

# ÍNDICE SISTEMÁTICO

## PARTE I

### EL PROCESO DIGITAL Y EL DERECHO PROCESAL DIGITAL

<b>CAPÍTULO 1. CARACTERIZACIÓN DEL PROCESO DIGITAL. . .</b>	<b>41</b>
1. EL DERECHO PROCESAL DIGITAL . . . . .	43
2. EL PROCESO DIGITAL. . . . .	44
2.1. Notas conceptuales. . . . .	44
2.2. Elementos del proceso digital . . . . .	48
2.3. Hacia un nuevo paradigma de proceso. . . . .	49
3. PROCESO DIGITAL Y ACCESO A LA JUSTICIA . . . . .	50
3.1. Beneficios del proceso digital para el acceso a la justicia . . . . .	50
3.2. El reto de combatir la brecha digital . . . . .	51
4. ACTOS PROCESALES ESCRITOS Y ACTOS PROCESALES ORALES . . . . .	54
5. NORMATIVA REGULADORA DEL PROCESO DIGITAL. . . . .	55
5.1. Ordenamiento español y de la Unión Europea . . . . .	55
5.2. Dualidad normativa procesal vs. normativa de efi- ciencia digital . . . . .	55
<b>CAPÍTULO 2. PRINCIPIOS DEL PROCESO DIGITAL . . . . .</b>	<b>59</b>
1. PRINCIPIOS OPERATIVOS Y PRINCIPIOS DEL PROCEDI- MIENTO. . . . .	61
2. PRINCIPIO TRANSVERSAL DE ORIENTACIÓN AL DATO. . .	61

2.1.	Dimensión procesal del principio de orientación al dato . . . . .	62
2.2.	Regulación en el RDL 6/23: Eficiencia Digital del Servicio Público de Justicia . . . . .	62
3.	PRINCIPIO DE RIGOR EN LA GESTIÓN DE RIESGOS . . . . .	64
3.1.	Sobre la seguridad de la información en el proceso. Ciberseguridad . . . . .	65
3.1.1.	Ciberseguridad judicial: medidas técnicas y medidas organizativas. . . . .	65
3.1.2.	Medidas de ciberseguridad judicial del RDL 6/23 . . . . .	67
3.1.2.1.	Política de seguridad de la información. . . . .	68
3.1.2.2.	Subcomité de Seguridad. . . . .	69
3.1.2.3.	Centro de Operaciones de Ciberseguridad de la Administración de Justicia. . . . .	69
3.1.3.	Seguridad de la información en la protección de datos personales . . . . .	70
3.2.	Régimen de protección de los datos personales . . . . .	72
4.	OTROS PRINCIPIOS . . . . .	72
4.1.	Principio de obligatoriedad de uso . . . . .	72
4.2.	Principio de preferencia digital en los actos procesales . . . . .	73
4.3.	Principio de interoperabilidad. . . . .	74
4.3.1.	Dimensiones de la interoperabilidad . . . . .	74
4.3.2.	Sistema Común de Intercambio . . . . .	75
4.4.	Principio de respeto de las leyes procesales . . . . .	76

## PARTE II

### SOBRE LA E-JUSTICIA

<b>CAPÍTULO 1. CONCEPTO Y ELEMENTOS DE LA E-JUSTICIA . .</b>	<b>79</b>
1. ¿QUÉ ES LA E-JUSTICIA? . . . . .	81

2.	ELEMENTOS DE LA E-JUSTICIA . . . . .	82
2.1.	Relación con los ciudadanos y profesionales . . . . .	83
2.2.	Interoperabilidad entre sistemas de información del sector justicia . . . . .	83
<b>CAPÍTULO 2. ACCESO DIGITAL A LA ADMINISTRACIÓN DE JUSTICIA . . . . .</b>		<b>85</b>
1.	INTRODUCCIÓN CONCEPTUAL . . . . .	87
2.	SEDES JUDICIALES ELECTRÓNICAS . . . . .	87
2.1.	¿Qué es y para qué sirve la sede judicial electrónica? . . . . .	87
2.2.	¿Cuál es su régimen jurídico? . . . . .	88
2.3.	¿Cuáles son las principales novedades de 2023? . . . . .	88
2.4.	¿Qué es el Punto de Acceso General de la Administración de Justicia? . . . . .	89
2.5.	¿Qué actos de trámite puede realizar una persona en la sede judicial electrónica? . . . . .	90
2.5.1.	Actos procesales de los ciudadanos . . . . .	91
2.5.2.	Actos procesales de comunicación . . . . .	92
2.5.3.	Otras actuaciones procesales . . . . .	93
3.	CARPETA JUSTICIA: ACCESO A LA INFORMACIÓN DE LA ADMINISTRACIÓN DE JUSTICIA. . . . .	94
3.1.	¿Qué es la Carpeta Justicia? . . . . .	94
3.2.	¿Cuál es su régimen jurídico? . . . . .	94
3.3.	¿Cuál es su contenido? . . . . .	95
3.3.1.	Acceso al expediente judicial electrónico. . . . .	95
3.3.2.	Acceso a notificaciones . . . . .	96
3.3.3.	Cita previa . . . . .	96
3.4.	Experiencia del Ministerio de Justicia . . . . .	96
<b>CAPÍTULO 3. ACTOS PROCESALES ESCRITOS EN EL PROCESO DIGITAL . . . . .</b>		<b>99</b>
1.	ACTOS DE COMUNICACIÓN POR MEDIOS ELECTRÓNICOS . . . . .	102

