Universitat de Girona
Centre d'Estudis de Postgrau

Máster en Razonamiento Probatorio

Trabajo final de máster

Máster en Razonamiento Probatorio

Titulo:

Elementos probatorios en entornos digitales
La tensión entre la escasez y la sobreabundancia de información en la etapa de investigación.

Alumno/a: Matías Meza

Tutor/a: Dra. Carmen Vázquez

Convocatoria: enero-abril 2024

Elementos probatorios en entornos digitales

La tensión entre la escasez y la sobreabundancia de información en la etapa de investigación.

Matías José Meza[1]
abmatiasmeza@gmail.com

Resumen: El artículo tiene como objetivo iniciar un camino de reflexión sobre los elementos probatorios en entornos digitales durante la etapa de investigación. Para ello, en primer lugar, se realiza una aproximación al razonamiento probatorio en esta fase; seguidamente, se describe el proceso de investigación en entornos digitales. Posteriormente, se abordan dos extremos en tensión: por un lado, la falta de información típica de esta etapa y, por el otro, el efecto de desborde que se produce ante la gran cantidad de información relevante e irrelevante que se puede encontrar en las fuentes que la contienen. Con todo ello, se argumenta sobre la necesidad de un mayor razonamiento probatorio en la etapa de investigación, proponiendo algunas sugerencias para un abordaje adecuado del entorno digital, desde una concepción racionalista de la prueba y acorde a los requisitos de un debido proceso.

Palabras clave: Entornos digitales; etapa de investigación; evidencia digital; escasez informativa; sobreabundancia de información; razonamiento probatorio.

Abstract: The article aims to begin a path of reflection on evidentiary elements in digital environments during the research stage. To do this, firstly, in this phase an approach to evidentiary reasoning is made; Next, the research process in digital environments is described. Subsequently, two extremes in tension are addressed: on the one hand, the lack of information typical of this stage and, on the other, the overflow effect that is produced by the large amount of relevant and irrelevant information that can be found in the sources that contain it. With all this, the need for greater evidentiary reasoning in the investigation stage is argued, proposing some suggestions for an adequate approach to the digital environment, from a rationalist conception of evidence and in accordance with the demands of due process.

Keywords: Digital environments; research stage; digital evidence; information scarcity; overabundance of information; evidentiary reasoning.

[1] Maestro en razonamiento probatorio por la Universidad de Girona (España). Abogado por la Universidad Siglo 21 (Argentina). Licenciado en Criminalística por la Universidad Nacional del Nordeste (Argentina). Con estudios de especialidad en Derecho Procesal por la Universidad Nacional de Córdoba (Argentina). Docente Universitario en carreras de pregrado, grado y posgrado. Integrante del Poder Judicial de la Provincia de Córdoba (Argentina)

1- Una aproximación al razonamiento probatorio en la etapa de investigación con entornos digitales.

Los presuntos hechos delictivos que investigamos cada vez se encuentran más envueltos en entornos digitales. La Academia Nacional de Ciencias de los EE.UU. advertía esta situación como una posible problemática cuando, hace aproximadamente una década, se refería a ellos como una disciplina de la ciencia forense emergente: «los medios digitales se han convertido en testigos de las actividades cotidianas, como resultado, casi todos los delitos podrían tener evidencia digital asociada». [2] Hoy en día, algunos estudios revelan que alrededor del 90% de los casos criminales que se investigan contienen algún elemento digital asociado.[3]

Esto ha producido un cambio de paradigma, ya que la tradición investigativa se basaba, en gran parte, en abordar solamente los elementos probatorios materiales (indicios biológicos, físicos, químicos, cadáveres, etc.).[4] Posteriormente, con el aumento de la utilización de dispositivos que contienen información digital, se hizo necesario incorporar una visión dual, que incluye tanto lo material como lo digital.[5] Por este motivo, resulta importante indagar sobre el impacto de la dinámica descripta en el razonamiento probatorio.

Si consideramos los tres momentos claves en la actividad probatoria delineados por Ferrer Beltrán (2021, p. 22): «1) el momento de la conformación del conjunto de elementos de juicio o del acervo probatorio; 2) el momento de la valoración de la prueba y 3) el momento de la decisión sobre la prueba», es evidente que la información proveniente de entornos digitales enfrenta distintos desafíos en cada una de ellas, pero vale la pena notar que lo que suceda al inicio impactará fuertemente en todas las demás etapas del proceso.

---

[2] Cfr. NRC (2009). *Strengthening forensic Science in the United Stated: A Path Forward*. National Academies Press. https://nap.nationalacademies.org/catalog/12589

[3] En el reciente trabajo de Wilson-Kovacs, et al (2023) se aborda la creciente importancia de la evidencia digital en la práctica legal, destacando que, en la actualidad, elementos digitales están presentes en un 90% de los casos judiciales en Inglaterra y Gales. En esa línea de ideas, la empresa Cellebrite, especializada en el análisis forense de dispositivos móviles, señala que la evidencia digital se encuentra presente entre un 80 % y un 90 % de todos los casos delictivos que se investigan, abarcando delitos como «pornografía infantil, intrusión en redes, homicidios, crímenes de cuello blanco, pandillas, terrorismo y narcotráfico.». Para obtener más información, se puede consultar el siguiente enlace: https://cellebrite.com/es/principales-desafios-y-cambios-en-el-uso-de-evidencia-forense-digital/

[4] Desde una concepción clásica, la investigación del denominado lugar del hecho es entendido como un proceso que incluye el estudio del espacio físico susceptible de investigación científica criminal. Desde esta perspectiva, la exclusividad está dada por la investigación de los elementos materiales que, en el caso dado, conformaba el conjunto de elementos aportados a la causa.

[5] Investigar en entornos digitales requiere evaluar la autenticidad, integridad y cadena de custodia de la evidencia, así como la confiabilidad de las fuentes digitales. Además, enfrenta desafíos como la evolución rápida de herramientas digitales, la posible manipulación de evidencia y la necesidad de comprender las complejidades técnicas asociadas con la obtención y presentación de pruebas digitales.

La fase de investigación es la que se ve afectada de manera más inmediata. La complejidad inherente a la búsqueda, recopilación y organización de potenciales elementos de prueba provenientes de entornos digitales, se manifiesta de manera pronunciada en este punto, introduciendo una serie de desafíos particulares al comienzo mismo del proceso probatorio.

Una de las características típicas de la etapa de investigación, de interés a nivel del razonamiento probatorio,[6] se encuentra en relación con la marginalidad que tiene la racionalidad en la realización de las primeras actuaciones, que también se ve reflejada en forma particular cuando lo que se investiga está vinculado a entornos digitales. En general, los procedimientos realizados en dicha etapa están caracterizados por actividades mayoritariamente intuitivas,[7] y en el mejor de los casos mediante razonamiento abductivo.[8] En ese sentido, en el tratamiento de la denominada evidencia digital, los protocolos o guías de buenas prácticas[9] intentan disminuir la subjetividad característica de los primeros momentos de la investigación.[10]

Al igual que las investigaciones donde se procura obtener información sobre potenciales elementos de prueba materiales o tangibles, en las investigaciones en entornos digitales también existen lineamientos generales para abordar los sucesos delictivos o presuntamente delictuosos.[11] En general, estos procesos están orientados en pasos que incluyen: el relevamiento, la adquisición, preparación, extracción y análisis para su posterior presentación.

---

[6] Lo consideramos de interés debido a su escasa discusión. A ello se refiere Abimbola (2002, p. 337) cuando indica: «las cuestiones sobre la etapa de descubrimiento tienen un papel escaso o nulo en el razonamiento probatorio en derecho». En ese mismo sentido, Ferrer Beltrán (2020, p. 15) también advierte que, «las reflexiones sobre la fase de investigación penal reciben, lamentablemente, poca atención en la literatura sobre epistemología jurídica.».

[7] Binder (1999, pp. 236-237) se refiere a esta etapa como una actividad creativa, que implica superar la incertidumbre mediante la exploración de diversos recursos que puedan proporcionar la información necesaria para disipar dicha incertidumbre.

[8] Para Tuzet (2021, p.125) en la fase de formulación de la hipótesis (fase de investigación o preparatoria) las inferencias son «sustancialmente abductivas». Por su parte para Anderson, Shum y Twining (2015, p.89) «es el proceso creativo del razonamiento. Más que razonar desde una hipótesis hacía una conclusión basada en pruebas, involucra un razonamiento que va desde la prueba hacía una hipótesis que la pueda explicar». Así mismo, Moscatelli (2022. p. 127) nos comenta que se lo utiliza como un instrumento de investigación que permita generar hipótesis para explicar un determinado fenómeno a partir de datos incompletos y disponibles.

[9] Es importante tener en cuenta que existe poca regulación en materia de evidencia digital.

[10] Si bien no es objeto del presente trabajo, es importante considerar que no siempre todos los protocolos o guías de buenas prácticas son eficientes; muchas de ellas camuflan procedimientos intuitivos o los formalizan. Un ejemplo de ello lo encontramos en documentos de instrucción policial de la policía de Brasil donde textualmente se afirma: «El policía civil, en el curso de una investigación policial, podrá apoyarse, como aporte, en la intuición, la presunción y las hipótesis, hasta completar su trabajo, que culminará con llegar a una conclusión determinada por la convicción o la certeza.». En el mismo documento posteriormente se establece una definición de intuición. Se puede acceder al documento en el siguiente enlace: https://www.acadepol.ms.gov.br/artigos/importancia-da-pratica-didatica-na-investigacao-policial/

[11] El término potencial elemento de prueba digital es propuesto por el Protocolo de Actuación para la Investigación Científica en el lugar del hecho (2021, p.5) del Ministerio de Seguridad en Argentina para referirse a: «cualquier dato (registro y/o archivo) que pueden ser generados, transmitidos o almacenados por los equipos de tecnología informática y que está constituida por campos magnéticos y pulsos electrónicos, los cuales pueden ser recolectados y analizados con herramientas y técnicas especiales. Resulta independiente a su valoración jurídica de indicio o evidencia.»

Los dos primeros pasos, el relevamiento y la adquisición, [12] constituyen puntos críticos y, por ello, ahí nos centraremos en la primer parte del presente trabajo. En relación con estos puntos críticos, la problemática inicial radica en la escasa información característica de la etapa de investigación. Desde una perspectiva crítica, Collie (2018. p.1) manifiesta que: saber cómo iniciar y recuperar evidencia digital puede ser desafiante, incluso para expertos. Sin embargo, la interpretación adecuada de los datos recopilados es crucial para la justicia. Frecuentemente, aquí es donde el sistema falla.

En ese sentido podemos identificar al menos 3 aspectos: a) lo que se busca en un entorno digital no está bien definido; b) los elementos provenientes de entornos digitales se encuentran en multiplicidad de fuentes; y, c) hay menos control intersubjetivo ya que es la etapa donde predomina la intuición.[13]

Por otro lado, en las fases de laboratorio se presenta una segunda problemática en relación al abrumador volumen de información que debe ser recopilada, analizada y presentada. Para ilustrar este desafío, consideremos una sencilla analogía: la diferencia entre una colilla de cigarrillo y un smartwatch, ambos hallados en el lugar del hecho. Por un lado, la colilla de cigarrillo, al contener información genética, nos brinda al menos dos elementos de referencia: en primer lugar, la identificación de la persona que estuvo en contacto con la colilla a través de la obtención de un perfil de ADN (a partir de las células descamadas de la boca) y la presencia física de esa persona en el lugar del hecho. En contraste, un smartwatch nos suministra información a un nivel considerable, con al menos 1 GB de datos, abarcando una multiplicidad de aspectos relacionados con la actividad realizada por la persona (su ubicación, ritmo cardíaco, horas de descanso, y otros parámetros relevantes para conocer el contexto del hecho investigado).

