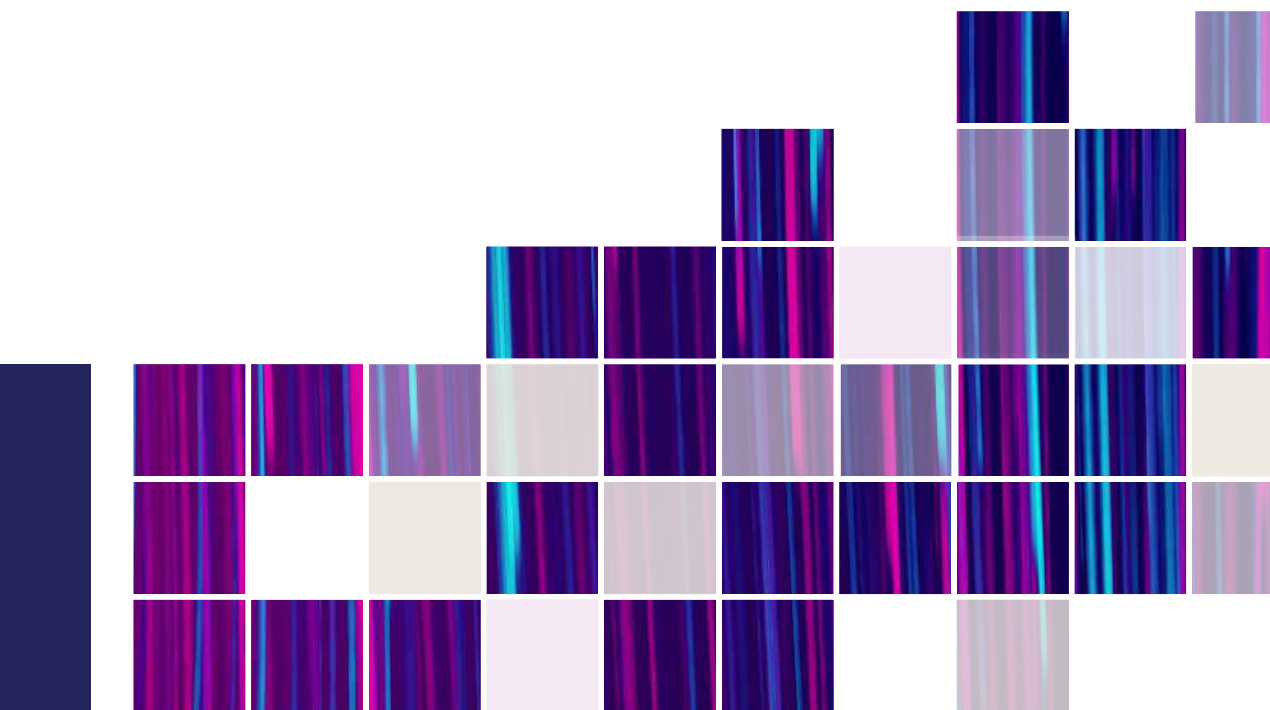


TEMAS

Kit avanzado para la obtención y práctica de la prueba digital

Joaquín Delgado Martín



III LA LEY

ÍNDICE SISTEMÁTICO

CAPÍTULO 1. TEORÍA GENERAL DE LA PRUEBA DIGITAL . . .	23
1. ¿QUÉ ES LA PRUEBA DIGITAL?	25
1.1. Concepción amplia: evidencia electrónica	25
1.1.1. Delimitación conceptual	25
1.1.2. Retos para la obtención de evidencias digitales	26
1.1.3. Clases de datos	28
1.2. Concepción estricta: prueba digital en el proceso judicial	28
2. ¿CUÁLES SON LAS FASES DE LA PRUEBA DIGITAL?	31
3. MODALIDADES DE EVIDENCIAS ELECTRÓNICAS	32
3.1. Datos de dispositivos electrónicos	32
3.1.1. Según el tipo de dispositivo electrónico	33
3.1.2. Según el estado de los datos	34
3.1.3. Según la forma de acceso	35
A. Registro de dispositivos aprehendidos	35
B. Registro remoto	35
3.2. Datos de comunicaciones.	35
3.2.1. Clases de datos por los derechos fundamentales afectados.	36
A. Datos de los abonados	36
B. Datos relativos al acceso	36
C. Datos de transacciones	37
D. Datos de contenido	37

