitución Nacional. Según la disidencia, no es suficiente que las autoridades

tuvieran una sospecha razonable; se requiere que haya elementos objetivos concretos para justificar la medida. La disidencia cuestionó la validez de la orden de allanamiento y las condiciones de garantía para evitar injerencias arbitrarias.

La Cámara Nacional de Casación Penal resolvió que la orden de allanamiento y la subsecuente incautación de los teléfonos celulares fueron legales y no vulneraron derechos constitucionales. La calificación de los delitos como independientes se mantuvo, y se ajustó la imputación de acuerdo con el principio in dubio pro reo. La disidencia, al señalar una falta de garantía en la sospecha inicial, no logró modificar la decisión mayoritaria del Tribunal.

Falta de notificación de la defensa de la realización de extracción.

"Bogado Ortega, F. Nulidad peritaje. Robo agravado." Expediente: CCC 50941/2022/1/CA2. Fecha: 6 de diciembre de 2022 Tribunal: Cámara Nacional de Apelaciones en lo Criminal y Correccional, Sala 7. Juez de Primera Instancia: Juzgado Nacional en lo Criminal y Correccional Nº 33

En el caso de F. Bogado Ortega, la defensa oficial apeló una decisión del juzgado de primera instancia que había rechazado un planteo de nulidad. El planteo de nulidad se refería a la extracción de información de teléfonos celulares secuestrados en el domicilio de Bogado Ortega. La defensa alegaba que, al no haber sido notificada de la realización de esta extracción, se había vulnerado el derecho de defensa de su cliente, dado que se trataba de un acto definitivo e irreproducible.

De acuerdo con la fiscalía, solo se realizó la extracción de datos de uno de los teléfonos celulares secuestrados utilizando un programa específico. No se pudo desbloquear ni extraer información de los otros dispositivos incautados.

La defensa pidió la anulación de lo actuado en relación con la extracción de datos, argumentando que la medida afectó su derecho de defensa al no haber sido notificada.

La Cámara Nacional de Apelaciones en lo Criminal y Correccional, Sala 7, decidió confirmar la resolución del juzgado de primera instancia, rechazó el planteo de nulidad y la medida impugnada. Los puntos clave de la decisión fueron:

El tribunal consideró que no se habían vulnerado normas del ordenamiento adjetivo ni garantías constitucionales. La extracción de datos se consideró reproducible y no incurrió en vicios que justificaran su anulación.

Aunque se discutió si la extracción de datos debía considerarse un informe técnico o un peritaje, la Sala argumentó que lo importante era que la extracción podía ser reproducida. Esto significaba que el procedimiento no afectó de manera irreversible el derecho de defensa del imputado. No se advirtió un concreto perjuicio que comprometiera la cadena de custodia de los datos o la evidencia en sí. La sala no encontró justificación para aplicar una sanción procesal restrictiva en este caso.

La Cámara de Apelaciones confirmó ese criterio, al entender que la diligencia que es reproducible más allá de la discusión que pudiere suscitarse en torno a si se trata de un informe técnico (art. 184, inc. 4°, del CPPN), que no está sometido al régimen de los exámenes periciales, propiamente de un peritaje -como lo afirma la defensa- o de una indagación de características simples -según la resolución apelada.

"A., J. A. y otros s/ nulidad. DET Asociación ilícita y otros” Expediente:CCC 81978/2018/11/CA9. Fecha:20 de septiembre de 2019. Tribunal: Cámara Nacional de Apelaciones en lo Criminal y Correccional, Sala 4. Juzgado de Primera Instancia: Juzgado Criminal y Correccional Nº 53

Las defensas de los imputados J. A. A., A. E. S., y Y. M. O. presentaron recursos de apelación contra un auto que rechazó su planteo de nulidad. La nulidad se refería al acceso y extracción de datos de teléfonos celulares incautados, alegando que dicha medida no había sido

notificada a la defensa.

Los teléfonos celulares fueron incautados y se procedió a su apertura para extraer la información contenida en ellos. Las defensas argumentaron que esta medida era nula porque no fueron notificadas previamente. El tribunal de primera instancia denegó la nulidad, considerando que la medida no violaba las normas procesales aplicables.

La defensa de J. A. A. no se presentó para sustentar su recurso, por lo que el Tribunal consideró que la apelación de esta parte debía ser desestimada conforme al artículo 454, segundo párrafo del Código Procesal Penal de la Nación (CPPN).

La Cámara clasificó la extracción de datos como una operación de copia de la información almacenada en los teléfonos celulares, y no como un peritaje. Por lo tanto, no se requería la notificación previa a la defensa.

La operación de extracción de datos fue considerada como una diligencia para preservar y copiar elementos ya incautados, regulada por el artículo 233 del CPPN.