En ese marco, el objetivo general de este trabajo es reflexionar sobre los elementos probatorios en entornos digitales durante la etapa de investigación. Y, específicamente, describir dos extremos: Por un lado, la falta de información típica de esta etapa y, por el otro, el efecto desborde que se produce ante la gran cantidad de información relevante e irrelevante que se

[12] En la fase de relevamiento el objetivo principal es poder identificar la información digital de un universo variado de potenciales elementos de prueba contenido en dispositivos (físicos, analógicos, convencionales, no convencionales, etc…). Por su parte, en la fase de recolección el objetivo es seleccionar dentro de un espectro de elementos, los que se consideren relevantes para la investigación.

[13] El control intersubjetivo implica la capacidad de validar o verificar la comprensión o interpretación de un fenómeno entre diferentes individuos. En ese sentido, la verificación de la veracidad se basa en criterios reconocidos por los sujetos del sistema, que permiten evaluar la validez (probabilidad, plausibilidad) de los resultados obtenidos. (Haba, 1990, p. 178) En procesos intuitivos, donde la toma de decisiones se basa en percepciones internas y subjetivas, este control puede ser limitado debido a las diferencias individuales en experiencias, perspectivas y conocimientos. Partiendo que la concepción racionalista implica por definición razonamientos, podemos anclar la idea de razonamiento como vehículo de control intersubjetivo.

puede encontrar en las fuentes que la contienen. Con todo ello, se pretende argumentar sobre la necesidad de un mayor razonamiento probatorio en la etapa de investigación, proponiendo algunas sugerencias para un abordaje adecuado del entorno digital, desde una concepción racionalista de la prueba y acorde a los requisitos de un debido proceso.[14]

2. Desandando el proceso de investigación en entornos digitales.

Ante la ocurrencia de un acontecimiento delictivo o presuntamente delictuoso, se pone en funcionamiento un mecanismo que comienza con la toma de conocimiento del hecho (ya sea de oficio, por denuncia o por actividad policial).[15] Seguidamente, el órgano encargado de la investigación penal, continuará con las actuaciones. Por ejemplo, en el caso que sea el Fiscal de instrucción, estará a cargo de promover o desestimar la acción penal, tomando las primeras medidas de investigación. En relación con ello, Moscatelli (2023, p. 131) nos explica:

> Como en todo proceso de investigación, se debe plantear una hipótesis, aunque sea provisional, a través de la cual la Fiscalía forme su *opinio delicti* y, sobre esa base, determine si existen elementos para iniciar o desestimar un caso, analizando i) la posible autoría; ii) la materialidad del delito; iii) las circunstancias y razones probables que llevaron a la comisión del ilícito, y en general, iv) la existencia del elemento subjetivo (dolo).

Una de las medidas más importantes llevada a cabo en esta instancia, consiste en instruir a las personas interventoras del lugar del hecho, ya sean de fuerzas de seguridad o cuerpos forenses, para que realicen las intervenciones criminalísticas o periciales correspondientes, con el fin de obtener los posibles elementos de prueba, que tendrá como objetivo acreditar el hecho, sus protagonistas y sus circunstancias.[16]

---

[14] Siguiendo esa línea de ideas, y como fundamento de la importancia de reflexionar sobre estas cuestiones, Haack (2015, p. 69) manifiesta: «es mejor, en la medida de lo posible, prevenir un problema que arreglar las cosas más tarde». Por su parte Gascón Abellán (2016, p. 365), en acuerdo con Haack, agrega «más efectivo concentrarse en lo que sucede "antes" con el fin de evitar que se produzcan cosas indebidas (fraudes en los laboratorios, malas prácticas en la investigación y en la promoción de una técnica, expertos incompetentes, sesgos evitables, etc.) y de que, si se producen, queden rápidamente al descubierto». Por último, refiriéndose a la etapa de investigación, y específicamente a la labor policial, Merkel (2022, p. 14) comenta que lamentablemente se ha puesto poco foco en la función policial, como si se ha hecho en otros órganos del Estado. De allí la importancia de abordar esta problemática.

[15] A ello se refiere Borrás Andrés (2023, p. 2019), cuando nos comenta que la implementación de la labor policial en etapas previas y simultáneas al proceso penal es una práctica habitual en el ámbito del derecho comparado. Aunque en la mayoría de los casos se lleva a cabo bajo la supervisión del Ministerio Público, suele haber una primera intervención policial orientada a la prevención, relacionada con la seguridad ciudadana y la asistencia inmediata en situaciones de amenaza.

[16] Es importante aclarar que, en la generalidad de los casos, el primer momento de intervención es llevado a cabo por personal policial (con mayor o menor formación en el campo forense). En menor medida, la intervención es llevada a cabo por equipos forenses con formación como tal. En Argentina, por ejemplo, la situación es bastante diversa de acuerdo con la implementación o no de la Policía Judicial.

En ese sentido, la investigación del denominado lugar del hecho, desde su perspectiva clásica, es decir, aplicada a elementos materiales, se entiende como un proceso que implica la intervención del espacio físico donde ocurrió o se sospecha que ocurrió un hecho delictivo. Para abordar este proceso en la investigación forense se aplica una metodología específica que incluye la preservación, observación, registro, levantamiento y traslado al laboratorio de los elementos materiales presentes en dicho lugar.[17]

Desde hace varias décadas atrás, el desarrollo de la tecnología produjo un impacto significativo en la vida de las personas y en sus actividades cotidianas. Todas las actividades, ya sean comunicativas, de transporte, tareas domésticas, laborales, formativas y hasta de descanso, pueden contener asociada información digital. Esto también tuvo su efecto en los procesos de investigación de hechos criminales. En esa línea se refiere Fernando (2021, p. 138) cuando manifiesta: «Con ello se dejan huellas digitales que quedan alojadas en registros disímiles que pueden ser evidencia digital en un proceso judicial.»

Hoy convivimos con un sistema dual donde lo analógico y lo digital requiere ser investigado por igual y donde no necesariamente hay una diferenciación, sino más bien un entrelazamiento constante. En consecuencia, es importante la investigación en entornos digitales, ya que la información proporcionada en estos contextos puede ayudar a rastrear, explicar y comprender el comportamiento de quienes participan en actividades delictivas. (Wilson-Kovacs, et al. 2023, p. 1). Actualmente, la información digital se emplea en investigaciones penales no solo para abordar ciberdelitos como el robo de identidad, el phishing y el ciberacoso, sino también para indagar en delitos que pueden ocurrir incidentalmente con el uso de dispositivos o que se ven facilitados por un entorno digital.

La evidencia digital ha comenzado a ser útil en los procesos investigativos y, con ello, se ha vuelto indispensable en los procedimientos judiciales.[18] La primera cuestión a establecer, entonces, es: ¿a qué nos referimos con "evidencia digital"? Aunque existen innumerables conceptos, podemos obtener una aproximación recurriendo a la norma ISO/IEC 27037:2012,[19]

[17] Guzmán (2011, p.9) lo denomina proceso de investigación en el escenario del delito. A través de estos pasos se busca garantizar la obtención de elementos probatorios en los primeros momentos de la investigación. Se inicia con la participación de la primera persona que tiene contacto con el mismo (preservación), seguido por el relevamiento del lugar (observación y registro). Posteriormente, se lleva a cabo el secuestro u obtención de los elementos para su traslado a los laboratorios correspondientes (levantamiento y traslado).

[18] En la actualidad, para la investigación de hechos criminales, la tendencia es que la utilización de la evidencia digital sea una regla y no la excepción. «La demanda de pericias informáticas (actuación forense) por parte de la justicia es cada vez mayor, y crece permanentemente, dado que los rastros digitales se multiplican y son cada vez más importantes y determinantes en la investigación.» (Di lorio et al. 2017, p. 17)

[19] Se selecciona la siguiente definición por considerarla lo suficientemente amplia, teniendo en cuenta la finalidad del presente trabajo.

que la define como: «Información o datos almacenados o transmitidos de forma binaria que pueden ser considerados como evidencia o prueba. »[20]

La evidencia digital presenta características particulares que lo diferencian de la evidencia analógica, entre ellas podemos nombrar la intangibilidad y la volatilidad.[21] Por otro lado, también presenta particulares discusiones en el ámbito probatorio. Una de las más predominantes se relaciona con la atribución de autoría, es decir, la vinculación entre la evidencia digital y el autor del hecho. En este sentido, la importancia de considerar que, si bien las pruebas digitales ofrecen datos valiosos, por sí solas no son suficientes para establecer la identidad de la persona que está llevando a cabo una acción, a menos que estén respaldadas por otros elementos que confirmen quién está utilizando el dispositivo en ese momento específico. (Merkel, 2022, p. 251)

Otra de las cuestiones se encuentra en relación con el procedimiento adecuado para el tratamiento de la evidencia digital, uno que permita que la información sea introducida adecuadamente a un proceso judicial.[22] En ese sentido, en principio, nos encontramos con procedimientos que surgieron al extrapolar el proceso de investigación tradicional (exclusivamente de la evidencia física) a la investigación de la evidencia digital. Esto, como dijimos anteriormente, tiene relación con la poca regulación que existe aún en la temática, a la que agregamos la falta de cultura digital en el sistema de justicia.[23]

Debido a la falta de regulación, los protocolos de tratamiento de la evidencia digital empezaron a ganar protagonismo. Con respecto a ello, Merkel (2022, p. 2014) advierte que, si bien dichos protocolos son de utilidad, dado que generalmente son elaborados por profesionales o ámbitos

[20] Para Wilson-Kovacs et al. (2023. p. 236). Esto abarca información recopilada de diversos dispositivos digitales y plataformas en línea, como teléfonos, computadoras, tabletas, routers, wifi, cámaras, consolas de juegos, dispositivos de Internet de las cosas, vehículos conectados y sensores inalámbricos, entre otros. En este sentido, resulta imprescindible reconocer la diferencia entre el componente físico (hardware) y los datos almacenados en él, es decir, la evidencia digital (Semprini, 2017, p. 91).

[21] La intangibilidad de la evidencia digital se refiere al hecho de que la misma no tiene una existencia física tangible como la tienen los objetos físicos. A diferencia de la evidencia física, como armas, huellas dactilares en papel, o documentos en papel, la evidencia digital consiste en datos almacenados en dispositivos electrónicos o sistemas informáticos. Por su parte, la volatilidad se refiere a la naturaleza transitoria y efímera de la evidencia digital. A diferencia de la evidencia física, que puede permanecer relativamente intacta durante largos períodos de tiempo, la evidencia digital puede ser fácilmente modificada, eliminada o sobrescrita.

[22] En este sentido, nos referimos a las discusiones sobre la admisibilidad de las pruebas digitales.

[23] Así lo señala Merkel (2022, p. 76). Cuando dice: «Los datos informáticos son aterradores porque son en gran parte desconocidos para los que participan en el proceso. El análisis de los datos es, por tanto, una actividad completamente ajena a las categorías mentales de los abogados y jueces, que siguen razonando según cánones de la experiencia que no son plenamente aplicables a esta nueva realidad.». Por otro lado, concebimos esta problemática en el sistema de justicia, considerando a todos los operadores, incluyendo intervenciones policiales, forenses, fiscalía, defensa y jueces. En ese sentido, Duce (2013, p.2) se refiere a errores del sistema y no errores judiciales, ya que considera: «que no es un problema de los jueces exclusivamente, sino del sistema en su conjunto.».

destacados de la disciplina, lo cierto es que presentan dos problemas: la falta de uniformidad y la ausencia de carácter vinculante.[24]

Entre las instituciones más destacadas que comenzaron a involucrarse en los procesos de tratamiento de la evidencia digital, y que emitieron los primeros documentos para el procesamiento de la misma, se encuentran el Federal Bureau of Investigation (FBI) y el National Institute of Standards and Technology (NIST). En el año 2006, el último de ellos, emitió un documento integral de recomendaciones que no se limitaba exclusivamente a su aplicación en el ámbito penal[25]. Ya para el año 2012, la Organización Internacional de Normalización (ISO) en colaboración con la Comisión Electrotécnica Internacional (IEC), publicaron la norma ISO/IEC 27037, que proporciona pautas y orientaciones para la gestión de la evidencia digital. Esta norma ha tenido un impacto tan significativo, que se la continúa aplicando en la actualidad.