3.2.2.	Clases de datos por el régimen jurídico de obtención	37
A.	Obtención de datos en tiempo real	37
B.	Acceso a datos conservados por los proveedores	38
3.3.	Especial referencia a los datos almacenados por proveedores de servicios	39
3.3.1.	Concepto y clases de proveedores de servicios	39
3.3.2.	Régimen jurídico de acceso a los datos	39
3.4.	Datos relativos a dirección IP	42
3.4.1.	Concepto	42
3.4.2.	Valor para la investigación y prueba de los delitos	43
3.4.3.	Dificultades en la investigación	43
3.4.4.	Régimen jurídico de la obtención de direcciones IP	44
4.	OBTENCIÓN DE EVIDENCIAS DIGITALES EN FUENTES ABIERTAS	47
4.1.	¿Qué son las fuentes abiertas?	47
4.2.	Principales modalidades	48
4.2.1.	Redes Sociales	48
4.2.2.	Motores de búsqueda	48
4.2.3.	Páginas y sitios web	49
A.	Concepto y notas características	49
B.	Derechos fundamentales afectados en el acceso a una página web	50
C.	Prueba de una página web	51
4.2.4.	Datos de personas físicas y de entidades	51
4.2.5.	Identificación de propietarios de nombres de dominio	52
4.2.6.	Rastreos informáticos en redes P2P	53
4.2.7.	Deep web y Dark web	54
4.3.	Inteligencia en fuentes abiertas	55
4.3.1.	Concepto y fases	55

4.3.2.	Valoración de la OSINT	57
4.4.	¿Qué derechos fundamentales resultan afectados? . . .	
4.4.1.	Principio general	
4.4.2.	Canal cerrado de comunicación: secreto de comunicaciones	
CAPÍTULO 2.	PRUEBA DIGITAL EN EL PROCESO CIVIL.	61
1.	RÉGIMEN COMÚN DE LA PRUEBA DIGITAL: LEY DE ENJUICIAMIENTO CIVIL	63
2.	¿CÓMO SE OBTIENE VÁLIDAMENTE LA PRUEBA DIGITAL?	63
2.1.	Obtención con respeto de los derechos fundamentales.	64
2.2.	¿Cómo acceder a las fuentes de la prueba digital? . . .	64
2.1.1.	Acceso a los datos. Información digital en poder de otro	65
2.1.2.	Diligencias preliminares	65
2.1.3.	Diligencias preliminares para la obtención de datos en propiedad intelectual o industrial . .	67
2.1.4.	Deber de exhibición documental	69
	A) Entre partes	69
	B) Por terceros	69
	C) Por entidades oficiales.	69
	D) Exhibición de las pruebas en procesos para el ejercicio de acciones por daños derivados de infracciones del Derecho de la competencia. Discovery	70
2.1.5.	Medidas de aseguramiento de la prueba . . .	71
2.1.6.	Medidas cautelares	71
2.1.7.	Art. 336.5 LEC.	72
3.	¿CÓMO SE APORTA LA PRUEBA DIGITAL AL PROCESO? EL PROCEDIMIENTO PROBATORIO	72
3.1.	El medio probatorio regulado en el art. 299.2 LEC . . .	72
3.2.	Procedimiento probatorio	74

