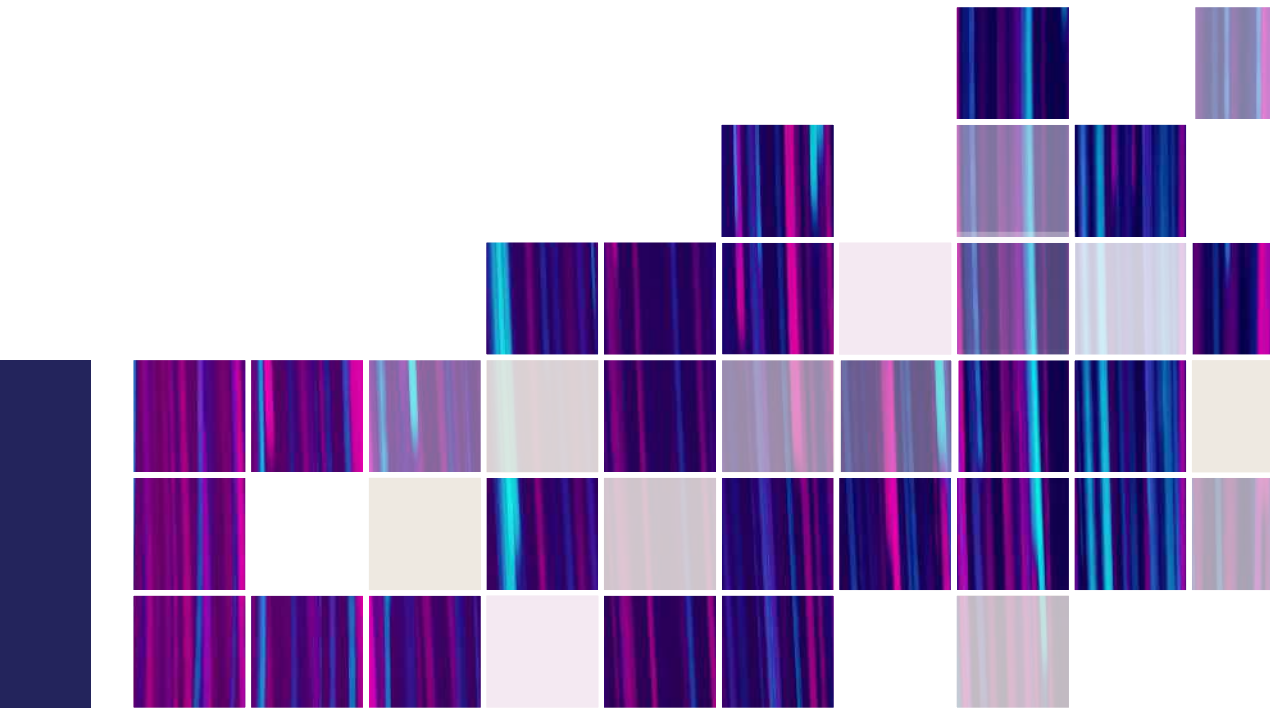
TEMAS

Kit avanzado para la obtención y práctica de la prueba digital

Joaquín Delgado Martín



LA LEY

ÍNDICE SISTEMÁTICO

CAPÍTULO 1

TEORÍA GENERAL DE LA PRUEBA DIGITAL

1. ¿QUÉ ES LA PRUEBA DIGITAL?
   - 1.1. Concepción amplia: evidencia electrónica
   - 1.2. Concepción estricta: prueba digital en el proceso judicial
2. ¿CUÁLES SON LAS FASES DE LA PRUEBA DIGITAL?
3. MODALIDADES DE EVIDENCIAS ELECTRÓNICAS
   - 3.1. Datos de dispositivos electrónicos
   - 3.2. Datos de comunicaciones
   - 3.3. Especial referencia a los datos almacenados por proveedores de servicios
   - 3.4. Datos relativos a dirección IP
4. OBTENCIÓN DE EVIDENCIAS DIGITALES EN FUENTES ABIERTAS
   - 4.1. ¿Qué son las fuentes abiertas?
   - 4.2. Principales modalidades
   - 4.3. Inteligencia en fuentes abiertas
   - 4.4. ¿Qué derechos fundamentales resultan afectados?