Se destacó que el artículo 144 de la Ley 27.063 también autoriza el registro y la copia de datos informáticos sin necesidad de notificación previa a la defensa.

La medida no constituía un peritaje (según el artículo 253 del CPPN) y, por tanto, no requería la notificación a la defensa.

El Tribunal argumentó que la medida cumplió con las formalidades legales y no afectó derechos constitucionales, como el derecho de defensa.

Los apelantes cuestionaron la cadena de custodia de los teléfonos, sugiriendo que podría haber habido alteración de los datos. Sin embargo, esto se consideró una conjetura sin evidencia concreta.

El Tribunal destacó que las dudas sobre la cadena de custodia no debían llevar a la exclusión de la prueba sino a intentar resolver esas dudas mediante peritajes u otras medidas probatorias

si fuera necesario. Asimismo enfatizó que los cuestionamientos relacionados con la cadena de custodia y la integridad de los datos deben ser abordados bajo el principio de la sana crítica racional. Este principio implica que la valoración de las pruebas se debe hacer de manera objetiva y razonada, considerando toda la evidencia disponible.

La sana crítica racional permite que las partes cuestionen la validez y la fiabilidad de las pruebas, pero tales cuestionamientos no deben ser meras especulaciones. En este caso, los alegatos de la defensa sobre posibles alteraciones de datos fueron considerados como conjeturas sin pruebas concretas de afectación a los datos originales.

En cuanto al software utilizado, el Tribunal indicó que los datos fueron extraídos usando el software "UFED 4PC". Este es un programa especializado en la extracción forense de información de teléfonos móviles, que es ampliamente aceptado y utilizado en investigaciones forenses. La utilización del software UFED se destacó como una herramienta estándar para la extracción forense, que ayuda a garantizar la integridad y la preservación de los datos durante el proceso de copia. La Cámara no encontró irregularidades en el uso de este software, ya que se utiliza en conformidad con las normas técnicas y procesales vigentes para la preservación de datos electrónicos.

La Cámara concluyó que la medida de extracción de datos no fue nula ya que se ajustó a las normativas aplicables y no afectó el derecho de defensa.

Las formalidades legales fueron observadas y no se demostró perjuicio concreto alguno que justificara la nulidad. La Cámara Nacional de Apelaciones en lo Criminal y Correccional, Sala 4, resolvió confirmar el auto de fs. 12/15, rechazando los recursos de nulidad interpuestos y manteniendo la validez de las actuaciones relacionadas con la extracción de datos de los teléfonos celulares.

"Shen, Yongchao s/Infracción Ley 23.737". Tribunal Oral en lo Criminal Federal N° 1.

Junio de 2022

El Tribunal determinó que la descarga repetida de información de un teléfono celular mediante una herramienta UFED no constituye una nueva pericia, ya que la primera descarga ya había cumplido esa función. Un aspecto relevante de este fallo es que la defensa alegó una violación de la privacidad debido a la repetición del procedimiento de extracción de datos. En respuesta, el tribunal resolvió que solo se utilizaría en el juicio la información obtenida que estuviera directamente relacionada con los hechos del caso, sin especificar qué sucederá con el resto de los datos extraídos. (Balcarce, 2022)

Balcarce (2022) remarca que en ambos fallos, el cuestionamiento se centra en la notificación y la reiteración del procedimiento de extracción de datos, no en las tecnologías utilizadas ni en su fiabilidad. Sin embargo, ninguna de las sentencias aborda la importancia de verificar el hash en la primera extracción de datos, un algoritmo que asegura que la información extraída coincida con la original. Cambios en el hash indicarían alteraciones en los datos, lo cual es crucial para mantener la cadena de custodia.

La judicatura aún no ha definido claramente aspectos fundamentales de la investigación digital, como si la evidencia es el dispositivo o la información extraída, ni el carácter judicial de la extracción de datos, si debe ser considerada una pericia o un secuestro de información, y si requiere una orden judicial expresa o notificación a la defensa. Estas definiciones, aunque parecen categorías jurídicas menores, son cruciales para proteger los derechos de defensa y el debido proceso.

Es importante señalar que no se ha establecido la confiabilidad ni el margen de error de las herramientas de extracción forense, lo que es esencial para valorar adecuadamente los datos obtenidos. La jurisprudencia muestra una falta de comprensión sobre la evidencia digital y un acercamiento limitado de los jueces a estos temas, generando una incertidumbre jurídica que

necesita ser resuelta urgentemente para alinear la práctica judicial con los estándares de protección de derechos fundamentales y actualizar la labor en la extracción forense de información digital.