3.2.1.	Sobre la presentación de documentos por medios electrónicos	74
3.2.2.	¿Cuál es el procedimiento probatorio de la prueba digital?	74
3.2.3.	Proposición	75
3.2.4.	Forma material de presentación	76
3.2.5.	Práctica	76
4.	¿CÓMO SE VALORA LA PRUEBA DIGITAL? VALORACIÓN JUDICIAL	77
4.1.	Regla general: libre valoración de la prueba electrónica	77
4.2.	Valoración de las distintas modalidades de documentos electrónicos.	79
4.3.	Valoración de los documentos electrónicos públicos .	80
4.3.1.	Documentos públicos	80
	A) ¿Cuáles son los documentos públicos? .	80
	B) ¿Qué es un documento público electrónico?	81
4.3.2.	¿Cuáles son las normas de valoración judicial de los documentos públicos electrónicos? . . .	81
4.3.3.	Impugnación, cotejo y gastos	82
	A) Impugnación	82
	B) Cotejo	83
	C) Costas, gastos y derechos derivados del cotejo o comprobación	83
4.3.4.	Documentos notariales	83
	A) Documento público notarial	84
	B) Copias electrónicas notariales	84
	C) Copia autorizada con la firma electrónica cualificada del Notario	85
	D) Copia simple electrónica	85
4.3.5.	Documentos registrales	86
4.3.6.	Documentos judiciales electrónicos	87
4.4.	Documentos oficiales	87
4.5.	Valoración de los documentos electrónicos privados .	87

4.5.1.	Consideraciones generales	87
4.5.2.	Caso específico: utilización de servicio de confianza	
A)	¿Qué son los servicios de confianza? . . .	
B)	¿Qué valor probatorio tiene un documento electrónico acreditado por un servicio electrónico de confianza?	
4.6.	Valoración de la postura procesal de las partes: impugnación	

CAPÍTULO 3. PRUEBA DIGITAL EN EL PROCESO PENAL 93

1.	¿CUÁLES SON LAS FUENTES DE LA PRUEBA DIGITAL? LAS EVIDENCIAS ELECTRÓNICAS.	95
1.1.	Datos generados en entornos virtuales	96
1.2.	Datos recogidos por dispositivos digitales utilizados por el investigador (tecnovigilancia)	96
2.	MEDIDAS DE INVESTIGACIÓN TECNOLÓGICA	97
3.	¿CÓMO SE PUEDE ACCEDER LÍCITAMENTE A LAS EVIDENCIAS ELECTRÓNICAS? PRINCIPIOS RECTORES	98
3.1.	Principio de especialidad	99
3.1.1.	¿Qué es el principio de especialidad?	99
3.1.2.	Concurrencia de indicios suficientes	100
3.1.3.	Ficha sobre la STS 141/2020 de 13 de mayo	101
A)	Resumen de los hechos	101
B)	Decisión del TS	102
3.2.	Principio de idoneidad	103
3.3.	Principios de excepcionalidad y necesidad	103
3.4.	Principio de proporcionalidad	104
3.4.1.	Dimensiones del principio de proporcionalidad	104
3.4.2.	Principio de proporcionalidad en sentido estricto	105
4.	¿CUÁL ES EL PROCEDIMIENTO DE ADOPCIÓN DE LAS MEDIDAS DE INVESTIGACIÓN TECNOLÓGICA?	107

4.1.	Inicio	107
4.2.	Audiencia del Ministerio Fiscal.....	108
4.3.	Decisión judicial	108
4.3.1.	Tiempo, forma y contenido	108
4.3.2.	Afectación de terceras personas	109
4.3.3.	Motivación	109
4.4.	Ejecución de la medida	111
4.4.1.	Pieza separada y secreta	111
4.4.2.	Duración.....	111
4.4.3.	Control judicial de la medida	112
	A) Auto autorizante	113
	B) Control durante la duración de la medida	113
	C) Control ex post por el órgano judicial sentenciador	113
4.4.4.	Utilización de la información en otro procedimiento distinto	114
4.4.5.	Hallazgos casuales	115
4.4.6.	Cese de la medida.....	120
4.4.7.	Destrucción de los registros.....	120
CAPÍTULO 4.	FIABILIDAD DE LA PRUEBA DIGITAL.....	121
1.	¿QUÉ ES LA FIABILIDAD EN RELACIÓN CON LA OBTENCIÓN Y CONSERVACIÓN DE LAS PRUEBAS DIGITALES? ..	123
1.1.	Digital forensics	123
1.2.	Principios aplicables al manejo de las evidencias digitales	124
1.3.	Fases relevantes para la fiabilidad de la prueba digital	125
1.3.1.	Identificación	125
1.3.2.	Recolección	126
1.3.3.	Preservación	127
1.3.4.	Análisis	127

