

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