1. ¿QUÉ ES LA PRUEBA DIGITAL?

1.1. Concepción amplia: evidencia electrónica

1.1.1. Delimitación conceptual

Desde esta dimensión amplia, resulta equivalente a la llamada evidencia electrónica (e-evidence): es *toda información de valor probatorio contenida en un medio electrónico o transmitida por dicho medio*[1]. En esta definición cabe destacar los siguientes elementos:

1. Cualquier clase de información[2];

2. Producida, almacenada o transmitida por un medio electrónico, es decir, por cualquier mecanismo, instalación, equipo o sistema que permite producir, almacenar o transmitir documentos, datos e informaciones; incluyendo cualesquiera redes de comunicación abiertas o restringidas como Internet, telefonía fija y móvil u otras[3].

3. Y que pueda tener efectos para la investigación de actos ilícitos, para la acreditación de hechos en cualquier ámbito (en una negociación,

(1) Carolina SANCHÍS CRESPO, define prueba electrónica o en soporte electrónico como «aquella información contenida en un dispositivo electrónico a través del cual se adquiere el conocimiento de un hecho controvertido, bien mediante el convencimiento psicológico, bien al fijar este hecho como cierto atendiendo a una norma legal», en «La prueba en soporte electrónico», dentro de la obra colectiva Las Tecnologías de la Información y de la Comunicación en la Administración de Justicia. Análisis sistemático de la Ley 18/2011, de 5 de julio, editorial Thomson Reuters Aranzadi, Navarra, 2012, pág. 713.

(2) Se tiene en cuenta la concepción amplia que se contiene en el Convenio de Budapest sobre Ciberdelincuencia de 23 de noviembre de 2001 (Instrumento de Ratificación por España en BOE de 17 de septiembre de 2010) que define «datos informáticos» de la siguiente forma: «se entenderá toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función».

(3) Definición de medio electrónico contenida en el Anexo del RDL 6/2023.

en un procedimiento de acreditación…) y/o para acreditar hechos[4] en el proceso tramitado en cualquier orden jurisdiccional.

Según el Informe del Grupo de Regulación de AUTELSI 2025[5], los contextos relevantes para la extracción y presentación de la prueba digital (evidencias digitales) son los siguientes:

CONTEXTOS	EJEMPLOS
Auditorías internas y externas: Las empresas a menudo necesitan demostrar cumplimiento con normativas internas de gobierno, normativas financieras y de seguridad.	Auditorías de seguridad de la información.
Investigaciones de fraude y delitos financieros: Detección y análisis de actividades potencialmente sospechosas, ya sea dentro de la organización o en las interacciones con terceros vinculados a las relaciones comerciales.	Investigaciones de fraude contable.
Litigios laborales y disputas de empleo: Resolución de conflictos entre empleados y empleadores; y resolución de conflictos entre empresas y aliados comerciales.	Pruebas de correo electrónico para justificar despidos por causa.
Incidentes de seguridad informática: Investigación de violaciones de seguridad informática, revelación de datos, vulneraciones a los sistemas y ciberataques.	Análisis forense de malware y brechas de seguridad relativas a datos.
Cumplimiento normativo. Asegurar el cumplimiento con la normativa de protección de datos y normativa de inteligencia artificial.	Evidencia de consentimiento para el tratamiento de datos personales.
Formalización de contratos. Garantizar la ejecución de las obligaciones asumidas por las partes.	Evidencia de contrato firmado por las partes digitalmente.

1.1.2. Retos para la obtención de evidencias digitales

Los investigadores se encuentran con graves problemas para la obtención de las evidencias digitales. Y estos problemas adoptan características específicas cuando se trata del acceso por parte de un investigador privado.