Inspección irregular de celulares

"G., F.J. S/ Nulidad" CCC 37443/2018/2/CA2 . Fecha: 31 de julio de 2018. Juzgado de Primera Instancia:Juzgado Nacional en lo Criminal y Correccional N.º 5. Tribunal: Cámara Nacional de Apelaciones en lo Criminal y Correccional - Sala 6

La defensa oficial de F. J. G. apeló contra el auto del Juzgado Nacional en lo Criminal y Correccional N.º 5 que rechazó el planteo de nulidad relacionado con la inspección del celular realizada durante el procedimiento policial. La apelación se centró en cuestionar la legalidad del procedimiento llevado a cabo por el inspector Pedro Alejandro Galian, quien inspeccionó el celular de G. durante la detención del imputado en conexión con un presunto delito de desapoderamiento del teléfono celular de la víctima.

La defensa argumentó que la inspección del celular por Galian no se realizó de acuerdo con los artículos 184 inciso 2 y 230 bis del Código Procesal Penal de la Nación. Se alegó que la inspección no contaba con la autorización judicial necesaria, ni se justificaba por una urgencia que permitiera el desbloqueo del dispositivo y la extracción del chip para realizar una llamada.

El Tribunal determinó que la inspección del celular fue llevada a cabo en condiciones irregulares. El inspector Galian actuó fuera del marco de intervención permitido por la ley, ya que no había una situación de urgencia que justificara su actuación y la falta de autorización judicial para proceder de esa manera resultó en una violación de los procedimientos establecidos.

La medida afectó el derecho de defensa del imputado, quien no tuvo oportunidad de controlar

la prueba obtenida ni de cuestionar su validez. Se destacó la vulneración del derecho a la privacidad y la inviolabilidad del domicilio y correspondencia, conforme a los artículos 18 de la Constitución Nacional y tratados internacionales, que protegen la privacidad y los datos personales.

El Tribunal subrayó la necesidad de seguir protocolos específicos para el manejo de evidencia digital. Los procedimientos establecidos son cruciales para garantizar la integridad de la prueba y proteger los derechos fundamentales del imputado, los cuales no fueron respetados en este caso.

La Cámara Nacional de Apelaciones en lo Criminal y Correccional resolvió declarar la nulidad de la requisa del celular realizada por el inspector Galian. Dado que la intervención y la recolección de evidencia se realizaron sin la debida autorización judicial y fuera de los protocolos legales, el procedimiento fue invalidado.

El Tribunal resolvió el sobreseimiento de F. J. G. al considerar que la evidencia obtenida a través de un procedimiento irregular no puede ser utilizada para sustentar una condena. Se dispuso la inmediata libertad del imputado.

“Estados Unidos contra Wurie”. Núm. 11–1792. Resuelto: 17 de mayo de 2013

Tribunal de Apelaciones de los Estados Unidos, Primer Circuito.

El 5 de septiembre de 2007, el sargento detective Paul Murphy observó a Brima Wurie aparentemente involucrado en una transacción de drogas. Posteriormente, Wurie fue arrestado y llevado a la estación de policía. Durante el arresto, se le confiscaron a Wurie dos teléfonos celulares, entre otros artículos. Poco después de llegar a la estación, los oficiales notaron que uno de los teléfonos estaba recibiendo llamadas repetidas de un número que identificaron como "mi casa" en la pantalla. Los oficiales examinaron el teléfono sin una orden judicial. Accedieron al registro de llamadas, identificaron el número y la dirección asociada. Luego,

obtuvieron una orden judicial para buscar en esa dirección, donde encontraron evidencia adicional que llevó a la condena de Wurie.

Wurie presentó una moción para suprimir la evidencia obtenida del teléfono celular, argumentando que la búsqueda sin una orden judicial violó sus derechos constitucionales. El tribunal de distrito desestimó la moción y Wurie fue condenado. Posteriormente, apeló la decisión.

El Tribunal de Apelaciones del Primer Circuito revocó la decisión del tribunal de distrito y anuló la condena de Wurie. La corte concluyó que:

La búsqueda de datos en un teléfono celular no puede ser justificada por la excepción de "búsqueda incidental al arresto". Aunque los artículos físicamente asociados con una persona arrestada pueden ser registrados sin una orden judicial, la búsqueda de información en un teléfono celular es diferente en naturaleza y alcance.

Los datos contenidos en un teléfono celular son extensos y profundos, lo que difiere significativamente de los artículos físicos que se pueden revisar rápidamente. La Corte reconoció que los datos digitales tienen un potencial de intrusión mayor y requieren una protección más estricta bajo la Cuarta Enmienda.

La corte observó que la policía podría haber solicitado una orden judicial antes de revisar el teléfono, y que no existía una justificación adecuada para realizar la búsqueda sin una orden, como una amenaza inmediata de destrucción de pruebas.