1.1.	Preferencia (obligación) por los medios electrónicos	102
1.2.	Forma de las comunicaciones electrónicas . . . . .	104
1.3.	Tiempo de las comunicaciones electrónicas . . . . .	104
1.3.1.	Principio de orientación al dato . . . . .	105
1.3.2.	Punto Común de Actos de Comunicación	105
1.3.3.	Excepciones a la notificación por medios electrónicos . . . . .	106
1.4.	Modalidades de las comunicaciones de actos procesales por medios electrónicos . . . . .	107
1.4.1.	Modalidades generales. . . . .	107
1.4.2.	Por sistema Lexnet o similar. . . . .	107
1.4.3.	Dirección electrónica habilitada . . . . .	108
1.4.4.	En la sede judicial electrónica . . . . .	109
1.4.5.	En la Carpeta Justicia . . . . .	109
1.4.6.	Formas específicas de comunicación . . . . .	110
1.4.6.1.	Comunicaciones masivas . . . . .	110
1.4.6.2.	Comunicación edictal electrónica . . . . .	110
1.4.6.3.	Comunicaciones transfronterizas . . . . .	111
2.	PRESENTACIÓN TELEMÁTICA DE ESCRITOS Y DOCUMENTOS . . . . .	112
2.1.	Modalidades de presentación de los documentos . . . . .	112
2.1.1.	Por medios electrónicos: preferencia por la presentación telemática . . . . .	112
2.1.2.	En soporte papel . . . . .	112
2.1.3.	Aportación de documentos en las actuaciones orales telemáticas . . . . .	113
2.2.	Ámbito subjetivo: sujetos obligados a la presentación por medios electrónicos . . . . .	114
2.2.1.	Requisitos de la presentación por medios electrónicos . . . . .	115

2.2.2.	Requisitos procesales de la presentación por medios electrónicos. . . . .	116
2.2.2.1.	Requisitos de contenido . . . . .	116
2.2.2.2.	Tiempo de presentación . . . . .	117
2.2.2.3.	Interrupción del servicio. . . . .	117
2.2.2.4.	Insuficiencia del servicio . . . . .	118
3.	OTORGAMIENTO ELECTRÓNICO DE REPRESENTACIÓN PROCESAL . . . . .	118
3.1.	Otorgamiento . . . . .	120
3.2.	Inscripción en el Registro Electrónico de Apoderamientos Judiciales . . . . .	120
3.3.	Acreditación de la representación procesal y efectos en el proceso. . . . .	122
4.	SUBASTAS ELECTRÓNICAS. . . . .	123
5.	CUENTA DE DEPÓSITOS Y CONSIGNACIONES JUDICIALES. . . . .	123

### PARTE III

## EL EXPEDIENTE JUDICIAL ELECTRÓNICO

<b>CAPÍTULO 1. EXPEDIENTE DIGITAL Y TRAMITACIÓN ELECTRÓNICA DEL PROCEDIMIENTO . . . . .</b>	<b>127</b>
1. ¿QUÉ ES EL EXPEDIENTE JUDICIAL ELECTRÓNICO?. . . . .	129
1.1. Concepto y dimensiones. . . . .	129
1.2. La dimensión estática del expediente judicial electrónico: concepto y componentes. . . . .	130
1.3. La dimensión dinámica: tramitación electrónica del proceso judicial . . . . .	131
1.4. Obligatoriedad de uso. . . . .	132
1.5. Otros requisitos de la tramitación electrónica de los procedimientos. . . . .	133
1.6. Problemas y posibles soluciones . . . . .	134

<b>CAPÍTULO 2. DOCUMENTOS JUDICIALES ELECTRÓNICOS ..</b>	<b>135</b>
1. CONCEPTO, VALOR JURÍDICO Y MODALIDADES DEL DOCUMENTO ELECTRÓNICO .....	137
2. CONCEPTO Y COMPONENTES DEL DOCUMENTO JUDICIAL ELECTRÓNICO .....	138
3. MODALIDADES Y EFECTOS JURÍDICOS DE LOS DOCUMENTOS JUDICIALES ELECTRÓNICOS .....	139
3.1. Documento electrónico generado / incorporado al proceso .....	139
3.2. Documentos judiciales electrónicos públicos / privados .....	139
3.3. Documento electrónico original / copias electrónicas .....	139
3.4. Comprobación de la autenticidad e integridad ....	141
3.5. Prohibición del formato papel .....	142

#### **PARTE IV**

#### **PRUEBA DIGITAL EN EL PROCESO CIVIL**

<b>CAPÍTULO 1. INTRODUCCIÓN .....</b>	<b>145</b>
1. DELIMITACIÓN CONCEPTUAL .....	147
2. ESTÁNDARES PROBATORIOS: EFICACIA PROBATORIA DE LA PRUEBA DIGITAL .....	149
<b>CAPÍTULO 2. FASES DE LA PRUEBA DIGITAL .....</b>	<b>151</b>
1. FASE DE OBTENCIÓN DE LA PRUEBA .....	153
1.1. Dificultades de acceso a la prueba digital en el proceso civil .....	154
1.2. Licitud en la obtención .....	155
1.3. Fiabilidad .....	155
1.3.1. Autenticidad .....	156