Teniendo en cuenta estos antecedentes, la mayoría de las normas técnicas indican que el proceso de investigación para la obtención de elementos probatorios provenientes de entornos digitales debería comprender, un camino planificado compuesto por un conjunto de pasos, donde la preservación es el eslabón previo a toda actuación. Posteriormente, la investigación incluye dos etapas consecutivas, la primera en el lugar del hecho, incluyendo el relevamiento[26] y la recolección, la segunda compuesta por los procedimientos de laboratorio donde se realiza la adquisición, preparación, la extracción y análisis para su posterior presentación mediante informes a los órganos judiciales correspondientes. Para comprender el proceso de investigación en entornos digitales, es necesario conocer su dinámica. Por ello, en las siguientes líneas se desarrollarán cada una de las etapas, teniendo en cuenta la finalidad que persigue el presente estudio.

---

[24] En relación con el primer aspecto, existen una diversidad de protocolos o guías de buenas prácticas con diferentes estándares. Entre ellos, a nivel internacional, podemos mencionar la norma ISO/IEC 27037:2012. Si bien fue un buen intento de sistematización, presenta algunas críticas. En primer lugar, es muy general, es decir, no es específica para procedimientos particulares. Por otro lado, no abarca la diversidad de dispositivos o fuentes de evidencia digital en su totalidad. Y, por último, pero no menos importante, dichas normas no son de acceso público, afectando directamente el derecho de defensa. Con respecto a la cuestión relacionada con el carácter no vinculante, en pocas ocasiones, el acatamiento de las normas técnicas relacionadas con el manejo de evidencia digital (por ejemplo, la norma ISO/IEC) se ve como un requisito obligatorio para que dicha evidencia sea aceptada como prueba en el proceso. Por esta razón, estas normas se consideran más bien como documentos orientativos de derecho, conocidos como «soft law»., aplicados por especialistas pero que carecen de un valor jurídico directo. En ese sentido Merkel (2022, p.215) entiende que esto último, constituye uno de los puntos más vulnerables en todo el proceso de análisis de la escena del crimen.

[25] Se puede acceder al documento en el siguiente link: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-86.pdf

[26] Es importante tener en cuenta que en este estudio se empleó el término «relevamiento» en lugar de "identificación", como sugiere la norma ISO/IEC 27037:2012. Esto se debe a que el término «identificación» se utiliza comúnmente en el ámbito forense para referirse a la acción o resultado de comparar o cotejar personas y/o cosas. Por lo tanto, se considera más apropiado referirse a esta primera actividad en la investigación en entornos digitales como «relevamiento». Sin embargo, ambos términos, a nivel práctico, se refieren a lo mismo.

Como primer aspecto, las actividades de relevamiento y recolección son las primeras en el proceso de investigación. Estas tareas son llevadas a cabo principalmente por las primeras personas interventoras del lugar del hecho, es decir, generalmente personal policial o de fuerzas de seguridad.[27] Mientras tanto, las etapas de adquisición, preparación y extracción se llevan a cabo normalmente en el laboratorio por especialistas en evidencia digital, como ingenieros y técnicos. (Di lorio, et al. 2017, p. 279. Este detalle no debe pasarse por alto, especialmente al considerar que la primera etapa, es la más vulnerable debido a la escasez de información típica de los primeros momentos de la investigación.

La fase de relevamiento es el paso crucial que implica la recopilación y documentación inicial de la información relacionada con los dispositivos y sistemas que serán objeto de investigación; implica identificar posibles elementos de interés (Di lorio, et. al. 2017, p. 284). En cuanto a esta fase, podemos indicar que la actividad principal es la búsqueda, que puede llevarse a cabo en equipos físicos o fuentes no físicas que contengan información digital.

Por su parte, en cuanto a la fase de recolección, implica tomar las medidas requeridas para obtener acceso a los equipos físicos y las fuentes de información que serán tratados en pasos subsiguientes del proceso (Di lorio et. al. 2017, p. 285). La norma ISO/IEC 27037:2012 describe como objetivo de esta fase: «la recolección de los dispositivos y la documentación (incautación y secuestro de los mismos) que puedan contener la evidencia que se desea recopilar o bien la adquisición y copia de la información existente en los dispositivos.» En los apartados 3 y 4 examinaremos cómo estas etapas se relacionan con el problema de la escasez de información y la sobreabundancia de datos en la investigación criminal en entornos digitales.

Como segundo aspecto, los elementos al laboratorio pueden ingresar por dos vías. Una es mediante el relevamiento y obtención en el lugar del hecho, mediante los procedimientos indicados. Y la otra posibilidad es que ingrese directamente sin pasar por los procedimientos anteriormente descritos[28]. La fase de laboratorio implica las actividades de adquisición, preparación, extracción y análisis de la información contenida en entornos digitales. En esta

[27] Con respecto a ello, el Protocolo de evidencia digital de la Argentina (2023, p. 7) refiriéndose a las funciones, indica que es responsable de localizar y recoger dispositivos electrónicos que puedan contener evidencia digital relevante para la investigación, garantizando su validez y fiabilidad durante el proceso.

[28] Es crucial destacar que en ocasiones los dispositivos que pueden contener evidencia digital son enviados directamente a laboratorios por la primera persona involucrada en el caso, como personal policial o de seguridad, en situaciones donde fueron obtenidos por diversas razones. Esto suele ocurrir cuando los dispositivos son hallados en un lugar diferente al de los hechos, pero que potencialmente están relacionados con la investigación. A veces, estos elementos son entregados voluntariamente por testigos u otras personas.

fase se debería realizar un exhaustivo análisis de los elementos recopilados durante la fase de recolección en el lugar de los hechos.

Este proceso implica el examen de dispositivos electrónicos, sistemas informáticos y cualquier otro medio que pueda contener información relevante para ser presentada posteriormente. Durante esta etapa, los expertos forenses emplean técnicas especializadas para extraer, preservar y examinar datos digitales. Se busca identificar patrones, conexiones o cualquier indicio que pueda proporcionar información valiosa para la investigación. Además, se aplican herramientas y metodologías forenses para garantizar la integridad de la evidencia atendiendo a los lineamientos de la cadena de custodia.

Actualmente, las fuerzas de seguridad y dependencias forenses utilizan diversos software de uso forense para el tratamiento de la evidencia digital.[29] Uno de los más destacados es el de la empresa israelí Cellebrite y, específicamente, el dispositivo universal de extracción forense denominado Cellebrite UFED (por sus siglas en inglés).[30] Este programa permite el tratamiento de los dispositivos más frecuentes en los hechos que se investigan: los dispositivos móviles.[31] Entre sus funciones se encuentra la de filtrar y extraer información «relevante» para la causa de un universo casi incontable de datos.[32] Si bien este y otros programas son considerados de gran utilidad en la comunidad forense, actualmente están recibiendo algunas críticas muy interesantes a nivel probatorio con respecto a la confianza depositada en las empresas proveedoras de los programas y el rol que ocupa en la actualidad el experto en evidencia digital.[33]

En los siguientes apartados, analizaremos las situaciones específicas que pueden surgir en relación con las intervenciones en el lugar del hecho y en laboratorio. Para ello, nos enfocaremos en dos problemáticas bien definidas. Por un lado, la falta de información típica

[29] Con el pasar del tiempo, y el notable incremento en la magnitud y complejidad de la información, se tornó esencial la creación de herramientas especializadas para respaldar este proceso, entre las cuales se encuentran varias soluciones comerciales. (Stelly; Rousevv, 2018, p. 1).

[30] Se puede acceder a la información básica en la página oficial: https://cellebrite.com/es/pagina-principal/

[31] Como dispositivos móviles podemos considerar una amplia gama de elementos como ser: celulares, drones, tarjetas SIM, Smartwatch, dispositivos de posicionamiento global (GPS), entre otros.

[32] Es relevante resaltar la cuestión de los puntos de pericia o de análisis de la evidencia digital después de haber secuestrado el equipo. Comúnmente se utilizan programas que, mediante palabras clave o patrones de búsqueda, buscan datos relevantes para el delito bajo investigación. Es decir, en lugar de examinar individualmente cada archivo del equipo, se recurre a estos programas de búsqueda automatizada. (Suarez, 2021, p. 5)

[33] Los autores Stelly y Rossev (2018, p. 1) nos comentan la siguiente problemática: «(...) esto requiere una confianza casi ciega en los sistemas implementados y no ofrece medios listos para realizar la verificación de los resultados por parte de terceros; esto se vuelve cada vez más inaceptable a medida que el volumen y la importancia de los datos examinados continúan creciendo rápidamente.» Por su parte, Contissa y Lasagni (2020, p. 293) se refieren a ello como Data Fundamentalism. Es decir, la tendencia a asumir que el análisis de dispositivos digitales es confiable, independientemente de las actividades operativas realizadas. Esto último, podría tener su analogía con el efecto «CSI» específico para las ciencias forenses.

durante los primeros momentos de la investigación y, por otro lado, el desborde de información cuando se investiga en entornos digitales.

3- Escasez informativa en la fase de investigación.

Con frecuencia, en los primeros momentos de la investigación la información es escasa.[34] Esto se debe a varios factores, como la complejidad del hecho, su tipología, que el lugar del hecho es abordado tardíamente,[35] la novedad incipiente de la ocurrencia del hecho delictivo y, por supuesto, que el acto de investigar implica generar nuevos conocimientos sobre el suceso.[36] En ese sentido, la persona responsable de la investigación criminal, al analizar los indicios recolectados en el lugar de un crimen o frente al informe de un posible delito, se enfrenta a la necesidad de elaborar una hipótesis que explique un conjunto específico de hechos pasados. Esto produce que se busque más información que confirme si la hipótesis es precisa o si, por el contrario, los datos disponibles son insuficientes para respaldarla, lo que puede implicar un cambio en la dirección de la investigación[37] (Moscatelli, 2023, p. 127).

Frente a esta situación, los escasos datos o información disponible en los primeros momentos son transmitidos a las primeras personas que intervienen en el lugar del hecho para llevar a cabo las acciones necesarias en busca de elementos que puedan ser útiles en la investigación. Esta característica de la escasez de información nos enfrenta a un panorama inicial impreciso, lleno de incertidumbre, que sin duda tendrá un impacto en esta fase y en las que siguen. Si bien podríamos plantear varias cuestiones, nos centraremos en tres aspectos específicos: la

[34] «La información no siempre está disponible gratuitamente para los investigadores, por lo que deben ser hábiles en diversas técnicas para perseguirlo, localizarlo y recuperarlo.» (Fahsing, 2016, p. 5). En esa línea de ideas Borrás Andrés (2023, p. 24) nos explica que en estos primeros momentos «es frecuente que exista poca claridad acerca de los hechos acontecidos, su tipología delictiva o los sujetos que han participado en ellos.» Además, en adición a la falta de datos, se presenta la circunstancia en la que el tiempo disponible para tomar acciones o decisiones es limitado y crítico. En este caso específico, la ausencia de información acerca de ciertas pruebas digitales entra en conflicto con la posibilidad de que estas sean modificadas, alteradas o incluso eliminadas.

[35] Con respecto a ello, Edmond Locard considerado uno de los precursores históricos del ámbito criminalístico, se refería a esta situación con la frase: «el tiempo que pasa es la verdad que huye». Si bien esta frase emblemática era específica para la evidencia física, hoy tiene una gran significación para la evidencia digital debido a la característica volátil de la misma, y su afectación por el paso del tiempo.