2.	¿CUÁLES SON LOS REQUISITOS PARA LA FIABILIDAD DE LA PRUEBA DIGITAL?	127
2.1.	¿Qué es la autenticidad y qué es la integridad de la prueba digital?	127
2.1.1.	Autenticidad	128
2.1.2.	Integridad	128
2.1.3.	Regulación en la Ley de Enjuiciamiento Criminal.	128
2.1.4.	Garantías de autenticidad e integridad	129
2.2.	Sobre la cadena de custodia de las evidencias digitales.	130
2.2.1.	¿Qué es la cadena de custodia?	130
2.2.2.	¿Cuáles son las consecuencias procesales de la fractura de la cadena de custodia?	131
2.2.3.	Registro de la cadena de custodia en procedimientos internos de las entidades	131
2.3.	¿Cómo ha de realizarse el volcado o copia de los datos?	132
2.3.1.	Concepto	132
2.3.2.	Proceso penal	133

CAPÍTULO 5. PRUEBA DIGITAL ILÍCITA 137

1.	¿QUÉ ES LA PRUEBA ILÍCITA?	139
2.	¿QUÉ EFECTOS TIENE EN EL PROCESO?	140
2.1.	Principio general: nulidad de la prueba	140
2.2.	La nulidad no es automática: juicio de ponderación (doctrina Falciani).	142
2.2.1.	Caso «lista Falciani»	142
	A) Resumen de antecedentes	142
	B) STS 116/17, de 23 de febrero	143
	C) STC 97/19 de 16 de julio (Pleno).	143
2.2.2.	Doctrina vigente del Tribunal Constitucional	143
2.3.	Vulneración por particulares y vulneración por agentes públicos	148

2.3.1.	Eficacia vertical y eficacia horizontal de los derechos fundamentales	148
2.3.2.	Efectos de la violación de derecho fundamental por particular.	149
2.4.	Efectos sobre las pruebas derivadas	152
2.4.1.	Regla general: nulidad.	152
2.4.2.	Excepción: validez de las pruebas derivadas carentes de conexión de antijuridicidad	152
	A) Falta de conexión natural	152
	B) Falta de conexión de antijuridicidad	153
3.	¿CUÁL ES EL CAUCE PROCESAL DE LA NULIDAD?.	154
3.1.	En el proceso civil	154
3.2.	En el proceso penal	155
3.2.1.	Procedimiento abreviado, juicio rápido y proceso penal de menores.	155
3.2.2.	Proceso ante tribunal de jurado.	155
3.2.3.	Proceso ordinario por delito y juicio por delito leve.	156
CAPÍTULO 6. EL RETO PROBATORIO DE LAS PLATAFORMAS DIGITALES		157
1.	SOBRE LA RELEVANCIA DE LAS PLATAFORMAS DIGITALES	159
1.1.	¿Qué es una plataforma digital?	159
1.2.	¿Por qué es importante el papel de las plataformas digitales contra los actos ilícitos?	159
2.	¿CÓMO SE INVESTIGAN LOS ACTOS ILÍCITOS EN LAS REDES SOCIALES?.	160
2.1.	Contexto.	160
2.2.	¿Qué derechos fundamentales resultan afectados?	160
2.2.1.	Principio general: fuentes abiertas.	160
2.2.2.	Existencia de proceso de comunicación	161
	A) Acceso ilegítimo a la parte reservada	162