La decisión en Estados Unidos v. Wurie establece un precedente importante en la protección de la privacidad digital, aunque la búsqueda incidental al arresto puede ser válida para ciertos artículos físicos, la búsqueda de datos en dispositivos electrónicos como teléfonos celulares requiere una orden judicial para ser considerada legal y razonable bajo la Cuarta Enmienda.

“Riley v. California”. Fecha de Resolución: 25 de junio de 2014 . Tribunal: Corte Suprema

de los Estados Unidos

Es el primer intento de la Corte Suprema de los Estados Unidos de regular las inspecciones de teléfonos celulares por parte de las fuerzas del orden. La decisión unánime de 2014 exige una orden judicial para todas las inspecciones de teléfonos celulares que tengan como objetivo la detención, salvo que se trate de una emergencia.

En este caso, la policía requisó el teléfono celular del imputado, David Riley, tras su detención por conducir con licencia vencida. La información contenida en el teléfono, como videos y fotografías, fue utilizada como evidencia para acusarlo de participar en un tiroteo.

La Corte Suprema revocó la sentencia en el caso de Riley, estableciendo que, aunque los oficiales pueden examinar físicamente un teléfono celular para asegurarse de que no represente una amenaza física, la inspección de los datos del teléfono requiere una orden judicial.Destacó que los teléfonos celulares modernos tienen una capacidad de almacenamiento inmensa y pueden contener una gran cantidad de información personal, incluyendo registros de llamadas, mensajes, fotos y aplicaciones que revelan aspectos significativos de la vida privada del individuo. Esta información es cualitativamente diferente de los registros físicos tradicionales debido a su naturaleza extensiva y detallada.

La Corte enfatizó que la inspección de los datos almacenados en un teléfono celular debe estar sujeta a una orden judicial, ya que la privacidad de la información contenida en estos dispositivos es altamente protegida por la Constitución, argumentó que la tecnología no disminuye la necesidad de protección constitucional de la intimidad personal.

Se reiteró que el requisito de obtener una orden judicial antes de registrar un teléfono celular es una parte esencial del sistema legal y protege los derechos fundamentales contra intrusiones arbitrarias. Esta medida asegura que la recolección de evidencia digital se realice conforme a las garantías constitucionales, por ello determinó que la requisa de datos en el

teléfono celular de Riley sin una orden judicial era inconstitucional y que la evidencia obtenida a través de esta requisa no podía ser utilizada para fundamentar una condena.

Como observamos, ambos casos se focalizaron en la búsqueda de información almacenada en un teléfono celular inteligente por parte de las fuerzas de seguridad sin contar con la debida orden judicial que así lo disponga. El máximo tribunal sostuvo que los teléfonos celulares modernos tienen una inmensa capacidad de almacenamiento, lo que los distingue significativamente de los registros físicos tradicionales. A diferencia de los registros físicos, que generalmente limitaban la información a lo que una persona podía llevar físicamente, los teléfonos celulares pueden contener una vasta cantidad de datos personales, desde correspondencia hasta fotografías y lecturas. La Corte subrayó que esta capacidad de almacenamiento convierte a los teléfonos celulares en una herramienta de gran intrusión en la privacidad, y por ello, el acceso a su contenido debe ser regulado por una orden judicial para proteger el derecho a la intimidad.

"Caso Silk Road" Tribunal de Distrito de Manhattan para el Distrito Sur de Nueva York.

Silk Road fue un mercado negro en la web profunda (deep web) operado a través del sistema Tor, que permitía a los usuarios comerciar de manera anónima. La plataforma facilitaba la venta de drogas, información robada como números de tarjetas de crédito y licencias falsas, y contenido audiovisual pirata.

Ross Ulbricht, conocido como "Dread Pirate Roberts", fue el creador y operador principal del sitio. Fue arrestado en 2013 y, en 2015, fue condenado a cadena perpetua sin posibilidad de libertad condicional por su papel en la operación de Silk Road.

Durante el proceso, Ulbricht alegó que se violó la Cuarta Enmienda de la Constitución de los Estados Unidos, que protege contra registros y allanamientos sin orden judicial específica. Argumentó que la orden de registro ejecutada por las autoridades era demasiado amplia y no

especificaba los elementos exactos a secuestrar.

La defensa sostuvo que la orden de registro debía ser más precisa para evitar la incautación indiscriminada de datos. En el contexto del caso, los investigadores aseguraron y peritaron una gran cantidad de material personal de Ulbricht, lo que, según la defensa, no cumplía con el estándar de especificidad requerido por la Cuarta Enmienda.

La Corte de Apelaciones afirmó que, en muchos casos, es impracticable prever todos los términos o frases necesarios para una búsqueda exhaustiva de los datos en un dispositivo. Reconoció que los archivos pueden tener nombres inesperados, estar encriptados, o contener códigos que eviten que se realicen búsquedas efectivas a través de patrones o palabras clave.