[36] La actividad de investigar es inherente a la vida de los individuos, constantemente nos encontramos realizando procesos investigativos a mayor o menor escala. En nuestra rutina diaria, es común formular suposiciones y elaborar explicaciones hipotéticas sobre lo que aún no comprendemos: como el origen de un mal olor, la causa detrás del retraso de un vuelo, las razones por las cuales alguien podría mentir, o los motivos que llevaron al fin de una relación de pareja. (Mocatelli, 2023, p. 126). Con esto queremos decir que la investigación no es exclusiva de los científicos, «Todo aquel que quiera saber cómo es un aspecto del mundo –el físico y el detective, el historiador y el entomólogo, el químico cuántico y el investigador periodístico, el estudioso de la literatura y el cristalógrafo de rayos X- trabajan en una parte de una parte del mismo vasto crucigrama.» (Haack, 2009, p. 15)

[37] En esa misma línea de ideas, Di lorio et al. (2017) refiere que: la información recopilada permite refinar y adaptar la hipótesis inicial, verificando su idoneidad con respecto a los diferentes tipos de delitos y formas de participación criminal establecidas por la ley.

problemática de lo que se busca, el control intersubjetivo limitado y la protección de los derechos fundamentales, todo esto orientado a la investigación criminal en entornos digitales.

3.1. ¿Qué se busca?

A pesar de que, por lo general, en los primeros momentos de la investigación aún no se cuenta con suficiente información para comprender la complejidad del hecho, el órgano encargado de la investigación debe tomar decisiones que la guíen. Las personas investigadoras, en el lugar del suceso encargados del relevamiento y la recolección de los potenciales elementos de prueba, ya sean físicos o digitales, se encuentran ante un problema importante. Si se cuenta con poca información: ¿Cómo abordar el relevamiento y la recolección? ¿Por dónde se empieza? ¿Qué se busca? ¿Cómo garantizar que los elementos relevados y recolectados sean los suficientes para conocer el hecho?

Como vimos, las actividades de relevamiento y recolección constituyen puntos de inflexión en el proceso de investigación. Esto es así debido a que, en la generalidad de los casos, estas primeras intervenciones son realizadas por personal no especializado en investigación digital. No es exagerado afirmar que, en la mayoría de las ocasiones, el oficial de la ley que protege y examina una escena del crimen desempeña un papel crucial en la determinación de si las pruebas serán utilizadas para resolver o enjuiciar delitos violentos (Guzmán, 2011, p.9).

Por un lado, como la actividad de relevamiento consiste en poder captar de un universo de potenciales elementos de prueba cuáles serían aquellos que contengan la información para acercarse a conocer el hecho, resulta que existen diversas posibilidades de encontrar información digital y esta realidad no siempre es tenida en cuenta por los investigadores. Pondremos un ejemplo. Al investigar un presunto homicidio, en primer lugar, existirá una tendencia a buscar información digital en dispositivos tecnológicos tradicionales como computadoras, teléfonos, discos duros (dispositivos clásicos). Sin embargo, podría existir información relevante que se encuentre en dispositivos menos convencionales, como dispositivos IoT (Internet de las cosas)[38], dispositivos camuflados[39], electrodomésticos

[38] El término Internet de las cosas (IoT por sus siglas en inglés) es definido por la Unión Internacional de Telecomunicaciones (UIT) como la «Infraestructura mundial para la sociedad de la información que propicia la prestación de servicios avanzados mediante la interconexión de objetos (físicos y virtuales) gracias a la interoperabilidad de tecnologías de la información y la comunicación presentes y futuras».

[39] Nos referimos a aquellos dispositivos que han sido alterados o camuflados para que parezcan diferentes de lo que realmente son. Los mismos pueden ocultar su verdadera función o contenido, lo que los hace útiles para diferentes propósitos de espionaje, seguridad o evasión. Por ejemplo, un dispositivo camuflado podría parecer un bolígrafo común, pero en realidad es un grabador de voz o un pendrive.

inteligentes. En ese sentido, Semprini (2017, p. 91) nos comenta: «Las evidencias digitales están adquiriendo formas cada vez más inesperadas en nuevos dispositivos o componentes tecnológicos que desafían los procedimientos y metodologías actuales.»,

La cuestión aquí radica en preguntarse si las personas que intervienen en primer lugar tienen el conocimiento adecuado para, frente a esta escasez de información, saber dónde buscar. Atentos a ese interrogante, nos encontramos con dos realidades; por un lado, y lo más frecuente, es que la actividad de relevamiento lo realice personal policial dotado de una instrucción general, es decir, sin conocimiento especializado en cuestiones tecnológicas específicas.[40] Por otro lado, nos encontramos con la segunda situación, personal policial o forense que tengan alguna o mucha formación en investigar en entornos digitales. Será obvia la respuesta de quien tendrá más herramientas para poder investigar eficazmente, aun contando con poca información sobre el hecho.[41] Entonces, podemos inferir que si no se sabe dónde específicamente buscar, se estará ante el problema de que el universo de elementos posibles será tan abundante que, posiblemente, mucha información relevante podría no ser recabada.

Frente a la escasez de información en la fase de relevamiento, se destaca una cuestión importante: a pesar de los esfuerzos mediante protocolos, guías de actuación o pautas de trabajo para dirigir de la mejor manera posible la actividad,[42] en general, se suele depender en gran medida de la "creatividad" o la "intuición" como herramientas principales para abordar esta actividad[43]. Con respecto a ello, Di lorio, et al. (2017, p. 190) nos comenta que:

[40] Casey (2019, p. 6) al referirse a la gestión deficiente del conocimiento, expresa: «Generalmente, los policías con experiencia forense digital limitada tienen la responsabilidad inicial de identificar las fuentes de evidencia digital y aplicar métodos básicos de preservación y procesamiento. Están expuestos a un alto riesgo de no ser conscientes de las limitaciones de los métodos y herramientas disponibles, lo que conduce a errores y oportunidades perdidas».

[41] En este sentido, algunos autores afirman que tener en claro la metodología de investigación sumada a la adecuada capacidad de los investigadores son elementos claves para lograr investigaciones eficaces. (Roatta et al. 2015, p. 1) Por otro lado, Haack (2009, p. 15) nos habla del aspecto actitudinal. «La investigación puede ser dificultosa y exigente, y con frecuencia ir por el camino equivocado. A veces, el obstáculo es una falla de voluntad; realmente no queremos saber la respuesta suficientemente mala como para cargar con el problema de explicar, o realmente no queremos saber, y generamos una cantidad de problemas para no llegar a saber.»

[42] Los códigos no estipulan ningún requisito, más allá que en la práctica de las actividades de laboratorio. El personal debe cumplir con la norma ISO 17025 y, para las escenas del crimen, cumplir con la norma ISO 17020. (Wilson-Kovacs et al, 2023, p.240)

[43] Partiendo de lo que manifiesta Flashing (2016, p. 11), «los detectives criminales suelen dejarse llevar por sus propias intuiciones.» La crítica en relación con el recurso de la intuición en las investigaciones criminales suele centrarse en la subjetividad y falta de fiabilidad como método de toma de decisiones. En ese sentido, la intuición puede estar influenciada por prejuicios personales, experiencias pasadas o emociones, lo que puede llevar a conclusiones erróneas o sesgadas. Además, la intuición no puede ser verificada ni validada de la misma manera que otras formas de evidencia, lo que la hace vulnerable a cuestionamientos sobre su credibilidad y objetividad. Por su parte, Anderson et al. (2021, p. 588) con respecto al recurso de la «experiencia» nos comenta: A medida que los límites de la experiencia se vuelven menos claros, también lo hacen la propiedad y la responsabilidad, lo que provoca que la evidencia digital, especialmente la proveniente de dispositivos móviles, sea cuestionada en los tribunales.

> Debido a la falta de adecuación de normas procesales que definan concretamente la cuestión en análisis, estos se encuentran frente a un panorama de cierta incertidumbre, en la que impera el ingenio y la creatividad en la recolección de la evidencia que sustenta una investigación penal.

Con la finalidad de poder contrarrestar actividades tan subjetivas, la mayoría de los protocolos o guías de buenas prácticas recomiendan que se brinde información contextual a las personas investigadoras con la finalidad de poder guiar el relevamiento. López (2019, p. 8) Es decir, aportar información sobre el tipo de hecho para orientar qué dispositivos buscar en el lugar del suceso. Por ejemplo, si el hecho tiene relación con un delito en el ámbito financiero o económico, se aconseja buscar en plataforma de juegos, donde generalmente se contactan y ejecutan las actividades delictivas o con palabras claves que se creen que suelen ser frecuentes en la jerga delictiva. Sin embargo, estas prácticas, que provienen de estrategias diarias, pueden traer varios inconvenientes. Reedy (2020, p.497) nos advierte sobre esta última situación cuando manifiesta que: agentes de policía sin formación adecuada descargan datos de teléfonos móviles y ofrecen interpretaciones superficiales que pueden ser incorrectas. Debido a la falta de capacitación, pueden malinterpretar los datos de inmediato, como confundir palabras clave descargadas automáticamente con términos de búsqueda, o interpretarlos sin contexto.

Una vez concluido el relevamiento, identificando las posibles fuentes de información digital, tiene lugar la segunda fase: la recolección. En ese sentido, surgen elementos conflictivos al plantearse qué se debe recolectar y qué no, y en cada caso, la fundamentación del porqué. La fase de recolección tiene su fundamento en que, frente a una diversidad de elementos de interés, se deben considerar recolectados (incautados o secuestrados) los que se consideren adecuados según los objetivos de la investigación. Un término vinculado a la actividad antes mencionada es el concepto de triage. El protocolo para la identificación, recolección, preservación, procesamiento y presentación de la evidencia digital (2023, p. 8) lo define como:

> Proceso de selección de dispositivos o filtrado de información ordenado por la autoridad judicial, quien aporta los criterios de evaluación sobre los dispositivos electrónicos en el lugar del hecho, susceptibles a ser secuestrados para llevar a cabo un posterior análisis forense.

Ahora bien, de acuerdo con lo antes expresado, la información contextual y el triage se establecen como posibles soluciones a las prácticas subjetivas en los primeros momentos de investigación en entornos digitales. Sin embargo, estas dos prácticas traen aparejadas algunas complicaciones si ponemos a la luz de la cuestión probatoria.

En primer lugar, en relación con la información contextual, es importante destacar que la información referente al contexto del hecho suele ser proporcionada a los primeros intervinientes por la fiscalía o las áreas de investigación. El cuestionamiento surge al plantearse si la información suministrada se limita a una única hipótesis del caso (proveniente de la fiscalía), con el riesgo potencial de omitir elementos que respalden hipótesis alternativas, así como circunstancias exculpatorias, en contraposición al principio de inocencia.

En segundo lugar, en cuanto a la utilización del triage en el ámbito de la recolección de evidencia digital, presenta ciertos desafíos y aspectos que podrían ser objeto de crítica. En primer lugar, la dependencia de la autoridad judicial en la definición de los criterios de evaluación para el triage puede introducir sesgos cognitivos,[44] o tomar decisiones que no reflejan adecuadamente la complejidad de la investigación digital, debido a la pobre cultura digital de nuestros sistemas judiciales.

Además, la rapidez requerida en el triage puede llevar a una selección apresurada de dispositivos o información, lo que podría resultar en la omisión de datos relevantes. Este enfoque, centrado en la eficiencia temporal, podría pasar por alto detalles cruciales para la investigación. Otro aspecto crítico podría ser la falta de uniformidad en la aplicación del triage, ya que diferentes autoridades judiciales podrían establecer criterios divergentes,[45] lo que podría generar inconsistencias en la recolección de evidencia digital. La problemática de «¿Qué se busca?» en una investigación en entornos digitales, especialmente en los primeros momentos, cuando la información sobre el hecho delictivo es escasa, presenta varios desafíos. En esta fase inicial, la falta de detalles sobre la naturaleza y el alcance de la conducta delictiva dificulta la definición clara de los objetivos de la investigación en entornos digitales.