(4) Afirma Lluís MUÑOZ SABATÉ, que «para la probática no hay en principio hechos civiles y hechos penales, sino simplemente, hechos», en «La prueba», forma parte del libro Curso superior de probática judicial. Cómo probar los hechos en el proceso, 1.ª edición, Editorial LA LEY, Madrid, septiembre 2013.

(5) Informe AUTELSI 2025 (Grupo Regulación), sobre «La protección jurídica en un entorno digital: obtención, custodia y presentación de la prueba», págs. 5 y 6.

Siguiendo un informe 2025 de la Comisión UE[6], las principales dificultades para acceder a las evidencias digitales son las siguientes:

Minimización por datos personales (**volatilidad**)	Eliminación por los proveedores de servicios en un plazo de días, de acuerdo con sus obligaciones de protección de datos personales y privacidad o sus necesidades comerciales.
Localización de datos en extranjero (**dimensión internacional**)	No se pueden obtener debido a conflictos de leyes entre jurisdicciones, ya que los diferentes países tienen leyes y regulaciones diferentes con respecto al acceso a los datos, lo que dificulta la obtención de datos almacenados en el extranjero.
Dificultades en el **análisis forense** de dispositivos	No pueden recuperarse de los dispositivos confiscados en investigaciones criminales porque la investigación forense digital es difícil, si no totalmente impracticable.
Encriptación de datos	No se puede leer porque los datos están encriptados.
Masividad de datos	No pueden analizarse de manera eficaz y legal debido a la falta de tecnologías adecuadas o de recursos humanos suficientes para filtrar y analizar eficazmente grandes cantidades de datos incautados sin afectar a los marcos jurídicos de la UE y de los Estados miembros.

Según un reciente informe de Eurojust y Europol sobre «Desafíos comunes en el cibercrimen»[7], un número cada vez mayor de investigaciones contiene grandes volúmenes de datos (terabytes o incluso petabytes de datos), lo que

(6) «Hoja de ruta para el acceso legal y efectivo a los datos para la aplicación de la ley», Comunicación de la Comisión de 24 de junio de 2025; COM(2025) 349 final.

(7) «Desafíos comunes en el cibercrimen», 2024, Review by Eurojust and Europol, 2025.

dificulta su almacenamiento, gestión y análisis efectivo sin contar con conocimientos avanzados, recursos computacionales y herramientas especializadas (**masividad**). Por otro lado, existe una **gran heterogeneidad de las formas** de los datos, desde datos estructurados como bases de datos SQL (Structured Query Language) hasta bases de datos no estructuradas y datos como correos electrónicos, publicaciones en redes sociales e imágenes. Asimismo, un porcentaje significativo y creciente de investigaciones sobre ciberdelincuencia implicaban el uso de alguna forma de cifrado para ocultar datos relevantes y pruebas de comunicaciones (**encriptación**).

1.1.3. Clases de datos

Datos de acceso público	Datos que se encuentran en el dominio público y que están disponibles para cualquier persona que tiene acceso a internet, sin que dicho acceso suponga ninguna afectación a derechos fundamentales.	• Información obtenida en fuentes abiertas. • Inteligencia sobre datos de fuentes abiertas (OSINT).
Datos de acceso no público	Datos que no se encuentran en el dominio público, de tal manera que su acceso afecta a derechos fundamentales. Existen tres categorías básicas.	• Datos de comunicaciones. • Datos de dispositivos electrónicos. • Datos obtenidos por medios propios del investigador (mediante instrumentos de geolocalización, o de grabación de audio y/o video).