B) Uso de usuario/contraseña por persona legitimada	162
3. OBTENCIÓN DE INFORMACIÓN DE LOS SERVICIOS DE INTERMEDIACIÓN: DSA	163
3.1. ¿Cuándo responden por los contenidos los prestadores intermediarios?	164
3.2. Obligaciones de colaboración para la persecución de los contenidos ilícitos	165
3.3. ¿Qué prestadores de servicios resultan afectados por estas obligaciones?	166
3.4. Órdenes de entrega de información	167
3.4.1. Elementos de la orden	167
3.4.2. Contenido mínimo de la orden	168
3.4.3. Procedimiento	169
3.5. Notificación de sospechas de delitos	170
3.5.1. ¿En qué supuestos nace la obligación de notificar sospechas?	171
3.5.2. ¿Qué información se ha de remitir?	171
3.5.3. ¿A qué Estado debe notificarse la sospecha?	171
3.6. Colaboración voluntaria	172
3.6.1. ¿Cómo resultan afectados los derechos fundamentales?	173
3.6.2. ¿Qué modalidades de colaboración existen?	174
CAPÍTULO 7. IMPACTO DE LA INTELIGENCIA ARTIFICIAL EN LA PRUEBA DIGITAL	177
1. INTRODUCCIÓN	179
1.1. ¿Cómo afecta la Inteligencia Artificial a la prueba en el proceso?	179
1.2. Esquema general	181
2. IA PARA LA ALTERACIÓN DE LAS PRUEBAS	181
2.1. ¿Qué es una deepfake o ultrafalsificación?	181
2.2. ¿Cómo accede la deepfake al proceso?	183
2.3. ¿Cómo detectar una ultrafalsificación?	183

2.3.1.	Consejos o pistas para identificar el posible contenido falso generado con IA	183
2.3.2.	Herramientas técnicas útiles para identificar contenido falso generado por IA	184
2.3.3.	Herramientas técnicas avanzadas	185
2.4.	Efectos jurídicos de la aportación de deepfakes como pruebas.	185
2.5.	Conclusiones	186
3.	IA PARA GENERAR PRUEBAS.	187
3.1.	IA para mejorar la calidad de las pruebas: pruebas digitalmente mejoradas	187
3.2.	IA para generar pruebas a partir de simulaciones	188
 CAPÍTULO 8. LA PRUEBA DIGITAL INTERNACIONAL. COOPERACIÓN JUDICIAL CONTRA LA CIBERDELINCUENCIA		 189
1.	NECESIDAD DE LA COOPERACIÓN JUDICIAL INTERNACIONAL	191
1.1.	Desafíos para la persecución de los ciberdelitos. . . .	191
1.1.1.	Volatilidad. Peligro de pérdida de datos	191
1.1.2.	Complejidad técnica. Desafíos de las novedades tecnológicas	192
1.1.3.	Localización de los datos. Internacionalización.	193
1.2.	Complejidad de la prueba digital internacional	193
1.2.1.	Falta de un marco legal adecuado.	194
1.2.2.	Dificultades en la obtención de datos en poder de los proveedores de servicios.	195
2.	PREVENCIÓN Y SOLUCIÓN DE CONFLICTOS DE JURISDICCIÓN EN LA CIBERDELINCUENCIA.	196
2.1.	Prevención de conflictos.	196
2.2.	Solución de los conflictos de jurisdicción.	197
3.	LA PRUEBA DIGITAL INTERNACIONAL.	198
3.1.	Cooperación judicial Clásica	198
3.1.1.	Normativa.	198