3.2. El escaso control intersubjetivo.

Otra de las cuestiones que se plantea frente a la escasez informativa en los primeros momentos de la investigación, y de alguna manera en continuidad con el planteamiento establecido en el

[44] Estos sesgos podrían producirse por la falta de información, conocimiento u objetividad. Duce (2022, p. 79) indica que: "Los sesgos cognitivos son errores sistemáticos en el razonamiento que tienen lugar cuando los seres humanos procesamos e interpretamos información y, por supuesto, las decisiones y conclusiones que tomamos se ven afectadas por ello". La manipulación sesgada de indicios y la elección tendenciosa de premisas para respaldar una hipótesis defensiva o acusatoria generan un efecto antiepistémico al distorsionar y manipular los vestigios del delito (Borrás Andrés, 2023, p. 195). En este caso particular, por ejemplo, podría producirse un sesgo de confirmación al buscar evidencia que respalde una hipótesis en lugar de considerar pruebas que puedan contradecirla, o un sesgo de contexto cuando se expone a los investigadores a datos contextuales que, aunque pertinentes para la situación, no son necesarios para sus funciones (Vázquez, 2023, p. 31).

[45] Reedy (2020, p.497) nos alerta sobre esta situación al manifestar: «Quienes toman las decisiones jurídicas rara vez poseen suficiente competencia técnica para examinar la calidad de la evidencia digital en sí o el proceso en el que se produjo.»

punto anterior, consiste en la limitación o insuficiencia en el control sobre qué elementos deben ser relevados y recolectados. La problemática del escaso control intersubjetivo se refiere a las dificultades asociadas con la verificación y supervisión mutua entre las diferentes personas involucradas en el proceso investigativo, ya sean forenses, fiscales, jueces o defensores. En entornos digitales, donde la complejidad técnica y la rápida evolución de la tecnología son prominentes, la falta de control intersubjetivo puede generar diversas complicaciones.

En los puntos anteriores, hemos reflexionado sobre la naturaleza intuitiva y la falta de regulación en la verificación de actuaciones en el ámbito judicial. Esto nos lleva a considerar un problema fundamental: ¿cómo podemos verificar si las actuaciones son adecuadas y se ajustan a un debido proceso? Por ejemplo, ¿cómo puede un fiscal verificar si un experto forense realizó un relevamiento adecuado si carece de las herramientas específicas para hacerlo? ¿O cómo podemos saber si un oficial de policía llevó a cabo correctamente su labor si el fundamento de la actuación se basó únicamente en la experiencia y la intuición?

Otra de las principales complicaciones se encuentra en relación con la brecha de conocimientos técnicos entre las áreas jurídicas y las áreas forenses o expertos en investigaciones en entornos digitales. Esto implica estar al tanto de los avances tecnológicos, que incluyen el aumento en las capacidades de almacenamiento de datos y la variedad de sistemas, así como realizar inversiones costosas en infraestructura y formación del personal. A pesar de los esfuerzos en curso para abordar estos problemas, las capacidades actuales de los involucrados en el sistema de justicia penal se ven superadas por estas demandas. (Wilson-Kovacs et al., 2023, p. 237).

En esta etapa de la investigación es crucial que la información se transmita adecuadamente, incluso si es escasa, para que pueda cumplir su función. En esa línea de ideas Wilson-Kovacs et al. (2023. p. 237) afirma: «un elemento central de esta interacción es la selección de información y su comunicación oportuna entre la policía, la fiscalía y la defensa.»). Pero estas cuestiones se vuelven dificultosas cuando no se tiene conocimientos mínimos en tecnología.[46] Esto puede resultar en la falta de comunicación efectiva y en la duplicación de esfuerzos, lo que afecta la eficiencia global de la investigación.

[46] Con respecto a ello, Samprini (2017) manifiesta: «el avance y la complejidad de los distintos escenarios hacen necesario que el personal que interviene en los secuestros de dispositivos tecnológicos deba contar con las capacitaciones en incautación para garantizar la suficiencia de la evidencia.»

Se produce una dinámica muy particular: si se tiene poca información sobre el hecho que se está investigando, difícilmente se podrá aplicar una estrategia adecuada para el relevamiento y la recolección. Por su parte, si se tiene poca información y además poca instrucción en cuestiones tecnológicas, difícilmente se podrá reconocer qué potenciales elementos de prueba (además de los convencionales) puedan permitir obtener información sobre las circunstancias del hecho. La falta de información típica, sumada a la falta de conocimiento en cuestiones tecnológicas, puede ocasionar que los investigadores judiciales, tienden a confiar en demasía en los operadores forenses o primeras personas interventoras. Este exceso de confianza en las prácticas, específicamente en las actividades de relevamiento y recolección de potenciales elementos de prueba, no permitiría que se tenga un control intersubjetivo adecuado.

3.3. La protección de los Derechos fundamentales.

Finalmente, en lo que respecta a las cuestiones que surgen ante la escasez de información y considerando las actividades de relevamiento y recolección, podemos señalar la problemática en relación con la protección de los derechos fundamentales.[47] En este sentido, nos centraremos brevemente en un desafío que consideramos evidente en el contexto del presente trabajo: la vulneración del derecho a la intimidad.[48]

La falta de información precisa, sobre lo que se busca, sumado a la falta de control que se tiene sobre ello, puede dar como resultado que potencialmente los derechos fundamentales y, específicamente, el derecho a la intimidad, sean vulnerados[49]. Estas situaciones se dan, por ejemplo, cuando por falta de información característica de los primeros momentos de la investigación, y ante la imposibilidad de buscar información precisa, las personas investigadoras obtienen información de la esfera íntima de la persona irrelevante para la

[47] Binder (1999, p. 71) hace referencia a las garantías establecidas en la Constitución Nacional y Tratados Internacionales como: «escudo protector frente a la fuerza arbitraria y frente a toda posible degradación tiránica del poder.»

[48] El derecho a la intimidad comprende el conjunto de actividades que forman un círculo íntimo, personal y familiar, facultando a todo individuo a excluir a los extraños de entrometerse en él, evitando así una publicidad que no desea el interesado. Se encuentra relacionado con el derecho al honor, a la propia imagen y a la protección de datos, todos derechos personalísimos y protegidos en la gran mayoría de las constituciones estatales. (Becerra; Zarate, 2015, p. 2018). Para Merkel (2022, p. 255) «cuenta con dos componentes: uno positivo, que consiste en el derecho a ejercer el control sobre nuestros datos y la información que queremos compartir con los demás, y uno negativo, que consiste en el derecho a no ser importunado por nadie y a poder excluir a los demás de nuestra esfera privada.»

[49] A ello se refiere Suarez (2021, p. 4) cuando nos comenta: «Las autoridades no saben qué buscar de antemano, y la afectación a la privacidad e intimidad es de tal magnitud, que resultará conveniente legislar sobre la materia.»

causa,[50] pero que es captada de igual forma por el efecto red de pesca.[51] Esta problemática ya era avizorada años atrás. En el año 2001, el Consejo de Europa, durante su reunión en Budapest, firmó el Convenio sobre Ciberdelincuencia. En su preámbulo, destacó la necesidad de respetar los derechos humanos reconocidos por varios tratados internacionales, incluyendo explícitamente la privacidad de todas las personas y la protección de sus datos personales y comunicaciones. Demandando un «equilibrio adecuado» entre ellos. (Bernard, 2021, p. 40).

Específicamente, nos referimos en este caso a aquellas situaciones donde en los primeros momentos de la investigación se relevan dispositivos o fuentes de información digital, que además de la información autorizada a buscar, se obtiene otro tipo de información sensible sobre la vida del individuo o también información considerada neutral.[52] La característica propia de la era digital trae aparejada esta problemática que debe ser tenida en cuenta para no vulnerar los derechos fundamentales. Teniendo en cuenta que tienen la capacidad de poner en riesgo seriamente la privacidad de los individuos, dado que significa que una gran cantidad de datos personales estará accesible para las autoridades y las fuerzas de seguridad, (Ferreyra, 2018, p. 9) y los cuestionamientos que puedan surgir con relación al uso inadecuado de dicha información.

Es importante recordar que una computadora o un teléfono celular no constituyen evidencia en sí mismos, sino que son dispositivos de almacenamiento. La verdadera evidencia digital reside en los datos contenidos dentro de estos dispositivos. Esta distinción plantea dificultades al tratar de aplicar las mismas reglas a la evidencia física y digital por analogía, lo que puede resultar en la violación de las garantías constitucionales de los ciudadanos. (Suarez, 2021, p. 4)

Considerando, que no todos los datos personales son sensibles y cualquier petición de información no necesariamente vulnera derechos constitucionales, existen diversos niveles de impacto, desde una intrusión mínima hasta una más significativa, y su admisión está condicionada al cumplimiento de ciertos requisitos. (Bernard, 2021, p.52). Sin embargo, resulta

[50] «Se advierte que, con facilidad, se puede vulnerar la privacidad de las personas investigadas si se realizan pedidos de información indiscriminados, en base a sospechas fundadas en datos sensibles como orientación política, religión, raza, etc., que podrían conducir incluso a prácticas que atenten contra el derecho a la igualdad y el ámbito de reserva de cada ciudadano.» (Bernard, 2021, p. 42)

[51] El término «efecto red de pesca» lo utilizamos en este sentido para describir una práctica en la que los investigadores, en un intento de obtener información relevante para una investigación criminal, recopilan datos de manera indiscriminada y extensiva, ya sea por la falta de información o con la esperanza de atrapar cualquier información potencialmente útil. Este enfoque a menudo se asocia con la obtención de información masiva, incluida la que no está directamente relacionada con la causa que se investiga.

[52] Como información neutral queremos significar aquella que no ofrece inconvenientes, salvo que se almacenen junto a otros o se crucen.

importante poder remarcar la potencial vulneración de derechos fundamentales en estas situaciones particulares cuando se investiga en entornos digitales.[53]

Tal vez, el problema central radica en no tener la notable distinción entre la evidencia física y la evidencia digital, y que ello tiene un impacto directo tanto en la forma en que se llevan a cabo las medidas de investigación como en las garantías constitucionales de los ciudadanos (Suarez, 2021, p. 3). En ese sentido, se requiere reconsiderar y reexaminar los conceptos legales convencionales y considerar las nuevas formas y usos de los derechos constitucionales tradicionales, establecidos en un contexto completamente diferente al presente[54] (Merkel, 2022, p. 15).

4. El desborde de información digital en la fase de investigación.

Sumado a la problemática de la falta de información cuando se investiga en entornos digitales encontramos los inconvenientes relacionados con la cantidad de información generada en esta instancia. [55]

Para comprender mejor la problemática, podemos considerar algunos datos de referencia. Por ejemplo, los informes de análisis de dispositivos con posible evidencia digital suelen entregarse en formato PDF por parte de las áreas de investigación. Un teléfono de 8 GB produce un informe de aproximadamente 10.000 páginas, uno de 32 GB de 40.000 páginas, y uno de 128/256 GB de 100.000 páginas. Aunque estos números no son impactantes en sí mismos, pueden resultar abrumadores al analizarlos en un caso específico. Los investigadores de hechos criminales tienen acceso a una amplia gama de dispositivos, y las capacidades de almacenamiento de los mismos están en constante aumento. Además, se pueden agregar los

[53] Como ejemplo ilustrativo de la problemática, se puede mencionar el caso Estados Unidos vs. Walser. Durante una investigación relacionada con la venta de drogas, una oficial de policía entró en contacto con una computadora portátil propiedad de Walser. Después de varias horas de búsqueda, encontró material visual relacionado con pornografía infantil, lo que llevó a su acusación por posesión de dicho material, a lo que se declaró culpable. Posteriormente, Walser solicitó al Tribunal de Distrito que excluyera las pruebas obtenidas durante el registro de su computadora personal, argumentando que la oficial había excedido el alcance de la orden al abrir un archivo de video que no guardaba relación con la investigación. Se argumentó que los archivos apropiados para la búsqueda serían aquellos de texto o planillas. Este caso se puede consultar en el siguiente enlace:https://caselaw.findlaw.com/court/us-10th-circuit/1004455.html

[54] En ese sentido Lanzón (2023, p.108) manifiesta: «Debido a ese cuadro, es sencillo concluir que la "privacidad" ha pasado a ser un concepto dinámico y fuertemente condicionado al contexto social. Indudablemente, el universo digital que atraviesa la vida actual de las personas jamás pudo ser imaginado por el constituyente de 1853.» En clara alusión a la realidad social de la época donde se sentaron las bases jurídicas del estado argentino.