La Corte sostuvo que exigir una especificidad total en las órdenes de registro podría ser inviable debido a la naturaleza de cómo se almacenan y protegen los datos digitales. En lugar de patrones de búsqueda "ex ante", la Corte permitió un enfoque más flexible y adaptativo para la búsqueda y incautación de pruebas digitales.

Irregularidades en conservación y manejo de evidencia digital

“BNP Paribas y otros s/ Lavado de Dinero”. Causa nro. 19888/2009

Juzgado de Instrucción 35, secretaria 120. Sala I de la Cámara Criminal y Correccional.

En el contexto de una investigación por defraudación contra el INSSJP en el fuero federal, se allanaron 132 oficinas del BNP Paribas con el objetivo de determinar si el imputado R tenía dinero en el exterior. Durante el allanamiento, se secuestraron diversos documentos, computadoras, agendas electrónicas, unidades zip, discos compactos y duros. Sin embargo, se cometieron múltiples irregularidades en la conservación y manejo de la evidencia digital. Los CPU secuestrados no fueron conservados ni lacrados adecuadamente, lo que permitió su alteración o pérdida de integridad.

Los soportes informáticos (discos, unidades zip, etc.) fueron manejados sin seguir las

prácticas recomendadas para la protección de la evidencia digital.

Se secuestraron datos y documentos no relacionados con el objeto de la investigación, violando la orden judicial y los principios de legalidad.

El fiscal, sin autorización judicial, accedió a datos de correos electrónicos y archivos confidenciales, violando la ley de protección de datos y el derecho a la intimidad, también solicitó datos a organismos del Estado y empresas (como Telecom) sin la debida orden judicial, lo que contradice la jurisprudencia que exige autorización judicial para tales medidas.

El perito técnico estableció criterios de búsqueda sin orden judicial y desbloqueó contraseñas sin autorización, afectando la privacidad y la integridad de los datos.

Las copias de los datos no se realizaron de acuerdo con las buenas prácticas (sin códigos hash), lo que hizo que los datos fueran ir reproducibles y la prueba vulnerable.

A pesar de las irregularidades, la resolución judicial no invalidó la prueba ni corrigió los errores. La Corte argumentó que la investigación primitiva había revelado maniobras sospechosas, validando las pruebas obtenidas a pesar de los problemas en la cadena de custodia y la gestión de la evidencia.

La Cámara de Apelaciones no revisó adecuadamente las irregularidades, y los imputados fueron procesados con base en esta prueba defectuosa.

“HSBC Bank Argentina SA y otros s/ Ley 24.769”. Causa nro. 1652/2014

Juzgado Penal Económico 11, Fiscalía Penal Económico 9, Sala B Cámara Penal Económico

El caso HSBC involucra una investigación penal en Argentina por evasión tributaria basada en información digital proporcionada por la administración fiscal francesa. Esta información provino de un ex empleado del banco HSBC en Suiza, Hervé Falciani, quien había copiado datos de clientes del banco, incluyendo a clientes en Argentina, y los compartió con las

autoridades francesas. La información obtenida por Falciani fue inicialmente el resultado de delitos como espionaje económico y violación de secretos bancarios. Falciani fue investigado y detenido en Francia, donde la información fue secuestrada. Esta información fue entregada a las autoridades fiscales de varios países, incluida Argentina, sin el resguardo adecuado de la cadena de custodia. La defensa de los imputados alegó que la evidencia digital era inválida debido a su origen ilícito. Se argumentó que el acceso y manejo de los datos violaron derechos constitucionales, incluyendo la privacidad y el secreto bancario.

Se citó la doctrina de la "regla de exclusión" y la "doctrina del fruto del árbol envenenado", señalando que la prueba obtenida ilegalmente no debería ser utilizada en el proceso.

Se cuestionó la cadena de custodia de la evidencia digital desde su secuestro en Francia hasta su recepción en Argentina. Se alegó que la información fue manipulada sin seguir las reglas forenses adecuadas, afectando su integridad.

La defensa también alegó que la información sobre los clientes del banco fue obtenida de manera indebida durante un allanamiento cuyo objeto era investigar a Falciani, no a los clientes. Esto violó la doctrina de la "plain view", que exige que el hallazgo de evidencia de otro delito durante un allanamiento sea accidental.

La jueza rechazó la nulidad de la prueba, argumentando que los delitos cometidos por Falciani no invalidaban automáticamente los documentos secuestrados. Sostuvo que la evidencia no violaba directamente los derechos fundamentales y que la cadena de custodia, aunque cuestionada, no constituía una causal de nulidad per se, sino que afectaba el valor probatorio. El recurso de apelación fue rechazado, manteniéndose la validez de la evidencia digital a pesar de las irregularidades en su obtención y manejo. La Sala B de la Cámara Nacional de Apelaciones en lo Penal Económico confirmó la decisión.