1.2. Concepción estricta: prueba digital en el proceso judicial

Cabe recordar que la prueba es la actividad de acreditación de la realidad de un hecho afirmado por las partes y que resulta relevante para el objeto del proceso[8]. Esta actividad probatoria tiene como objetivo que el Juez perciba por sus sentidos la información sobre ese hecho que es proporcionada

(8) Afirma Francesco CARNELUTTI, que «el uso de la palabra prueba se limita a los procedimientos instituidos por el juez para la comprobación de los hechos controvertidos», en La prueba civil, Ediciones Depalma, Buenos Aires, 1982, pág. 43.

por personas (testimonios) o por cosas (documentos u otros objetos). Desde esta dimensión, resulta necesario delimitar diferentes conceptos[9]:

1. *Hecho digital*: es un hecho que tiene lugar de manera virtual (no de forma física)[10], especialmente en el ciberespacio a través de internet como, por ejemplo, un mensaje de odio en redes sociales, o un correo electrónico que informa del bloqueo de la tarjeta salvo que se haga clic en un enlace que conduce a un sitio web simulado del banco y que solicita determinados datos.

2. *Prueba del hecho digital*: es la acreditación en el proceso de un hecho digital, que plantea problemas relativos a su obtención (licitud), a su conservación (fiabilidad, que se refiere a las condiciones de autenticidad e integridad), y a la forma en que se lleva a juicio (admisibilidad procedimental). En este último sentido, es necesario tener presente que un hecho digital puede ser acreditado por distintos medios probatorios[11]: testifical de la víctima de ciberacoso, interrogatorio del acusado o interrogatorio de parte, pericial informática, incluso documental en soporte papel (impresión de mensajes de whatsapp o de mail…), documento electrónico (prueba digital en sentido estricto); y pueden utilizarse diversos medios probatorios de forma conjunta para probar un hecho digital.

3. *Prueba digital* en sentido estricto: *es la aportación de la prueba al proceso en formato digital (documento electrónico)*. Esta prueba sirve para acreditar un hecho digital; pero también para probar hechos «físicos» pero que se recogen en un elemento probatorio en formato digital, como puede ocurrir con la grabación con las cámaras de videovigilancia de la empresa, o la grabación en audio de una conversación por parte de un progenitor que lo aporta a un proceso de divorcio. Se encuentra plenamente admitida como prueba en el proceso español. Así se deduce del artículo 46 Reglamento (UE) 910/2014 (Reglamento eIDAS), de aplicación directa y general a todas las materias; y del artículo 24.2 Ley 34/2002 de servicios de la sociedad de la información y comercio electrónico (LSSI) para la contratación electrónica. Plantea las siguientes preguntas: ¿cómo se lleva al proceso? ¿cómo se valora por el Juez? ¿qué reglas de

(9) Véase mi trabajo sobre «Problemas actuales de la práctica y valoración de la prueba digital. Y un epílogo para abogados», La Ley Probática, N.º 6, 2021.

(10) Joan PICÓ I JUNOY, «Retos del derecho probatorio ante las nuevas tecnologías», Estudios. Inteligencia artificial legal y administración de justicia, Editorial Aranzadi, S.A.U., enero de 2022.

(11) Joan PICÓ I JUNOY, considera que «los medios tradicionales de prueba todavía sirven para aportar al proceso las nuevas fuentes probatorias digitales que aparecen en las redes sociales, en la contratación electrónica, o en mundo de IoT»; en «Retos del derecho probatorio…», obra citada.

carga de la prueba existen? La contestación a estas preguntas está vinculada, de tal manera que la forma de aportación puede determinar diferentes reglas de valoración y de distribución de la carga de la prueba:

3.1. *Fuente de prueba digital*: hecho exterior que sirve para probar el hecho objeto de la prueba; en este caso, es todo hecho (contenido o información) que se encuentre en formato electrónico o digital. Siguiendo a PICÓ i JUNOY[12], las tecnologías están aportando nuevas fuentes de prueba que se encuentran especialmente en cuatro ámbitos de la sociedad: en la forma de relacionarse las personas, mediante el uso continuo de las redes sociales; en la contratación electrónica, especialmente con el desarrollo vertiginoso de grandes empresas multinacionales dedicadas al comercio electrónico de cualquier tipo de producto o servicio; en la interconexión directa de los instrumentos electrónicos habituales en la vida de los ciudadanos a través de internet, esto es, internet de las cosas (IoT); y en la forma de comunicarse las personas, sustituyendo las palabras por símbolos o figuras (emojis o emoticons)[13].