1.3.2.	Integridad . . . . .	156
1.3.3.	Garantías de autenticidad e integridad . . .	157
2.	FASE DE APORTACIÓN AL PROCESO. . . . .	157
2.1.	Proposición. . . . .	159
2.2.	Práctica. . . . .	160
3.	FASE DE VALORACIÓN JUDICIAL . . . . .	161
3.1.	Regla general: libre valoración de la prueba electrónica. . . . .	161
3.2.	Valoración de las distintas modalidades de documentos electrónicos . . . . .	163
3.2.1.	Valoración de los documentos electrónicos públicos. . . . .	163
3.2.2.	Valoración de los documentos electrónicos privados. . . . .	166
3.2.3.	Caso específico: utilización de servicio de confianza. . . . .	166
3.2.3.1.	¿Qué son los servicios de confianza? . . . . .	166
3.2.3.2.	¿Qué valor probatorio tiene un documento electrónico acreditado por un servicio electrónico de confianza? . . . . .	167
3.3.	Valoración de la postura procesal de las partes: impugnación. . . . .	167
<b>CAPÍTULO 3. CARGA DE LA PRUEBA DIGITAL . . . . .</b>		<b>171</b>
1.	SOBRE LA CARGA DE LA PRUEBA . . . . .	173
2.	REGLAS DE INVERSIÓN DIRECTA DE LA CARGA DE LA PRUEBA DIGITAL . . . . .	174
2.1.	Previstas en norma legal expresa. . . . .	174
2.1.1.	Faltas de conformidad en los contratos de compraventa de elementos digitales con consumidores. . . . .	174
2.1.2.	Entrega de bienes y suministro de contenidos o servicios digitales que no se presten en soporte material . . . . .	175

2.1.3.	Contratos bancarios electrónicos . . . . .	177
2.1.4.	Otros supuestos . . . . .	178
2.2.	Principio de disponibilidad y de facilidad probatoria . . . . .	178
2.3.	Sobre la contratación electrónica . . . . .	180
2.3.1.	Concepto y modalidades . . . . .	180
2.3.2.	Prueba de la contratación electrónica . . . . .	182
3.	REGLAS DE INVERSIÓN INDIRECTA DE LA CARGA DE LA PRUEBA DIGITAL . . . . .	184
3.1.	Documento electrónico con utilización de servicio de confianza cualificado . . . . .	184
3.2.	Documento con firma electrónica . . . . .	185
3.2.1.	Concepto y modalidades de la firma electrónica . . . . .	185
3.2.2.	Valor probatorio de los documentos con firma electrónica . . . . .	188
3.3.	Otras presunciones recogidas en el Reglamento eIDAS . . . . .	190
3.3.1.	Esquema general . . . . .	190
3.3.2.	Eficacia probatoria de documentos electrónicos en otros Estados de la UE . . . . .	191
 <b>CAPÍTULO 4. PROTOCOLO DE ACTUACIÓN JUDICIAL EN PRUEBA DIGITAL . . . . .</b>		 193

**PARTE V**

**CONFIANZA DIGITAL Y SISTEMA DE JUSTICIA**

<b>CAPÍTULO 1. IDENTIFICACIÓN DIGITAL, FIRMA ELECTRÓNICA Y DOCUMENTOS ELECTRÓNICOS . . . . .</b>		<b>201</b>
1.	SOBRE EL REGLAMENTO UE 910/14 (EIDAS) . . . . .	203
2.	IDENTIFICACIÓN ELECTRÓNICA . . . . .	204
2.1.	¿Qué es y para qué sirve la identificación digital? . . . . .	204
2.2.	¿Cómo se realiza la identificación digital? . . . . .	205

2.3.	Valoración del sistema actual: hacia el eIDAS 2 . . .	208
2.4.	Identificación electrónica en la Unión Europea: sistema del Reglamento eIDAS 2014. . . . .	209
2.5.	Identificación electrónica en las relaciones con la Administración pública española . . . . .	211
3.	SERVICIOS DE CERTIFICACIÓN ELECTRÓNICA . . . . .	213
3.1.	¿Qué son y para qué sirven? . . . . .	213
3.2.	Sistema de certificación electrónica en la Unión Europea . . . . .	215
3.2.1.	Modalidades de servicios de certificación	215
3.2.2.	Prestadores de servicios de confianza . . .	215
4.	SOBRE LA FIRMA ELECTRÓNICA EN EL SISTEMA EIDAS . .	217
4.1.	¿Cuál es el régimen jurídico de la firma electrónica y qué modalidades existen?. . . . .	217
4.2.	Modalidades de la firma electrónica y sus efectos probatorios . . . . .	217
5.	MODIFICACIÓN DEL REGLAMENTO EIDAS EN 2024 . . . .	217
5.1.	La identificación electrónica tras la modificación del Reglamento (eIDAS 2). . . . .	219
5.1.1.	Conceptos fundamentales . . . . .	220
5.1.2.	Principios de la Identidad Auto-soberana.	221
5.1.3.	Elementos del sistema de identificación tras la reforma de 2024 . . . . .	222
5.2.	Servicio de libro mayor electrónico. . . . .	223
5.2.1.	¿Qué son las DLT (Distributed Ledger Technology) o Tecnología Libro Mayor Distribuido? . . . . .	223
5.2.2.	¿Qué es y para qué sirve el servicio de libro mayor electrónico? . . . . .	224
5.2.3.	¿Cuáles son sus efectos jurídicos?. . . . .	225
5.3.	Servicio de declaración electrónica de atributos . .	226
5.3.1	¿Qué es y para qué sirve?. . . . .	226
5.3.2.	¿Qué requisitos que debe cumplir la declaración cualificada de atributos? . . . . .	227