Ambos casos, BNP Paribas y HSBC, implican la utilización de evidencia digital obtenida y

manejada de manera que comprometió el derecho a la privacidad y la intimidad de las personas implicadas. La falta de respeto a la cadena de custodia y las irregularidades en el manejo de la evidencia digital reflejan una violación significativa de los derechos fundamentales. En BNP Paribas, no se respetaron las normativas básicas para la conservación de la evidencia, lo que impidió su validación. En HSBC, la información se obtuvo y manejó sin un adecuado resguardo de la cadena de custodia, afectando su integridad y validez.

A pesar de la evolución tecnológica y el tiempo transcurrido entre ambos casos (6 años), el sistema judicial no logró adaptarse adecuadamente para proteger los derechos fundamentales de privacidad e intimidad. Esto resalta la falta de una respuesta efectiva ante la complejidad y la volatilidad de la evidencia digital.

Medidas coercitivas para desbloqueo de dispositivo telefónico.

"Incidente de Reposición… en autos: 'MORA, Brisa Aylén por infracción ley 23.737 (art. 5 inc. c)'". FBB 3139/2022/1/CA1 .Fecha:27 de mayo de 2022

El juez de primera instancia ordenó a Brisa Aylén Mora que proporcionara voluntariamente la clave de desbloqueo de su teléfono celular secuestrado. En caso de negativa, se autorizó la extracción compulsiva del patrón de desbloqueo (biométrico).

La defensa de Mora se opuso a la medida, argumentando violaciones a derechos constitucionales como el derecho a la intimidad, privacidad y a no autoincriminarse. Consideró que la medida era irrazonable e innecesaria y que debía llevarse a cabo en el Juzgado Federal con presencia del magistrado.

El juez desestimó el recurso de reposición y concedió el recurso de apelación en subsidio. La defensa interpuso una apelación adicional contra el rechazo de nulidad.

La defensa argumentó que aún no se habían agotado todas las alternativas para desbloquear el celular y cuestionó la necesidad de medidas coercitivas. En particular, cuestionó la

desactualización del sistema UFED y la necesidad de actualización del software para proceder con la apertura del celular.

El Fiscal General propuso el rechazo de los recursos y la confirmación de la medida dispuesta, mientras que la defensa reafirmó sus argumentos.

La medida de extracción compulsiva del patrón de desbloqueo del teléfono se consideró necesaria y proporcional, dados los hechos del caso, como la incautación de grandes cantidades de droga y la necesidad de avanzar en la investigación.

Se concluyó que la compulsión para la obtención de datos biométricos no contraviene la garantía de no autoincriminarse, ya que no se exige al imputado realizar una manifestación de voluntad o declaración que pueda incriminarlo.

La medida se ordenó con garantías adecuadas, incluyendo registro fílmico y la presencia de testigos, para evitar cualquier trato degradante o invasivo.

Se rechazaron los recursos interpuestos y se confirmó el auto de fs. 44/50 que autorizaba la medida compulsiva para obtener el patrón de desbloqueo del teléfono celular.

Referencias

1.Aboso, G. (2019). Técnicas de investigación y vigilancia electrónicas en el proceso penal y el derecho a la privacidad en la moderna sociedad de la información. En V. Ferrazuolo (Coord.), *Era digital. Delito y prevención* (p. 61). Jusbaires.

2.Asociación por los Derechos Civiles & Privacy International. (2017, marzo).*Informe de las partes interesadas: Examen Periódico Universal 26º período de sesiones – Argentina: El derecho a la privacidad en Argentina.* Recuperado de https://adc.org.ar/wp-content/uploads/2019/06/026-el-derecho-a-la-privacidad-en-argentina-03-2017.pdf

3. Baclini, J., & Schiappa Pietra, L. (2017). *Código Procesal Penal de Santa Fe comentado, anotado y concordado* (Tomo 1).

4. Bernard, J. (2022). *Equilibrio entre el derecho a la intimidad y el poder investigativo del Estado en la era digital*.Revista Jurídica de la Universidad de Palermo, 19(2). https://www.palermo.edu/derecho/revista_juridica/pub-19-2/Revista_Juridica_Ano19-N2_02.pdf

5.Bruzzone, G. (2005). La nulla coactio sine lege como pauta de trabajo en el proceso penal. En *Estudios sobre Justicia Penal. Homenaje al Profesor Julio B. J. Maier.* Ed. Del Puerto.

6.Casey, E. (2005). *Digital evidence and computer crime: Forensic science, computers, and the internet* (3ra ed.). Academic Press.