3.2. *Medio de prueba digital*: es la percepción por el juez de fuentes en formato digital (documento electrónico); es decir, cómo se percibe por el juez el contenido (información o datos) producido, almacenado o transmitido por medios electrónicos (formato digital).

4. *Documento electrónico*. El artículo 3.35 del Reglamento (UE) 910/2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, lo define como «*todo contenido almacenado en formato electrónico, en particular, texto o registro sonoro, visual o audiovisual*». El documento electrónico tiene *pleno valor jurídico*, porque «*no se denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales a un documento electrónico por el mero hecho de estar en formato electrónico*» (artículo 46 Reglamento UE 910/2014). De esta manera, puede ser aportado al juicio como prueba de hechos.

(12) Joan PICÓ I JUNOY, «Retos del derecho probatorio...», obra citada.

(13) Algunos autores niegan la naturaleza de medio probatorio a la prueba digital, afirmando que se trata de una fuente de prueba. En ese sentido, Julio SIGÜENZA LÓPEZ, afirma que «cuando se habla de prueba digital o electrónica, en realidad se está haciendo referencia a una fuente de prueba, no a uno de los concretos medios regulados en la ley para incorporar a un proceso una realidad anterior a éste y poder valorarla en él. En el caso que nos ocupa, dicha fuente de prueba son los instrumentos electrónicos y digitales en los que se contiene determinada información que puede ser relevante para la resolución del conflicto suscitado ante la jurisdicción. O, si se prefiere, dichos instrumentos electrónicos y digitales y la información que en ellos se contiene; en "Tres problemas que suscita la llamada «prueba electrónica»: la obtención de la información, su incorporación o aportación a una causa civil y su posterior valoración"», Revista Aranzadi Doctrinal n.º 4/2021.

PRUEBA	PRUEBA DIGITAL
Objeto de la prueba: datos afirmados por cada parte para fundamentar su pretensión (hechos).	Datos en formato digital afirmados por cada parte para fundamentar su pretensión (evidencias electrónicas). Pueden referirse a: • hechos en ciberespacio; o • hechos en mundo «físico» recogidos mediante dispositivo digital.
Fuente de la prueba: ¿dónde se encuentran esos datos?	1. Datos generados en entornos virtuales: a) Datos en dispositivos electrónicos (acceso mediante registro); b) Datos en poder de prestadores de servicios-PSSI (acceso mediante solicitud); c) Datos en Internet (acceso online mediante web o aplicaciones); 2. Datos recogidos por dispositivos digitales del investigador (sin intervención PSSI): tecnovigilancia: a) Datos de localización (acceso mediante balizas o similares). b) Datos de audio y/o video (acceso mediante micrófonos o cámaras).
Medios probatorios: forma en que esos datos son percibidos por el juez.	El juez lee, visualiza y/o escucha el texto, audio, imagen o video mediante la utilización de un dispositivo digital usado para el acceso al documento electrónico.
Valoración de la prueba: el juez aplica reglas de la experiencia a lo percibido, otorgando o no eficacia probatoria.	El juez aplica reglas para evaluar la licitud (respeto derechos fundamentales) y fiabilidad (autenticidad e integridad de los datos digitales).

2. ¿CUÁLES SON LAS FASES DE LA PRUEBA DIGITAL?

En cualquier orden jurisdiccional, la prueba electrónica o digital atraviesa por las siguientes fases:

A) La primera fase consiste en la *obtención de los datos o información* producidos, almacenados o transmitidos, mediante el acceso a las fuentes de la prueba electrónica o digital antes de su incorporación al proceso; recordemos la gran heterogeneidad de estas fuentes. En esta fase, las par-

tes (o la autoridad pública en el ámbito penal) han de acceder a la información o datos de forma lícita, es decir, sin violación de derechos fundamentales.