[55] El extenso alcance y la cantidad masiva de estas huellas digitales presentan nuevos desafíos para las fuerzas policiales, ya que deben ser capaces de identificar y ubicar estas «pistas de investigación» dentro del vasto océano de datos digitales y el constante flujo de información que la mayoría de las personas generan en la actualidad. En cuanto a sus causas, Collie (2018, p.1) señala la considerable influencia de la tecnología, al afirmar: «La enorme cantidad de datos digitales que los agentes policiales deben investigar se ha convertido en una carga considerable.»

datos proporcionados por las empresas tecnológicas y los provenientes de fuentes de acceso público (Di lorio, 2017, p. 554).

En este apartado, nos referiremos a dos aspectos relacionados con el efecto desborde que se produce en la investigación en entornos digitales y que resulta interesante tener en cuenta en el contexto del impacto que puede producir en la actividad probatoria: a) la multiplicidad de las fuentes, y b) el riesgo de pérdida de información relevante.

a) En relación al primer aspecto, consideramos que requiere fundamental reflexión cuando nos referimos al desborde de información digital, por el impacto que puede producir cuando se está investigando en entornos digitales. Con la creciente digitalización de la sociedad, el universo de fuentes de información disponibles para las investigaciones criminales ha experimentado un crecimiento exponencial.[56] Las opciones de búsqueda de información son variadas y heterogéneas y las fuentes de datos pueden ser muy diversas. (Di lorio, 2017, p. 68). En ese sentido, podemos destacar dos aspectos, uno positivo y otro negativo. El aspecto positivo se refiere a la mayor posibilidad que trae aparejado la inclusión de fuentes que antes no existían.[57] El aspecto negativo, y que representa realmente un gran desafío en la actualidad,[58] consiste en la problemática de la diversidad de dispositivos clásicos y no tan clásicos que podrían contener información de interés para la investigación, sumado a la caudalosa información que es aportada por los mismos, y que podría dar respuesta a preguntas claves, como por ejemplo: ¿Cuándo ocurrió el hecho?, ¿Dónde ocurrió precisamente?, ¿Quiénes pueden tener relación con el mismo?, entre otros aspectos.

En referencia a ese asunto, a nivel de la práctica investigativa, frecuentemente se solicita a los investigadores la obtención de diversas fuentes que potencialmente puedan contener evidencia digital, indicando que se extraiga del dispositivo información relevante para la causa sin especificar un criterio determinado. Esta dinámica trae varias problemáticas en el contexto de la investigación criminal, como son: falta de claridad en los criterios de relevancia, pérdida de

[56] «Durante las últimas dos décadas, el impacto del cambio tecnológico condujo al crecimiento exponencial de la diversidad de fuentes y el volumen de evidencia digital, el uso de la misma en los tribunales y una escasez de experiencia forense digital.» (Wilson-Kovacs et al., 2023, p. 238)

[57] Hasta hace poco, era impensable utilizar datos de electrodomésticos como lavarropas, aire acondicionado, medidor de agua o televisores para investigaciones criminales. Un caso destacado involucra el seguimiento de una persona que cometió un hecho delictivo utilizando un televisor conectado a Netflix. Se puede acceder a más detalles en el siguiente enlace: https://www.lacapital.com.ar/robo-varios-electrodomesticos-y-lo-rastrearon-un-televisor-conectado-netflix-n1502260.html

[58] Respecto a eso, un estudio reciente sobre cómo los abogados defensores penales en el sistema acusatorio inglés entienden y utilizan la evidencia digital, indica que la cantidad y variedad de pruebas digitales contribuyen a tensiones, retrasando el acceso a dichas pruebas y prolongando los tiempos de respuesta para su análisis, tanto para la fiscalía al presentarlas como para la defensa al solicitarlas. (Wilson-Kovacs et al., 2023, p. 250)

datos potencialmente importantes (cuestión que trataremos en el siguiente punto) y potencialmente, la vulneración de derechos fundamentales como vimos anteriormente.

El desafío surge al considerar que una fuente de evidencia digital produce una gran cantidad de datos. Si esto se extiende a varias fuentes, la cantidad de datos aumenta considerablemente, lo que podría dificultar su análisis adecuado debido a la limitación de tiempo durante la investigación y a la frecuente escasez de recursos materiales y financieros. Frente a esta situación, el sistema de justicia suele reaccionar de la siguiente manera: a mayor cantidad de fuentes de evidencia digital, menor capacidad de análisis de los datos.

La multiplicidad de fuentes presenta desafíos en la investigación, especialmente en los primeros momentos. A corto plazo, no parece haber una mejora en esta situación debido a la creciente dependencia de dispositivos electrónicos en la sociedad. Aunque esta tendencia podría ofrecer más información para las investigaciones, también conlleva desafíos adicionales, como la selección de fuentes pertinentes y el manejo de grandes cantidades de datos en fases posteriores. Este riesgo se agrava aún más por la naturaleza cambiante y en constante evolución de la tecnología (Wilson-Kovacs et al., 2023, p. 250)

b) En relación al segundo aspecto, la sobreabundancia de información digital presenta un riesgo significativo para la investigación en entornos donde se gestiona gran cantidad de datos. Este exceso de información puede dificultar la identificación de los elementos cruciales, además, puede llevar a la pérdida de tiempo y recursos al tener que revisar una cantidad considerable de datos, muchos de los cuales pueden resultar irrelevantes.

Lo interesante sería preguntarnos, ¿con qué criterios se establece la relevancia de una determinada fuente de información digital en los primeros momentos de la investigación? Si recurrimos al criterio de relevancia señalado por la norma ISO/IEC: 27037:2012, se indica un aspecto técnicamente jurídico que se refiere a los elementos pertinentes a la situación en cuestión, destinados a demostrar o refutar una hipótesis planteada sobre los hechos. Todo aquello que no satisfaga este criterio será considerado como irrelevante y no será tomado en cuenta como evidencia en el caso que se está analizando (Semprini, 2017, p. 92), Esto no lleva a inferir que el criterio de relevancia digital deviene del criterio de relevancia o pertinencia de todo contexto epistemológico. Pero evidentemente, se constata una carencia de pautas racionalmente acordes a la complejidad de investigar en estos entornos.

Lo anteriormente expuesto se verifica en la práctica. A veces se opta por secuestrar la mayor cantidad de fuentes, otras veces las «más significativas».[59] Ahora bien, este último punto podría ocasionar problemas considerables para determinar cuál es la prueba relevante. Partiendo de la idea de que existen casos en los que ni siquiera se sabe si se cometió un delito, es decir, no se tiene claridad en estos primeros momentos de la investigación si el hecho constituye un ilícito. O, por otro lado, existen casos en los que se sabe que se cometió un delito, pero no se conoce cuál fue el delito específico ni los detalles del caso. ¿Cuál sería entonces el objeto de prueba a relevar o adquirir? ¿Cómo se podría garantizar que no se pierda la información relevante?

Teniendo en cuenta que «la atención en la racionalidad de la valoración de la prueba tiene sus raíces en la asunción de que ésta es la mejor garantía de la mayor aproximación entre lo que resulta probado en el procedimiento y la verdad sobre los hechos» (Vázquez, 2015, p. 102), resulta indispensable considerar en los momentos iniciales de la investigación, donde los elementos probatorios comienzan a conformarse, la multiplicidad de las fuentes, el escaso control intersubjetivo y la pérdida de información relevante son aspectos que deben ser tenidos en cuenta para lograr un razonamiento adecuado.

5. La tensión entre la poca información en los primeros momentos de la investigación y la sobreabundancia de información digital. Su impacto en el debido proceso.

La escasez informativa y la sobreabundancia de información parecieran ser una contradicción paradójica. Sin embargo, forman parte de la realidad compleja que implica investigar en contextos actuales, donde los diferentes dispositivos, fuentes de información digital, son fundamentales para aproximarse a la verdad sobre los hechos.[60]A continuación, describiremos brevemente dos puntos de contacto donde se produce dicha tensión en la investigación criminal y sus implicancias en el debido proceso.

a) La tensión entre la recolección indiscriminada de información y la vulneración de los derechos fundamentales. Como pudimos constatar, una de las cuestiones que surgen debido a la escasa y abundante información, cuando se investigan en estos entornos, es lo referido a la

[59] A ello se refiere Anderson, et al. (2021, p.595) cuando señala que, en determinadas circunstancias, se puede considerar apropiado adquirir todos los dispositivos digitales disponibles. No obstante, en tales casos, se deben justificar las acciones tomadas, explicar la importancia de los elementos para la investigación y declarar el propósito de su adquisición

[60] Lanzón (2023, p.107) manifiesta que premisas fácticas, usualmente corroboradas mediante testimonios, peritajes o informes de entidades públicas o privadas, se podrán validar de forma más eficiente y directa mediante evidencia digital. Concluyendo incluso que las pruebas digitales pueden ofrecer una mayor certeza y fiabilidad que las pruebas disponibles en el mundo físico.

potencial vulneración de garantías constitucionales. En este sentido, se intensifica la continua tensión entre el interés por la persecución de los crímenes y el respeto por las libertades de los individuos.[61] (Merkel, 2022, p. 47). Debido a la falta de regulación específica sobre la evidencia digital en nuestros sistemas procesales, se revivió esta tensión entre la necesidad de investigar por parte del Estado y el derecho de los ciudadanos. Agregando otras aristas a debatir, cómo la diferencia entre el tratamiento de la evidencia física, la digital y su uso como prueba en el proceso.

Si bien esta tensión seguramente estará latente en todo el proceso penal, resulta que en los primeros momentos donde entran en contacto, la poca información junto con la abrumadora cantidad de datos podría potenciar estos riesgos al no ser reconocidos, detectados o, en el peor de los casos, sean vulnerados voluntariamente. La discusión no es nueva; dicha tensión es un tema bastante tratado en el ámbito probatorio.[62] Sin embargo, la cuestión digital la intensifica, debido a las características propias de este tipo de evidencia, las nuevas tecnologías, y las diferencias que se plantean con la evidencia material. En esa misma línea de ideas, Dupuy (2021, p. 272) considera que «el derecho penal y procesal clásicos se han construido sobre un modelo de delincuencia física e individual.» Teniendo en cuenta esa consideración, la dinámica entre la necesidad de investigar y la protección de los derechos de los individuos debe evolucionar y actualizarse mediante discusiones actuales.

Si consideramos un ejemplo actual y muy habitual, como lo es, el acceso del Estado al teléfono inteligente de un individuo sospechoso de haber cometido un delito, implica una intromisión mucho más invasiva que la que se produce con un registro domiciliario o una requisa personal en la vía pública.[63] En consecuencia, dado el mayor impacto en la garantía constitucional, parece razonable que existan mayores controles para permitir tal intromisión, a pesar de que esto no esté específicamente contemplado en ninguna cláusula constitucional o convencional. (Lanzón, 2023, p. 114).