3.1.2.	Fases de la cooperación judicial internacional.	199
3.2.	El convenio de Budapest.	200
3.2.1.	Asistencia mutua para medidas provisionales	200
3.2.2.	Asistencia mutua para remisión de datos. . . .	202
3.2.3.	Acceso transfronterizo a datos.	202
3.2.4.	Otras formas: obtención en tiempo real. . . .	203
3.2.5.	Supuestos de urgencia.	203
3.3.	Auxilio judicial para obtener prueba digital en la Unión Europea	203
3.3.1.	Conservación rápida de datos	204
3.3.2.	Remisión de los datos	205
	A) Emisión por órgano español	206
	B) Ejecución en España	208
4.	COOPERACIÓN JUDICIAL CON ESTADOS UNIDOS	212
4.1.	Tratado bilateral	212
4.1.1.	Preservación de datos	213
4.1.2.	Entrega de datos	215
4.1.3.	Entrega de datos en supuestos de urgencia . .	216
4.2.	Sistema Cloud Act	217
4.2.1.	EEUU como parte activa	217
4.2.2.	EEUU como parte pasiva.	217
5.	IBEROAMÉRICA: TRATADO DE MADRID	218
5.1.	Estado actual del convenio.	218
5.2.	Contenido.	219
6.	RECOMENDACIONES PARA MEJORAR LA OBTENCIÓN INTERNACIONAL DE DATOS	220
6.1.	Estrategia general	220
6.1.1.	Agotar fuentes abiertas y recursos internos . .	220
6.1.2.	Solicitud internacional alternativa a la Comisión Rogatoria formal	220
6.1.3.	Uso de la Asistencia Judicial Internacional . .	221
6.2.	Decálogo de recomendaciones para mejorar las solicitudes de cooperación judicial internacional.	221

6.3.	Acceso a datos abiertos al público	223
6.4.	Entrega voluntaria por el proveedor de servicios a requerimiento de la autoridad pública	223
7.	PANORAMA DE FUTURO	224
7.1.	Segundo Protocolo del Convenio de Budapest	225
7.2.	Nuevo sistema en la UE: sistema E-Evidence	227
7.3.	Sobre el Reglamento E-Evidence.	229
7.3.1.	Ámbito de aplicación	229
	A) ¿Cuál es el objeto?	229
	B) ¿Qué datos pueden ser objeto de una Orden?	229
7.3.2.	Emisión de la Orden	234
	A) ¿Qué autoridades pueden emitir las órdenes?	234
	B) ¿Cuál es la forma de emisión?	234
	C) ¿Cuál es la forma de remisión?	234
7.3.3.	Ejecución de la Orden.	235
	A) Orden de Conservación	235
	B) Orden de Producción:	235
8.	COOPERACIÓN POLICIAL INTERNACIONAL SOBRE EVIDENCIAS DIGITALES Y CONTRA LA CIBERDELINCUENCIA	236
8.1.	Canales de cooperación policial.	236
8.1.1.	Centro Europeo de Ciberdelincuencia (EC3)	237
8.1.2.	Red 24/7 del Convenio de Budapest	237
8.1.3.	Red 24/7 de Interpol	237
8.2.	Intercambio espontáneo de información.	238
8.3.	Valor probatorio de las evidencias digitales transmitidas por servicios policiales extranjeros	240

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
<i>Auditorías internas y externas:</i> Las empresas a menudo necesitan demostrar cumplimiento con normativas internas de gobierno, normativas financieras y de seguridad.	Auditorías de seguridad de la información.
<i>Investigaciones de fraude y delitos financieros:</i> 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.
<i>Litigios laborales y disputas de empleo:</i> 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.
<i>Incidentes de seguridad informática:</i> 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.
<i>Cumplimiento normativo.</i> Asegurar el cumplimiento con la normativa de protección de datos y normativa de inteligencia artificial.	Evidencia de consentimiento para el tratamiento de datos personales.
<i>Formalización de contratos.</i> 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
<i>Objeto de la prueba:</i> 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.
<i>Fuente de la prueba:</i> ¿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).
<i>Medios probatorios:</i> 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.
<i>Valoración de la prueba:</i> 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 entregado voluntariamente por su titular.

B. Registro remoto

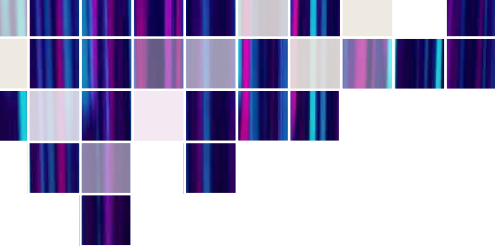
Se trata del acceso en tiempo real de la actividad de un dispositivo electrónico. Se lleva a cabo mediante la instalación de software, que permite de forma remota y telemática, el examen a distancia y sin conocimiento de su titular o usuario del contenido de un ordenador, dispositivo electrónico, sistema 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