B) La segunda fase radica en la *incorporación al proceso* de la información o datos obtenidos que sean relevantes para la acreditación de hechos. De esta manera, cabe hablar de tres tipos de requisitos aplicables en esta fase:

– Por un lado, la *pertinencia y la necesidad*, que resulta aplicable en cualquier jurisdicción y con independencia de la normativa procesal aplicable;

– Por otra parte, la *licitud*, entendida como el respeto a los derechos fundamentales durante la práctica del concreto medio probatorio;

– Por último, el cumplimiento de los requisitos exigidos por las leyes procesales[14], es decir, que la prueba acceda al proceso de conformidad con los requisitos exigidos por la normativa procesal del correspondiente orden jurisdiccional (civil, penal, laboral o contencioso-administrativo). En definitiva, ha de ser respetado el procedimiento probatorio contemplado por la respectiva legislación procesal para ejercitar válidamente el derecho a la prueba: es lo que denominamos *admisibilidad procedimental*.

C) La tercera fase consiste en la *valoración de la información o datos* por el Juez o Tribunal de enjuiciamiento. Si se cumplen los requisitos sobre obtención y práctica examinados en las dos fases anteriores, la prueba electrónica aportada o incorporada al proceso puede desplegar eficacia probatoria, siendo objeto de valoración por parte del Juez o Tribunal.

3. MODALIDADES DE EVIDENCIAS ELECTRÓNICAS

3.1. Datos de dispositivos electrónicos

A efectos de la investigación y prueba de hechos ilícitos, es posible establecer tres criterios relevantes: en primer lugar, en función de la modalidad de dispositivo electrónico accedido; en segundo término, por el estado de los datos; y, en tercer lugar, por la forma de acceso.

(14) Véase el último inciso del art. 230.2 de la Ley Orgánica del Poder Judicial.

1.1. Tipo de dispositivo electrónico	1.2. Estado de los datos	1.3. Forma de acceso
Ordenadores	Activos	Registro de dispositivos aprehendidos
Dispositivos móviles	Borrados	Registro remoto
Internet de las cosas (IoT)	Residuales o latentes	
Servidores	Ocultos	
Medios de almacenamiento		
Dispositivos de red		

3.1.1. Según el tipo de dispositivo electrónico

Resulta relevante porque cada modalidad de dispositivo almacena y organiza la información de forma distinta, lo que condiciona tanto la obtención como el análisis de datos, de tal manera que cada tipo de dispositivo requiere herramientas y procedimientos específicos para preservar la cadena de custodia y garantizar la autenticidad e integridad de la prueba (por ejemplo, Cellebrite para móviles, FTK/EnCase para ordenadores, Wireshark para dispositivos de red, Volatility para RAM).

A. Ordenadores, tanto de sobremesa y como portátiles (Windows, macOS, Linux):

- Archivos de usuario y de sistema.
- Metadatos de documentos.
- Historial de navegación y cookies.
- Registros de sistema (event logs, syslogs).
- Datos de aplicaciones de oficina, correo electrónico, mensajería.

B. Dispositivos móviles, tanto smartphones como tablets (Android, iOS)

- Listado de llamadas, SMS/MMS.
- Chats de mensajería instantánea (WhatsApp, Telegram, Signal).
- Fotos, vídeos y metadatos EXIF.
- Geolocalización y rutas.
- Aplicaciones instaladas y sus bases de datos internas.

C. Dispositivos IoT (Internet de las cosas): Cámaras IP, asistentes virtuales, electrodomésticos inteligentes, wearables

- Logs de actividad.
- Datos de sensores (temperatura, movimiento, GPS).
- Registros de conexión y autenticación.
- Capturas de vídeo o audio.