5.3.3.	¿Qué requisitos debe cumplir una declaración electrónica de atributos expedida por un organismo del sector público responsable de una fuente auténtica, o en nombre de este? . . . . .	228
5.3.4.	¿Qué efectos jurídicos tienen las diferentes modalidades de declaración electrónica de atributos? . . . . .	229
5.4.	Otros servicios de certificación electrónica o de confianza en la reforma 2024 . . . . .	230
5.4.1.	Servicio de gestión de dispositivos de creación de firmas electrónicas y sellos electrónicos a distancia . . . . .	230
5.4.2.	Servicio de archivo electrónico . . . . .	231

**CAPÍTULO 2. IDENTIFICACIÓN DIGITAL Y FIRMA ELECTRÓNICA EN LA ADMINISTRACIÓN DE JUSTICIA . . . . .** 233

1.	SOBRE LA IDENTIFICACIÓN Y FIRMA ELECTRÓNICAS . . .	235
2.	REGULACIÓN EN LA ADMINISTRACIÓN DE JUSTICIA . . .	235
2.1.	Antecedentes . . . . .	235
2.2.	¿Qué sistemas de identificación y firma electrónicas son admitidos por la Administración de Justicia para su utilización por los ciudadanos/as y los profesionales? . . . . .	236
2.3.	Sistema de identificación seguro en videoconferencias . . . . .	238
2.4.	¿Qué sistemas de identificación y firma electrónicas han de ser usados por la Administración de Justicia? . . . . .	238
3.	SISTEMAS DE FIRMA ELECTRÓNICA ADMITIDOS POR LA ADMINISTRACIÓN DE JUSTICIA. . . . .	240
3.1.	Servicios de certificación cualificados. . . . .	241
3.2.	Otro sistema de identificación válido para la Administración . . . . .	241
3.3.	Sistema de utilización de la firma electrónica del funcionario . . . . .	242
4.	INTERCAMBIO ELECTRÓNICO DE DATOS EN ENTORNOS CERRADOS DE COMUNICACIÓN . . . . .	242

**PARTE VI****PRESENCIA TELEMÁTICA EN ACTOS PROCESALES**

<b>CAPÍTULO 1. RÉGIMEN JURÍDICO COMÚN</b> .....	247
1. MODALIDADES Y RÉGIMEN JURÍDICO .....	249
1.1. ¿Qué es la presencia telemática? .....	249
1.2. Actos y servicios no presenciales .....	250
1.3. Modalidades de asistencia telemática a un acto procesal .....	251
1.3.1. Presencia telemática total/parcial. Vistas o juicios telemáticos .....	251
1.3.2. Modalidades tecnológicas para la presencia telemática. ....	252
1.3.3. Salas de vistas virtuales .....	252
1.3.4. Sistemas de grabación .....	253
2. RÉGIMEN JURÍDICO DE LA PRESENCIA TELEMÁTICA EN LOS ACTOS PROCESALES .....	253
2.1. Ámbito de aplicación .....	254
2.2. Constitución del tribunal en su sede física. ....	254
2.3. Preferencia por la presencia telemática de los asistentes .....	255
2.4. Normas comunes sobre la forma de realización ...	255
3. PUBLICIDAD .....	256
3.1. Sobre el principio de publicidad .....	257
3.2. Publicidad de un acto celebrado telemáticamente .	258
3.2.1. Retransmisión de imagen y sonido. ....	258
3.2.2. Publicidad de la agenda de actos orales. .	259
4. PROTECCIÓN DE DATOS PERSONALES EN LA ASISTENCIA TELEMÁTICA .....	259
4.1. Deber de confidencialidad: medidas de minimización del riesgo .....	260
4.2. Medidas específicas previstas en el RDL 6/23 .....	260