7. Castán, F. (2016). *Guía Integral de empleo de la Informática Forense en el Proceso Penal* (2da edición, revisada).

8.Consejo de Europa. (2001). *Convenio sobre la Ciberdelincuencia.* Recuperado de https://rm.coe.int/16802fa403

9. Darahuge, M. E., & Arellano González, L. (2012). *Manual de informática forense II* (Prueba indiciaria Informático Forense). Errepar.

10. Delbono, P. M. (2018). Investigación forense sobre medios digitales. En R. A. Parada & J. D. Errecaborde (Eds.), *Cibercrimen y delitos informáticos: los nuevos tipos penales en la era de internet* (pp. 192). Erreius.

11. Di Iorio, A. H., Castellote, M. A., Constanzo, B., Curti, H., Waimann, J., Lamperti, S. B., Giaccaglia, M. F., Cistoldi, P. A., Podestá, A., Iturriaga, J. I., Greco, F., Alberdi, J. I., Ruiz De Angeli, G. M., Trigo, S., & Núñez, L. (2017). *El rastro digital del delito: Aspectos técnicos, legales y estratégicos de la informática forense*. Universidad FASTA. Recuperado de [https://www.pensamientopenal.com.ar/system/files/2018/07/doctrina46835.pdf]

12. Di Iorio, A. H., Castellote, M., Constanzo, B., Curti, H., Waimann, J., Lamperti, S., Giaccaglia, M., Cistoldi, P., Podestá, A., Iturriaga, J., Greco, F., Alberdi, J., Ruiz De Angeli, G., Trigo, S., Núñez, L.(2016). *Guía integral de empleo de la informática forense en el proceso penal* (2da ed., revisada). Universidad FASTA. http://redi.ufasta.edu.ar:8082/jspui/bitstream/123456789/1592/2/PAIF.pdf

13. Dupuy, D. (2021). *Litigación & cibercrimen: experiencias latinoamericanas.* Recuperado de https://sistemasjudiciales.org/wp-content/uploads/2021/10/4.-SJ24.-Dupuy.pdf

14. España. (2015). *Ley Orgánica 13/2015*, *de 5 de octubre, de reforma de la Ley de Enjuiciamiento Criminal.* Recuperado de https://boe.vlex.es/vid/leyorganica-13-2015-583908674

15. Fernández Rodríguez, J. (2016). *Los datos de tráfico de comunicaciones: en búsqueda de un adecuado régimen jurídico que elimine el riesgo de control permanente*. Revista Española de Derecho Constitucional, 96. Recuperado de https://recyt.fecyt.es/index.php/REDCons/article/view/54343

16. García Balcarce, L. (2022). *¿Quién revisa tu teléfono? Situación de las herramientas de*

extracción forense de dispositivos móviles en sentencias judiciales y fuerzas de seguridad. Parte 2. Asociación por los Derechos Civiles.

17. Gómez Palacios, P. N., Colazo, D. J., & Solinas, M. A. (2019). Prototipo de aplicación para extracción de información de dispositivos móviles Android para uso forense. En I. M. Gallardo (Ed.), *Actas de la 3ra Conferencia Nacional de Informática Forense* (pp. 63–70). Universidad Nacional de Córdoba. http://info-conf-2019.congresos.unc.edu.ar/wp-content/blogs.dir/29/files/sites/29/2020/03/ActasINFOCONF2019-978-950-33-1553-8.pdf

18. González-Cuellar Serrano, N. (2008). Garantías constitucionales de la persecución penal en el entorno digital. En J. L. Gómez Colomer (Coord.), *Prueba y proceso penal* (p. 151). Tirant Lo Blanch.

19. Guariglia, F. (2005). Concepto, fin y alcance de las prohibiciones de valoración probatoria en el procedimiento penal: una propuesta de fundamentación. Editores del Puerto.

20. *Guía de obtención, preservación y tratamiento de evidencia digital.* (2016). Fiscalía General de la Nación. http://www.fiscales.gob.ar/wp-content/uploads/2016/04/PGN-0756-2016-001.pdf

21. Jauchen, E. (2013). *Tratado de Derecho Procesal Penal* (Tomo I). Rubinzal-Culzoni.

22. Kiguel, A. (2021). *¿Quién revisa tu teléfono? Primeras aproximaciones a las herramientas de extracción forense de dispositivos móviles en Argentina.* Asociación por los Derechos Civiles.

23. Lega, P. (2014). Intervenciones telefónicas y control del debido proceso. El necesario límite a la creación de irrazonables excepciones. *Revista de Derecho Penal y Criminología*, La Ley, VI(2), 23.

24.Maier, J. (2016). *Derecho Procesal Penal* (Tomo I, 1ª ed.). AdHoc.