D. Servidores

- Archivos de configuración y logs del sistema.
- Registros de acceso remoto (SSH, RDP).
- Bases de datos corporativas.
- Volcados de memoria para análisis de procesos.

E. Medios de almacenamiento (HDD, SSD, USB, tarjetas SD, discos ópticos…)

- Imágenes forenses completas (bit a bit).
- Archivos activos y borrados.
- Particiones ocultas o cifradas.

F. Dispositivos de red (Routers, switches, firewalls, puntos de acceso Wi-Fi…)

- Logs de tráfico.
- Tablas ARP y rutas.
- Configuración de seguridad.
- Capturas de paquetes (PCAP).

3.1.2. Según el estado de los datos

A. Datos activos. Información accesible directamente desde el sistema operativo o las aplicaciones (archivos, fotos, correos, bases de datos, documentos de usuario).

B. Datos borrados. Información que ha sido eliminada pero aún puede recuperarse mediante técnicas forenses (sectores no sobrescritos, papelera de reciclaje vaciada).

C. Datos residuales o latentes. Fragmentos de información parcial o incompleta, como restos en áreas no asignadas o en memoria RAM.

D. Datos ocultos. Almacenados intencionadamente para evadir detección (volúmenes cifrados, esteganografía, archivos con extensiones engañosas).

3.1.3. Según la forma de acceso

A. Registro de dispositivos aprehendidos

Cuando el investigador tiene legítimamente en su poder un dispositivo electrónico relevante para la investigación, ya sea porque se ha obtenido por medios de investigación diversos, ya sea porque se ha entrega voluntariamente por su titular.

B. Registro remoto

Se trata del acceso en tiempo real de la actividad de un dispositivo electrónico. Se lleva a cabo mediante la instalación de software, que permite de forma remota y telemática, el examen a distancia y sin conocimiento de su titular o usuario del contenido de un ordenador, dispositivo electrónico, sistema informático, instrumento de almacenamiento masivo de datos informáticos o base de datos. El método de instalación de un programa de vigilancia en un dispositivo electrónico es distinto en cada caso.

Como afectan gravemente a los derechos fundamentales del titular de dispositivo, su régimen de acceso es mucho más severo, estando siempre sometido a autorización y control judicial.

3.2. Datos de comunicaciones

Desde el punto de vista de la investigación y prueba del delito, podemos establecer dos criterios relevantes: en primer lugar, en función de los derechos fundamentales afectados; y, en segundo término, por el régimen jurídico que regula la obtención del dato (acceso) por parte de los órganos del sistema penal.

2.1. POR LOS EFECTOS DERECHOS FUNDAMENTALES	2.2. POR EL RÉGIMEN DE OBTENCIÓN DEL DATO
2.1.1. Datos de suscripción	2.2.1. Datos obtenidos en tiempo real
2.1.2. Datos de acceso	2.2.2. Datos almacenados
2.1.3. Datos transaccionales	
2.1.4. Datos de contenido	

Esta obra ofrece a los profesionales del Derecho aquellas herramientas (kit) necesarias para afrontar los complejos problemas que surgen en la obtención y práctica de la prueba digital en las diferentes jurisdicciones.

¿Cómo se obtiene la prueba digital sin infracción de los derechos fundamentales? ¿Qué consecuencias tiene la prueba digital ilícita? ¿Cómo se presenta una prueba digital al juzgado o tribunal? ¿Cómo se garantiza su fiabilidad (autenticidad e integridad)? ¿Cómo valora el juez la prueba digital? ¿Qué efectos tiene el RDL 6/2023 sobre eficiencia digital? ¿Cómo se obtiene la prueba digital internacional y qué efectos tiene en el proceso tramitado en nuestro Estado? ¿Cómo impacta la Inteligencia Artificial en la prueba digital? ¿Cómo se pueden obtener lícitamente pruebas en Redes Sociales y plataformas digitales? ¿Cuáles son las novedades del Derecho de la UE que afectan a la prueba digital?

ISBN: 978-84-10292-95-6

LA LEY