[61] En esa misma línea de ideas, Bernard (2021, p. 34) se refiere a una tensión entre las protecciones de los ciudadanos y el ejercicio del poder punitivo por parte del Estado, junto con las características inherentes al sistema acusatorio, se aborda a través de la antinomia fundamental del proceso penal, lo que permite equilibrar las fuerzas opuestas de manera justa durante las investigaciones penales.

[62] Como ejemplo, podemos señalar las discusiones en relación al uso de tecnologías de vigilancia masiva mediante reconocimiento facial, en relación al derecho a la privacidad, la interceptación de las comunicaciones, etc.

[63] En este caso, Lanzón (2023, pp.119) considera la marcada diferencia entre los datos obtenidos en un registro virtual (por ejemplo, un teléfono móvil) en relación con el físico (allanamiento de morada). En el primero se obtiene una inmensidad de datos relacionados con toda la esfera del individuo, inclusive relaciones con otras personas, etc. En la física, el límite es más claro y restringido.

Pero, sin duda, la falta regulación en la temática, junto a actividades de búsqueda basadas en la experiencia o en la intuición podrían provocar una recolección indiscriminada de información y, con ello, la obtención de gran cantidad de datos que dudosamente podría ser procesados racionalmente respetando, por ejemplo, la intimidad de las personas.[64] Teniendo en cuenta que el cuidado de los derechos fundamentales de las personas acusadas es un requisito riguroso para un debido proceso enmarcado en las constituciones y tratados internacionales, resulta imprescindible considerarlo al investigar en entornos digitales.

b) La tensión entre la escasez de información que tiene como efecto la adquisición indiscriminada de datos, versus la abrumadora cantidad de datos y su impacto en el derecho de defensa. De la misma forma en que para la fiscalía es dificultoso poder analizar la inmensa cantidad de información relevante e irrelevante que se obtiene de la investigación en entornos digitales, para la defensa lo es aún más, principalmente, porque no hay paridad de armas.[65]

Considerando la interpretación de Maier (1999, p. 577) sobre el derecho de defensa, implicando la capacidad de probar y controlar la prueba para garantizar la igualdad de posiciones, surgen varias problemáticas en este sentido. La primera de ellas se refiere al escaso control que puede ejercer la defensa ante las actividades intuitivas, fundamentadas desde la experiencia y realizadas en las fases de relevamiento y recolección, por parte de los investigadores en los primeros momentos de la investigación.[66] Como mencionamos, la falta de regulación en la temática dio lugar a normas técnicas diversas y no vinculantes, que muchas veces imposibilitan que la defensa pueda esgrimir algún cuestionamiento sobre los procedimientos llevados a cabo en el lugar del hecho.[67] Y en el caso de hacerlo y utilizar normas técnicas, como por ejemplo las normas ISO, dichos planteos pueden no ser considerados si el

[64] En el momento de realizar una diligencia que permite la incautación de evidencia digital, como un registro domiciliario, la fiscalía suele carecer de detalles precisos sobre lo que se busca confiscar. Por lo tanto, se requiere analizar cada dispositivo encontrado para determinar dónde puede estar la evidencia. La duración de esta diligencia depende de varios factores, como las herramientas forenses disponibles, el volumen de información recuperada, que no puede preverse de antemano, y el tipo de archivos en los dispositivos, como la encriptación (Lanzón, 2023, p.120).

[65] En ese sentido, se espera que la defensa tenga igual acceso para utilizar y cuestionar todas las pruebas de la acusación. (Wilson-Kovacs, et al., 2023, p.238)

[66] A eso deberíamos sumarle la actitud acrítica de las hipótesis policiales (Borrás Andrés, 2023, p. 231). Nieva Fenoll (2021, pp. 491-492) al criticar el sistema acusatorio advierte sobre esta situación, manifestando: «según el sistema, quienes recogieran el cuerpo del delito de la escena de un crimen, por ejemplo, lo que es absolutamente obvio que no es así. Incluso en los casos en que no hay nada que recoger al no implicar el delito la sangre de nadie, jueces y fiscales tienen la demasiado frecuente costumbre de encargar informes policiales en algunos delitos económicos o de otra índole que no dejan de ser forzados, al no tener la policía preparación para tales investigaciones que implican complejas operaciones económicas, societarias, urbanísticas o administrativas en general.»

[67] En ese sentido Dupuy (2022, p. 275) nos indica que la falta de regulación en evidencia digital provocó la aplicación del principio de libertad probatoria, trasladando por analogía las normas establecidas para la recolección de evidencia física a las investigaciones en entornos digitales.

juez así lo determina, debido a la falta de carácter vinculante.[68] También deberíamos sumar a esa cuestión que dichas normas no son de acceso público, es decir, requieren una suscripción para poder entrar en contacto con tales recomendaciones.

Por otro lado, podemos advertir que, ante la inmensidad de datos proporcionados por la multiplicidad de fuentes provenientes de entornos digitales, en la práctica judicial es muy habitual que la fiscalía presente un extracto de la información considerada relevante, es decir, datos filtrados de acuerdo con el supuesto interés de la investigación. Wilson-Kovacs et al., (2023, p. 245) se refiere a ello cuando indica que debido a la abundancia de información disponible no se exhiben todos los datos en su totalidad, sino más bien una síntesis del análisis del dispositivo. Dado que los equipos de defensa suelen recibir informes adaptados (como documentos PDF u hojas de cálculo de Excel) en lugar de datos en bruto y archivos de casos generados durante las fases iniciales de una investigación. La claridad y la transparencia cobran una relevancia particular cuando se tiene que ejercer una adecuada defensa.

Aun en el mejor de los casos, la información aportada por el entorno digital es tan abundante que, si la fiscalía proporcionara datos sin procesar, la defensa se encontraría con una gran cantidad de información, parte de la cual puede resultar irrelevante. Revisar exhaustivamente todo el contenido del dispositivo puede ser un desafío considerable y consumir una cantidad de tiempo muy notable (Wilson-Kovacs et al., 2023, p. 245).

Estos aspectos en tensión, deben ponerse en contexto con realidades que, usualmente, se manifiestan desde la práctica de la defensa y que no deben pasarse por alto como: la desigualdad de armas en relación con los recursos tecnológicos para analizar las fuentes de evidencia digital, en comparación con los recursos del Ministerio Público Fiscal.

6. Conclusiones y algunas propuestas para abordar los desafíos identificados.

Como pudimos constatar, la tensión entre la escasez y la sobreabundancia de información cuando se investiga en entornos digitales tiene implicancias significativas para el debido proceso, por eso es necesario poder abordarlos desde diferentes perspectivas, porque indudablemente si los problemas son complejos el abordaje debería ser lo más integral

[68] Sobre la cuestión de los protocolos y la utilización por parte de la defensa, Merkel (2022, p. 215) considera que la jurisprudencia debe definir claramente las implicaciones del incumplimiento de los protocolos. Sin embargo, la falta de uniformidad en dichos protocolos resulta en una posición difusa, especialmente en lo que respecta a las consecuencias legales de su violación. La jurisprudencia, siguiendo el principio de legalidad, tiende a ser cautelosa al rechazar pruebas en estos casos, prefiriendo abordar la resolución del problema en el ámbito de la evaluación de la evidencia.

posible. En este último apartado, y a modo de conclusión, veremos algunas propuestas que, si bien seguramente no serán las únicas, pueden ser útiles para ampliar la discusión y contribuir a una mejora en el sistema de justicia.

Un aspecto que consideramos transversal a las problemáticas descritas se relaciona con la alfabetización digital y la necesidad de una cultura forense digital en el sistema. En ese sentido, nos referimos a la necesidad de adquirir conocimientos y habilidades adecuadas para los procesos de investigación actuales. No es suficiente proporcionar simplemente herramientas tecnológicas a los sujetos que integran el sistema de justicia, ya que la alfabetización digital no se desarrollaría automáticamente como un efecto de osmosis.[69] Sino más bien, la adquisición de tecnología debería implicar también un programa formativo que permita crear habilidades, destrezas y una visión crítica de la información obtenida por esos medios.[70] El primer paso podría ser el más obvio: ser conscientes de que el sistema de justicia requiere una reflexión en este sentido y que los integrantes del sistema, en su mayoría, necesitan adquirir conocimientos tecnológicos para realizar procedimientos racionales acordes a un debido proceso.[71]

El asunto de la formación tiene un rol fundamental y empezó a ser muy debatido en el ámbito doctrinario. Por ejemplo, Marina Gascón (2016, p.365) se refiere a la educación de los jueces, pero perfectamente aplicable a otros sujetos que conforman el sistema de justicia. En ese sentido, la pregunta que surge es la siguiente: ¿Qué conocimientos deberían ser considerados básicos? La autora propone instruir en cuestiones básicas como método científico, estadística, etc., y en cuestiones elementales de las disciplinas forenses más requeridas, teniendo en cuenta que hay gran diversidad de temáticas. Sin lugar a dudas los conocimientos tecnológicos se presentan como un contenido necesario para las investigaciones actuales y que ningún sujeto que integre el sistema de justicia en la actualidad podría realizar su actividad de manera eficiente (de defensa, investigación, acusación, y juzgamiento) sin contar con herramientas que provengan de la cultura digital.

---

[69] «Podría pensarse que con el solo hecho de situarnos en un ecosistema de digitalidad nos encontramos permeados por algún tipo de pedagogía digital, como si este proceso se agotara sólo a través del acceso y el manejo de tecnologías digitales. Esta creencia se ve impulsada por la presencia de una ingeniería legal aparentemente eficiente (al menos como diseño enunciativo), pero vivir en una sociedad soportada por tecnologías digitales, cuya dinámica se define por sistemas informativos, no presupone una comprensión de los efectos de esta cultura, y lo determinante que se han vuelto estas herramientas para las capacidades cognoscitivas.» (Morán Reyes, 2022, p. 195)

[70] Como programa formativo, no solo nos referimos a actividades de capacitación formal o académica; sino más bien a programas que integren varias áreas, como la teoría, la práctica, las interrelaciones con otros sujetos del sistema, la generación de una visión crítica y la adquisición de habilidades de acuerdo con la función a desempeñar, entre otros aspectos.

[71] Como conocimientos tecnológicos nos referimos a: nociones sobre tipos de dispositivos, sistemas de almacenamiento de datos, sistemas de comunicación, redes sociales, perfiles, cuentas, registros de conexión, etc.

Con respecto a lo anterior, desde la práctica, hace algún tiempo se comenzó a observar la creación de fiscalías especializadas con el propósito de enfrentar las diversas dificultades asociadas con la investigación en estos entornos. La falta de conocimiento forense digital en el sistema de justicia ha llevado a la formación de unidades especiales, como las dedicadas al cibercrimen. Estas fiscalías si bien constituyeron un gran paso para el momento, hoy por hoy, pensar que los hechos que investigamos donde también buscamos evidencia digital son especiales, podría ser un error. La investigación en entornos digitales pasó a ser la regla y no la excepción.[72] Según Dupuy (2021, p. 282), los delitos informáticos no constituyen un conjunto definido, lo que implica que la recolección de pruebas no se limita únicamente a los delitos tipificados en la ley 26.388.[73] Para investigar es necesario contar con pruebas electrónicas que respalden algún aspecto de la teoría del caso tanto del fiscal como de la defensa, o para complementar la evidencia obtenida de fuentes físicas.

Como vimos, el problema no les compete solo a los juristas. Las áreas investigativas, policiales, la defensa e inclusive los científicos forenses requieren de un progresivo avance de su cultura digital. Cultura que implica, como dijimos anteriormente, la adquisición de conocimientos, habilidades, destrezas en procesos racionales que generen una postura epistémica adecuada frente a la información proporcionada por los medios tecnológicos. Consideramos en ese sentido que investigar en entornos digitales, hoy en día, no debe ser una especialidad, debe formar parte de un conocimiento general.