4.2.1.	Prohibición de grabación. . . . .	261
4.2.2.	Prohibición de uso para fines no jurisdiccionales. . . . .	261
4.2.3.	Sanciones por el incumplimiento de las obligaciones del art. 67 . . . . .	261
5.	IDENTIFICACIÓN DE LA PERSONA . . . . .	262
5.1.	¿Cuál es la normativa aplicable? . . . . .	262
5.2.	¿Cuándo se ha de identificar a la persona? . . . . .	262
5.3.	¿Cómo se identifica a la persona que está presente telemáticamente? . . . . .	262
5.4.	Sobre la identificación electrónica . . . . .	262
5.4.1.	Utilización preferente . . . . .	262
5.4.2.	Comprobación de la identificación electrónica. . . . .	263
5.4.3.	Medios para la identificación electrónica. . . . .	263
5.4.4.	Impugnación de la identificación. . . . .	265
5.4.5.	Escritorio Virtual de Interacción Digital (EVID) . . . . .	265
<b>CAPÍTULO 2. REGULACIÓN DEL PROCESO CIVIL . . . . .</b>		<b>267</b>
1.	ESQUEMA GENERAL EN EL PROCESO CIVIL . . . . .	269
2.	SUPUESTOS. . . . .	269
2.1.	Casos en que resulta necesaria la presencia física . . . . .	269
2.2.	Resto de supuestos: preferencia por la presencia telemática . . . . .	270
2.3.	Respeto de garantías procesales . . . . .	270
2.4.	Otras normas procesales civiles . . . . .	271
<b>CAPÍTULO 3. REGULACIÓN DEL PROCESO PENAL . . . . .</b>		<b>273</b>
1.	ESQUEMA GENERAL DEL PROCESO PENAL. . . . .	275
2.	CRITERIOS PARA LA DECISIÓN DEL JUEZ . . . . .	277
2.1.	Criterios generales. . . . .	277
2.2.	Presencia del sujeto pasivo del proceso penal. . . . .	278

2.3.	Presencia de determinadas víctimas . . . . .	279
2.4.	Resto de víctimas . . . . .	280
2.5.	Presencia de autoridades o funcionarios públicos . .	281
2.6.	Presencia del Ministerio Fiscal . . . . .	281
2.7.	Presencia de intérpretes . . . . .	281
2.8.	Personas que se encuentran en otro Estado de la UE	282
3.	FORMA DE REALIZACIÓN . . . . .	282
3.1.	Normas de la LECRIM. . . . .	282
3.2.	Respeto de las garantías procesales. . . . .	283
4.	PRESENCIA TELEMÁTICA DEL «INCUPLADO» DEL PROCE- SO PENAL . . . . .	285
4.1.	Esquema general. . . . .	285
4.2.	Peculiaridades a la participación del inculgado en el proceso penal . . . . .	286
4.3.	Pleno respeto del derecho defensa y garantías pro- cesales . . . . .	287
4.4.	Asistencia letrada al detenido . . . . .	289
4.5.	Lugar desde el que se realiza la conexión telemáti- ca . . . . .	290
4.5.1.	Lugares seguros . . . . .	290
4.5.2.	Puntos de acceso seguros. . . . .	291
4.5.3.	Condiciones materiales . . . . .	292
4.6.	Otros elementos . . . . .	292
4.6.1.	Documentación del acto . . . . .	292
4.6.2.	Aportación de documentos . . . . .	293
4.6.3.	Comprobaciones técnicas . . . . .	293
4.6.4.	Comportamiento de la persona presente telemáticamente. . . . .	294
4.6.5.	Instrucciones sobre la celebración del ac- to . . . . .	294

**CAPÍTULO 4. PRESENCIA TELEMÁTICA EN LA COOPERACIÓN  
JUDICIAL INTERNACIONAL . . . . .** 295

1.	ÁMBITO CIVIL . . . . .	297
----	------------------------	-----

1.1.	Unión Europea . . . . .	297
1.2.	Conferencia de la Haya de Derecho Internacional Privado (HCCH) . . . . .	298
1.3.	Iberoamérica. . . . .	298
1.4.	Otros ámbitos territoriales. . . . .	298
2.	ÁMBITO PENAL. . . . .	299
2.1.	Unión Europea . . . . .	299
	2.1.1. OEI: España como Estado de emisión. . . . .	299
	2.1.2. OEI: España como Estado de ejecución . . . . .	300
2.2.	Iberoamérica. . . . .	302
2.3.	Otros ámbitos territoriales. . . . .	302
2.4.	Futuro próximo de la videoconferencia en la cooperación penal . . . . .	303
	2.4.1. Unión Europea: nueva normativa sobre digitalización de la cooperación judicial . . . . .	303
	2.4.2. Segundo Protocolo Adicional a la Convención sobre la Cibercriminalidad . . . . .	303

## PARTE VII

### LA PROTECCIÓN DE DATOS PERSONALES EN EL PROCESO JUDICIAL

<b>CAPÍTULO 1. INTRODUCCIÓN A LA TUTELA DE LOS DATOS PERSONALES . . . . .</b>	<b>307</b>	
1. EL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS PERSONALES . . . . .	309	
1.1. Concepto de datos personales. . . . .	309	
1.2. El derecho a la protección de datos personales. . . . .	310	
1.3. Instrumentos internacionales. . . . .	310	
1.4. Tutela como derecho fundamental . . . . .	311	
1.5. Conceptos básicos de protección de datos . . . . .	313	
	1.5.1. Tratamiento de datos . . . . .	314
	1.5.2. Responsable del tratamiento . . . . .	315