25.Mera, M. M. (s.f.). *¿Es lícito acceder a los datos contenidos en el teléfono celular del imputado mediante la utilización de sus datos biométricos?* Biblioteca Poder Judicial de Córdoba. https://biblioteca.justiciacordoba.gob.ar/cgi-bin/koha/opac-retrieve-file.pl?id=3e871e4b94073a8f75f9399424f87f8a

26. Núñez Soto, É. (2020). *Investigación forense de dispositivos móviles: Metodologías y herramientas.* Recuperado de https://www.redseguridad.com/especialidades-tic/activos-de-informacion/investigacion-forense-de-dispositivos-moviles-metodologias-y-herramientas_20201021.html

27. Pérez Barberá, G. (2009). Allanamiento remoto, agente encubierto digital, vigilancia acústica, etc.: Nuevas Tecnologías y libertad probatoria en el proceso penal. Ponencia presentada en el IV Encuentro de Profesores de Derecho Procesal Penal, Salta.

28. Pina González, J. (2023). *Evidencia digital. Test para su valoración en el proceso penal*. Recuperado de https://riej1812.com/wp-content/uploads/2023/04/PINA_-Juan-Manuel.-Evidencia-digital-y-test-para-su-valoracio_n-en-el-proceso-penal.docx

29. Polansky, J. (2023). *La investigación penal en el entorno digital* (T. 1). Hammurabi.

30. Protocolo para la identificación, recolección, preservación, procesamiento y presentación de evidencia digital. (2023). Fiscalía General de la Nación. http://www.fiscales.gob.ar/wp-content/uploads/2023/04/MINSEG-MPFN-Protocolo-evidencia-digital-2.pdf

31. Roatta, S., Casco, M., & Fogliato, M. (2015). El tratamiento de la evidencia digital y las normas ISO/IEC 27037:2012. Recuperado de https://sedici.unlp.edu.ar/handle/10915/50586

32. Salt, M. (2017). *Nuevos desafíos de la evidencia digital: Acceso transfronterizo y*

técnicas de acceso remoto a datos informáticos. Ad-Hoc.

33. Sain, G. (2012).*Delitos y nuevas tecnologías: Fraude, narcotráfico y lavado de dinero por internet*. Del Puerto.

34. Semprini, G. (2017). *Simposio Argentino de Informática y Derecho (SID) - JAIIO 46*. Córdoba. Recuperado de https://sedici.unlp.edu.ar/bitstream/handle/10915/65212/Documento_completo.pdf-PDFA.pdf?sequence=1

35.Sergi, N. (2018). Análisis jurídico de la situación de la evidencia digital en el proceso penal en Argentina. Informe realizado para la Asociación por los Derechos Civiles.

36.Simian, M. (2023). *Investigación del crimen organizado mediante acceso remoto* (1ra ed.). Buenos Aires: Hammurabi.

37. Torres, S. (2023). Espejo Chubut: el software creado en Chubut que permite validar a los chat y audios de Whatsapp en juicios. Recuperado de https://www.mpfchubut.gov.ar/centro-de-noticias/puerto-madryn/espejo-chubut-el-software-creado-en-chubut-que-permite-validar-a-los-chat-y-audios-de-whatsapp-en-juicios

38. *Tribunal Constitucional Federal Alemán*. (1983). Sentencia de la Primera Sala – 1 BvR 209, 269, 362, 420, 440, 484/83 – del 15 de diciembre de 1983. Recuperado de https://www.kas.de/c/document_library/get_file?uuid=0a66a4a6-1683-a992-ac69-28a29908d6aa&groupId=252038

39. *Tribunal Supremo de Justicia Español*. (2016). Sentencia N° 204/16. Recuperado de https://supremo.vlex.es/vid/631962729#section_28

40. *Resolución N° 68/167* (2013). Emitida por la A.G. de Naciones Unidas. Recuperado de https://digitallibrary.un.org/record/764407?ln=es

41. *Resolución 234/2016* (2016). Protocolo general en la investigación y proceso de

recolección de pruebas en ciberdelitos. Publicada en el Boletín Nacional del 14-Jun-2016. Recuperado de https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-234-2016-262787/texto

Bibliografía

Argentina. (2018). *Código Procesal Penal Federal (Ley N.º 27.063)*. Recuperado de https://servicios.infoleg.gob.ar/infolegInternet/anexos/315000-319999/319681/norma.htm

Neuquén. (2023). *Código Procesal Penal de Neuquén.* Recuperado de https://www.jusneuquen.gov.ar/codigos-provinciales/

Salta, Provincia de. (2022). *Ley N.º 8386 de procedimiento para la obtención, conservación y presentación de evidencia digital en el proceso penal.* Recuperado de https://boletinoficialsalta.gob.ar/instrumento.php?cXdlcnR5dGFibGE9THw4Mzg2cXdlcnR5

Congreso de la Nación Argentina. (1994). Constitución de la Nación Argentina. https://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/804/norma.htm