Al ser un tema complejo dijimos que las soluciones deben ir de la mano con otras acciones necesarias, como una mayor regulación en la gestión de la evidencia digital. Aquí reside nuestro segundo aspecto considerado transversal, lo referido a la necesidad de una regulación específica en pruebas digitales.[74] Esta cuestión, sin duda, creemos que es la más compleja de abordar

[72] Lanzón (2023, p. 124) se manifiesta en esa dirección, afirmando que la situación actual requiere no solamente la creación de unidades especializadas y organismos de apoyo con conocimientos técnicos para abordar los desafíos mencionados. Además, es necesario implementar programas de formación para todo el personal del sistema penal. Es preocupante que las facultades de derecho no estén respondiendo a esta realidad ajustando sus planes de estudio para incluir el estudio de las implicaciones técnicas y jurídicas de la evidencia digital, como destacan expertos en la materia. En Argentina por ejemplo hace unos años se crearon: Unidad Fiscal Especializada en Ciberdelincuencia (UFECI, 2015, MPF de la Nación), Fiscalía especializada en cibercrimen (2018, MPF Córdoba) destinados a abordar delitos específicos como, aquellos casos en los cuales el sistema informático haya sido el objeto del delito o haya sido el medio principal o accesorio para cometerlo. https://www.mpf.gob.ar/ufeci/

[73] En este sentido se refiere a la Ley de delito informático promulgado en Argentina en el año 2008, y que incluye categorías como: robos de datos personales, de información comercial estratégica, suplantación de identidad, fraudes informáticos, ataques como cyberbulling, grooming, phishing,etc.

[74] Dupuy (2021, p. 283) afirma en este contexto, que existe una carencia de normas procesales penales para investigaciones 4.0. Con ello se refiere a que, la evolución en las formas delictivas subraya la importancia de contar con marcos legales que permitan aprovechar el potencial de la tecnología para llevar a cabo investigaciones

porque depende de varios factores por tratarse de una política pública. En este sentido, el camino se iniciaría definiendo, en primer lugar, si la cuestión, se identifica socialmente como una problemática, susceptible de ingresar en la agenda pública. Cuestión promovida no solamente desde lo político, sino también desde la academia, la seguridad, el Poder Judicial, y la sociedad en general, para ser abordada por los poderes del Estado, en este caso, el Poder Legislativo.

Frente a la necesidad de regulación, una experiencia a destacar, independientemente de lo referido sobre las normas técnicas que indican procedimientos para el tratamiento de la evidencia digital (normas ISO), se constata en el Consejo de Europa[75]. Uno de los documentos, EEG, por ejemplo, está orientado (a diferencia de las ISO) a servir como un punto inicial para que los legisladores desarrollen reglamentos específicos sobre el tratamiento de la evidencia digital acordes a un debido proceso. Por su parte, la guía de ENISA se centra en los requisitos formativos que deben cumplir los primeros interventores en investigaciones en entornos digitales. Por último, las directrices de la OLAF (2016) profundizan en una cuestión muy relevante a la luz de las problemáticas abordadas en el presente trabajo, proponiendo etapas intermedias que actúen como filtros. Esto podría ayudar a enfrentar la problemática de la multiplicidad de fuentes y la abrumadora cantidad de información que, potencialmente, podría afectar los Derechos Fundamentales.

En conclusión, los primeros momentos de la investigación demandan un mayor debate y reflexión. Es crucial un razonamiento probatorio sólido en estas etapas iniciales para establecer un marco acorde con el debido proceso. Esto podría ayudar a prevenir el tratamiento inadecuado de la información obtenida de los entornos digitales, mejorar su calidad epistémica y salvaguardar los Derechos Fundamentales. Una regulación adecuada en el tratamiento de la evidencia digital proporcionaría directrices (actualmente muy escasas) para los integrantes del sistema de justicia, lo que permitiría un mayor control de los procesos de relevamiento y adquisición, así como en las fases subsiguientes, asegurando un abordaje adecuado en los primeros momentos de la investigación. Además, promover una mayor alfabetización digital en el sistema de justicia colaboraría en la reducción de actividades intuitivas, facilitando un tratamiento más racional y, por ende, con mayor control intersubjetivo de los elementos probatorios provenientes de estos entornos.

criminales efectivas, al mismo tiempo que se garantizan los derechos fundamentales de las personas, según lo establecido en la constitución.

[75] En ese sentido, nos referimos a: La Guía para Policías Fiscales y Jueces EEG (2014); Guía básica para primeros intervinientes ENISA (2015) y las directrices sobre procedimientos forenses digitales para el personal de la OLAF (2016).

VIII: BIBLIOGRAFÍA.

- Abimbola, K. (2002). Abductive Reasoning in Law: Taxonomy and Inference to the Best Explanation. En M. Maccrimmon y P. Tillers (Eds.), *The Dynamics of Judicial Proof: Computation, Logic and Common Sense*. Physica-Verlag Heidelber.

- Anderson, T; Shum, D; Twining, W. (2015). *Análisis de la prueba*. Marcial Pons.

-Anderson, P; Sampson, D; Gilroy, S. (2021). Digital investigations: relevance and confidence in disclosure. *ERA Forum*, (22), 587–599

-Becerra, M; Zárate, P. (2015). Intimidad y Privacidad en Entornos Digitales luego de la Reforma del Código Civil. *15º Simposio Argentino de Informática y Derecho*.

-Benard, J. (2021). Equilibrio entre el derecho a la intimidad y el poder investigativo del Estado en la era digital. *Revista Jurídica de la Universidad de Palermo, (2*). 33-62

- Borrás Andrés, N. (2023). La instrucción sin perjuicios. La necesaria limitación a la recogida de vestigios. Marcial Pons.

-Binder, A. (1999). Introducción al Derecho Procesal Penal. AD-HOC.

-Casey, E. (2019). The chequered past and risky future of digital forensic. *Australian Journal of Forensic Sciences, (51),* 1-16.

- Collie, J. (2018), "Digital forensic evidence—Flaws in the criminal justice system. *Forensic Science International, (289),* 154-155.

-Contissa, G., Lasagni, G. (2020). When it is (also) Algorithms and AT that decide on Criminal Matters: In Search of an Effective Remedy. *Eropean Journal Of Crime, Criminal Law and Brill Criminal Justice*. (28), 280-304

- Convenio sobre ciberdelincuencia (2001). Budapest.

- Di Iorio, A., Castellote, M., Constanzo, B., Curti, H. (2017). *El rastro digital del delito: Aspectos técnicos, legales y estratégicos de la informática forense*. UFASTA.

-Duce, M (2013). *La prueba pericial*. Didot.

-Duce, M (2022). Las comunidades expertas y los sesgos cognitivos de los peritos. *Manual de prueba pericial*. Escuela Federal de Formación Judicial. Consejo de la Judicatura Federal.

- Dupuy, D (2021). *Tratado de la prueba electrónica*. Tomo III. La Ley.

- European Anti-Fraud Office. (2016). Guidelines on Digital Forensic Procedures for OLAF Staff.

-Fahsing, I. (2016). The making of an expert detective. Thinking and Deciding Criminal Investigations *[Tesis doctoral, University of Gothenburg]*. Politihøgskolen institujonelle arkiv.

-Fernando, R (2021). La evidencia digital en el proceso penal y la preservación de los derechos fundamentales. *Escola Superior do Ministério Público do Ceará, (13),* 135-161.

-Ferrer Beltrán, J (2020). *Del Derecho al razonamiento probatorio*. Marcial Pons.

-Ferrer Beltrán, J (2021). Prueba sin convicción. *Estándares de prueba y debido proceso. Marcial Pons.*

-Ferreyra, E. (2018). La Convención de cibercrimen de Budapest y América Latina. Breve guía acerca de su impacto en los derechos y garantías de las personas". *Asociación por los Derechos Civiles, (1).*

- Gascón Abellán, M (2016). Conocimiento experto y deferencia del juez. Apunte para la superación de un problema. *DOXA, Cuadernos de Filosofía del Derecho*. *(39,* 347-365.

- Guzmán, C (2011). Manual de Criminalística. BdeF. Buenos Aires.

- Haba, E (1990). Racionalidad y método para el Derecho: ¿Es eso posible? *DOXA.Cuadernos de filosofía del Derecho, (07),* 169-247.

-Haack, S. (2009). Esperando una respuesta: El desordenado proceso de buscar la verdad. trad. Edison Otero B. *Ciencia, Sociedad y Cultura*, Ensayos Escogidos. Universidad Diego Portales. *Republicado en Cuadernos de neuropsicología*, (3), 12-23.

-Haack, S. (2015). The Expert Witness: Lessons from the U.S. Experience. *Humana Mente: Journal of Philosophical Studies, (28),* 39-70.

-Lanzón, R (2023). La búsqueda de evidencias en los dispositivos de almacenamiento digital. Alcances y límites al análisis forense en el marco del procedimiento penal. *Revista de Derecho Penal y Criminología, (2),* 107-125.

- López, C. (2019). Evidencias electrónicas. TFM. *Máster Universitario en Seguridad de las Tecnologías de la información y de las telecomunicaciones*. Universidad Oberta de Catalunya.

- Merkel, L. (2022). *Derechos Humanos e investigaciones policiales. Una tensión constante*. Marcial Pons.

- Moscatelli, L. (2023). La importancia de la abducción en la etapa de investigación criminal. *Quaestio Facti. Revista Internacional Sobre Razonamiento Probatorio*, (5), 125–155.

-Nieva Fenoll, J (2021). La decadencia del sistema penal acusatorio. *Revista Vasca de Derecho Procesal y Arbitraje, (*33), 489-500.

-NRC. (2009). Strengthening forensic Science in the United Stated: A Path Forward.

-Protocolo de Actuación para la Investigación Científica del lugar del hecho (2021). Ministerio de Seguridad de la República Argentina.

-Protocolo para la identificación, recolección, preservación, procesamiento y presentación de evidencia digital (2023). Ministerio de Seguridad de la República Argentina.

-Reedy, P. (2020). Interpol review of digital evidence 2016 - 2019. *Forensic Science International: Synergy*, (2), 489-520.

- Roatta, S; Casco, M; Flogisto, G. (2015). El tratamiento de la evidencia digital y las normas ISO/IEC 27037:2012. *IV Workshop de Seguridad Informática (WSI). XXI Congreso Argentino de Ciencias de la Computación.* Junín.

-Semprini, G. (2017). El análisis integral de la evidencia digital. *Simposio Argentino de Informática y Derecho*. Río Negro.

- Stelly, C; Roussev, V. (2018). Nugget: A digital forensics language. *Digital Investigation*, (24), 38-47.

-Suarez, M (2021). Vulneración de las Garantías Constitucionales en la Investigación en entornos digitales. *Revista Pensamiento Penal*, (401), 1-30.

- Sunde, N. (2021). What does a digital forensics opinion look like? A comparative study of digital forensics and forensic science reporting practices. *Science & Justice*, (61), 586–596.

-Tuzet, G. (2021). *Filosofía de la prueba jurídica*. Traducción de Diego Dei Vecchi. Marcial Pons.

-Unión Internacional de Telecomunicaciones (2012). Descripción General de Internet de los Objetos.

- Vázquez, C. (2015). La admisibilidad de las pruebas periciales y la racionalidad de las decisiones judiciales. *DOXA, Cuadernos de Filosofía del Derecho*, (38), 101-130.

-Vázquez, C. (2023). Guía sobre el contenido de los informes periciales. Y su impacto en el debido proceso. Escuela Federal de Formación Judicial, Consejo de la Judicatura Federal.

- Wilson -Kovacs, D; Helm, R; Growns, B; Redfern, L. (2023). Digital evidence in defence practice: Prevalence, challenges and expertise. *The International Journal of Evidence & Proof. (23)*, 235-253.