1.5.3.	Principios del tratamiento . . . . .	316
2.	REGULACIÓN . . . . .	317
2.1.	Reglamento 2016/679 (RGPD) . . . . .	318
2.2.	Directiva 2016/680 . . . . .	318
<b>CAPÍTULO 2. DATOS PERSONALES EN LA ADMINISTRACIÓN DE JUSTICIA . . . . .</b>		<b>319</b>
1.	MODALIDADES DE TRATAMIENTO Y SU REGULACIÓN. . . . .	321
1.1.	Normativa reguladora . . . . .	321
1.1.1.	Actuaciones procesales por órganos judiciales . . . . .	321
1.1.2.	Actuaciones tramitadas por el Fiscal . . . . .	321
1.1.3.	Actuaciones procesales penales . . . . .	322
1.2.	Modalidades de tratamiento . . . . .	322
1.2.1.	Tratamiento con fines jurisdiccionales . . . . .	322
1.2.2.	Tratamiento con fines no jurisdiccionales . . . . .	323
2.1.	Delimitación conceptual . . . . .	324
2.2.	Un régimen jurídico singular . . . . .	325
2.3.	Licitud del tratamiento en el proceso judicial . . . . .	327
3.	RÉGIMEN JURÍDICO DEL TRATAMIENTO DE LOS DATOS PERSONALES CON FINES JURISDICCIONALES. . . . .	329
3.1.	¿Qué datos personales contendrán las resoluciones y actuaciones procesales? . . . . .	329
3.2.	¿Qué derechos pueden ejercitar los titulares de los datos personales obrantes en el proceso? . . . . .	329
3.3.	¿A través de qué procedimientos pueden ejercitar los derechos? . . . . .	330
3.4.	¿Sobre quién recaen las obligaciones impuestas a los responsables y encargados del tratamiento? . . . . .	331
3.4.1.	Responsable del tratamiento: órgano jurisdiccional/oficina judicial . . . . .	331
3.4.2.	Papel de la Administración Pública competente . . . . .	333

3.5.	Protección de datos en los documentos judiciales electrónicos . . . . .	335
4.	AUTORIDAD DE CONTROL EN RELACIÓN CON LOS FICHEROS JURISDICCIONALES . . . . .	336
4.1.	En el Consejo General del Poder Judicial . . . . .	337
4.2.	En la Fiscalía General del Estado. . . . .	338
4.3.	Relación con la Agencia Española de Protección de Datos . . . . .	339
4.4.	Cesión de datos a CGPJ, FGE y/o Ministerio de Justicia para el ejercicio de sus respectivas funciones .	340
 <b>CAPÍTULO 3. PROTECCIÓN DE DATOS PERSONALES Y PRUEBA EN EL PROCESO.</b> . . . . .		 341
1.	¿CUÁLES SON LAS RELACIONES ENTRE EL DERECHO A LA PRUEBA Y LA PROTECCIÓN DE DATOS PERSONALES? . . . . .	344
1.1.	Prueba y tratamiento de datos . . . . .	344
1.2.	Incumplimiento en el régimen de proposición, admisión y práctica de la prueba . . . . .	345
1.2.1.	Efectos de la vulneración . . . . .	345
1.2.2.	Datos de categoría especial . . . . .	345
1.3.	Violación en la obtención de la prueba. . . . .	347
2.	¿EN QUÉ SUPUESTOS ES LÍCITA LA APORTACIÓN DE DATOS PERSONALES AL PROCESO CON FINALIDAD DE PRUEBA? . . . . .	348
2.1.	Obtención del dato por requerimiento judicial . . . . .	349
2.1.1.	General . . . . .	349
2.1.2.	En el proceso penal . . . . .	350
2.1.2.1.	Base jurídica que legitima la obtención y tratamiento . . . . .	350
2.1.2.2.	Necesidad para una investigación concreta. . . . .	351
2.1.2.3.	Cesión de datos personales en la investigación y prueba de los delitos. . . . .	352

2.2.	Aportación de datos personales por una parte procesal . . . . .	353
2.3.	¿Qué efectos procesales se derivan la vulneración del derecho fundamental a la protección de datos personales en la obtención y aportación de datos al proceso? . . . . .	357
2.3.1.	Efectos directos . . . . .	357
2.3.2.	Efectos indirectos . . . . .	359
2.3.3.	Efectos verticales y horizontales . . . . .	359
2.3.3.1.	Vulneración por agentes públicos . . . . .	359
2.3.3.2.	Vulneración por particulares . . . . .	360
3.	¿CÓMO SE PUEDE HACER VALER LA NULIDAD EN EL PROCESO? . . . . .	361
3.1.	Nulidad de oficio por el Juez . . . . .	362
3.2.	Nulidad a instancia de parte procesal . . . . .	362
<b>CAPÍTULO 4. CONTENIDO DE LAS RESOLUCIONES JUDICIALES Y PROTECCIÓN DE DATOS. . . . .</b>		<b>365</b>
1.	EXAMEN DE LA JURISPRUDENCIA DEL TRIBUNAL EUROPEO DE DERECHOS HUMANOS. . . . .	367
1.1.	Sobre la STEDH de 6 de octubre de 2010 (asunto CC contra España). . . . .	367
1.1.1.	Antecedentes . . . . .	367
1.1.2.	Decisión del TEDH . . . . .	368
1.2.	Sobre la STEDH de 6 de noviembre de 2018 (asunto Vicent del Campo c. España). . . . .	369
1.2.1.	Antecedentes . . . . .	369
1.2.2.	Decisión del TEDH . . . . .	369
2.	ORDENAMIENTO ESPAÑOL . . . . .	371
2.1.	Fase de evaluación del riesgo . . . . .	372
2.2.	Juicio de ponderación: adopción de medidas en función del nivel y tipo de riesgo . . . . .	373
2.3.	Conclusión . . . . .	375

<b>CAPÍTULO 5. SUPRESIÓN Y CONSERVACIÓN DE DATOS PERSONALES EN EL PROCESO</b> .....	377
1. DATOS PERSONALES: DERECHO DE SUPRESIÓN O DERECHO AL OLVIDO .....	379
1.1. Normativa de protección de datos .....	379
1.2. Derecho al olvido en el proceso .....	380
2. DATOS PERSONALES: PRINCIPIO DE LIMITACIÓN DEL PLAZO DE CONSERVACIÓN .....	381
 <b>CAPÍTULO 6. OTROS ÁMBITOS DE TRATAMIENTO DE DATOS EN LA ADMINISTRACIÓN DE JUSTICIA</b> .....	 383
1. TRATAMIENTO DE DATOS PERSONALES POR EL MINISTERIO FISCAL .....	385
1.1. Tratamientos con fines jurisdiccionales o cuasijurisdiccionales .....	385
1.1.1. Ámbito penal .....	385
1.1.2. Actuaciones no penales .....	386
1.1.3. Autoridad de Control .....	386
1.2. Tratamiento de datos con fines no jurisdiccionales .	386
2. TRATAMIENTO DE DATOS POR ABOGADOS, PROCURADORES Y GRADUADOS SOCIALES .....	387
2.1. Datos de su representado y/o defendido .....	387
2.2. Datos personales conocidos en el proceso .....	387
2.3. Datos personales de la parte contraria. ....	387
 <b>CAPÍTULO 7. PROCESO PENAL Y PROTECCIÓN DE DATOS PERSONALES</b> .....	 389
1. NORMATIVA REGULADORA .....	391
1.1. Directiva (UE) 2016/680 .....	391
1.2. Normativa supletoria. ....	392
2. SISTEMA DE PROTECCIÓN DE DATOS PERSONALES EN EL PROCESO PENAL .....	392

2.1.	Derechos reconocidos a los titulares . . . . .	392
2.2.	Procedimientos para ejercitar los derechos . . . . .	394
3.	PRINCIPIOS APLICABLES AL TRATAMIENTO DE DATOS EN EL ÁMBITO PENAL. . . . .	395
3.1.	Principio de licitud y lealtad . . . . .	396
3.2.	Principio de limitación de la finalidad. . . . .	397
3.3.	Principio de minimización . . . . .	397
3.4.	Principio de exactitud . . . . .	398
3.5.	Principio de limitación del plazo de conservación . . . . .	398
3.6.	Principio de integridad y confidencialidad . . . . .	399
3.7.	Principio de responsabilidad . . . . .	400
3.8.	Principio de protección de datos por defecto y desde el diseño . . . . .	400
4.	DATOS ESPECIALMENTE SENSIBLES . . . . .	402
4.1.	Categorías especiales de datos . . . . .	402
4.2.	Tratamiento de datos sobre condenas e infracciones penales . . . . .	404
5.	CATEGORÍAS DE INTERESADOS EN EL PROCESO . . . . .	405
6.	PROTECCIÓN DE DATOS EN LA ORDEN EUROPEA DE INVESTIGACIÓN . . . . .	405
<b>CAPÍTULO 8. TUTELA PENAL DE LOS DATOS PERSONALES . .</b>		<b>407</b>
1.	LA PROTECCIÓN DEL ENTORNO VIRTUAL: TUTELA PENAL DE LOS DATOS PERSONALES. . . . .	409
1.1.	Papel del Derecho Penal . . . . .	409
1.2.	Bien jurídico protegido . . . . .	410
2.	ELEMENTOS DEL TIPO DEL ARTÍCULO 197.2 CP. . . . .	411
2.1.	Datos personales. . . . .	411
2.2.	Acceso no autorizado al dato . . . . .	412
2.3.	Sujeto activo . . . . .	412
2.4.	Falta de autorización. . . . .	413
2.5.	Formas comisivas . . . . .	414
2.6.	Sobre la expresión «en perjuicio» . . . . .	415

2.7.	Grave menoscabo para el bien jurídico. . . . .	418
2.8.	Parte subjetiva del tipo . . . . .	418
2.9.	Delito de peligro. . . . .	419
3.	FICHAS SOBRE SENTENCIAS RELEVANTES. . . . .	419
3.1.	Ficha sobre la STS 260/2021, de 22 de marzo. . . . .	419
3.2.	Ficha sobre la STS 538/2021, de 17 de junio . . . . .	422
3.3.	Ficha sobre la STS 259/2022, de 17 de marzo. . . . .	424
3.4.	Ficha sobre la STS 43/2022, de 20 de enero . . . . .	425
3.5.	Ficha sobre la STS 616/2022, de 22 de junio . . . . .	426

## **PARTE VIII**

### **INTELIGENCIA ARTIFICIAL Y AUTOMATIZACIÓN EN EL SISTEMA DE JUSTICIA**

<b>CAPÍTULO 1. AUTOMATIZACIÓN, ROBOTIZACIÓN E INTELIGENCIA ARTIFICIAL . . . . .</b>	<b>431</b>
1. INTRODUCCIÓN Y ELEMENTO CONCEPTUALES . . . . .	433
1.1. Objeto . . . . .	433
1.2. Delimitación conceptual. . . . .	433
1.3. Normativa aplicable . . . . .	435
2. NORMATIVA DE PROTECCIÓN DE DATOS PERSONALES. . . . .	436
3. REGULACIÓN EN LA LEY ORGÁNICA DEL PODER JUDICIAL. . . . .	438
3.1. IA para la gestión de recursos y el seguimiento de las actuaciones del sistema de justicia. . . . .	438
3.2. IA para la clasificación documental en el procedimiento . . . . .	439
4. NORMATIVA PROCESAL. . . . .	440
5. NORMATIVA SOBRE EFICIENCIA PROCESAL . . . . .	440
5.1. Actuaciones procesales automatizadas . . . . .	441
5.2. Actuaciones procesales proactivas . . . . .	442
5.3. Actuaciones procesales asistidas . . . . .	443

5.4.	Régimen común a los tres tipos de actuaciones. . . .	443
5.5.	Reglas para automatizadas y proactivas . . . . .	444
5.6.	Relevante papel del CTAJE . . . . .	444
5.7.	Papel del CGPJ (y de la FGE). . . . .	445
5.8.	Conclusiones . . . . .	446
<b>CAPÍTULO 2. APLICACIÓN DE LA INTELIGENCIA ARTIFICIAL EN EL SISTEMA DE JUSTICIA . . . . .</b>		<b>447</b>
1.	IA EN EL SISTEMA DE JUSTICIA: PLANTEAMIENTO GENERAL . . . . .	449
1.1.	¿Qué relación existe entre IA y JUSTICIA?. . . . .	449
1.2.	Necesidad de un debate social . . . . .	450
2.	¿QUÉ? INTELIGENCIA ARTIFICIAL PARA LA FUNCIÓN JURISDICCIONAL . . . . .	451
2.1.	Universo IA. . . . .	451
2.2.	IA débil/IA fuerte. . . . .	452
2.3.	Soluciones apoyo/Soluciones sustitutivas . . . . .	452
2.4.	Sistemas expertos/Machine learning . . . . .	454
2.4.1.	Delimitación conceptual . . . . .	454
2.4.2.	Sobre la estructura lógica de la sentencia: sistemas expertos . . . . .	456
2.4.3.	Aprendizaje automático. Sistemas de caja negra . . . . .	458
3.	¿PARA QUÉ? APLICACIÓN DE LA IA EN LA JUSTICIA. . . . .	459
3.1.	Detección y clasificación inteligente de información . . . . .	459
3.2.	Automatización. . . . .	460
3.3.	Asistencia inteligente . . . . .	461
3.3.1.	Para la toma de decisiones por el justiciable . . . . .	461
3.3.2.	Para la toma de decisiones por el juez, el fiscal o el letrado de la Administración de Justicia. . . . .	462
3.3.3.	Para la valoración de la prueba . . . . .	462

3.4.	Predicción: valoración del riesgo .....	464
4.	¿CÓMO? FACTORES ORGANIZATIVOS .....	466
4.1.	Marco de gobernanza .....	466
4.2.	Sistema de seguimiento y control .....	466
4.3.	Gestión del cambio .....	467
4.4.	Carácter multidisciplinario y colaboración público-privada .....	468
5.	USO DE LA IA GENERATIVA POR LOS PROFESIONALES DEL SISTEMA DE JUSTICIA .....	469
5.1.	¿Qué es la IA generativa? .....	469
5.2.	Uso de la IA generativa por profesionales del sistema de justicia .....	470
5.3.	Riesgos .....	471
5.4.	Uso de ChatGPT 3.5 por un juez: sentencia de la Corte Constitucional de Colombia .....	472

**CAPÍTULO 3. HUMANIZACIÓN DE LA INTELIGENCIA ARTIFICIAL .....** 475

1.	SOBRE LA HUMANIZACIÓN .....	477
1.1.	¿Qué es humanizar? .....	477
1.2.	¿Por qué es tan necesario humanizar la aplicación de la IA en la justicia? .....	478
2.	DECÁLOGO PARA UNA HUMANIZACIÓN .....	480
2.1.	Respeto a la dignidad humana: intervención y supervisión humanas .....	480
2.2.	Principio de control por el usuario del sistema de justicia .....	481
2.3.	Respeto de los derechos fundamentales .....	482
2.4.	Respeto de las garantías del proceso debido .....	484
2.5.	Garantía del acceso a la justicia .....	485
2.5.1.	Personas vulnerables .....	486
2.5.2.	Brecha digital .....	487
2.6.	Respeto de la garantía jurisdiccional .....	487
2.6.1.	Juez humano .....	488

2.6.2.	Independencia judicial. . . . .	488
2.6.3.	Competencia (riesgo para el ejercicio adecuado de la función judicial) . . . . .	489
2.6.4.	Decisiones judiciales automatizadas . . . . .	489
2.7.	No discriminación y prohibición de sesgos. . . . .	491
2.7.1.	Principio de no discriminación . . . . .	491
2.7.2.	Ausencia de sesgos . . . . .	491
2.8.	Transparencia . . . . .	493
2.8.1.	Elementos de la transparencia de los sistemas IA . . . . .	493
2.8.1.1.	Explicabilidad . . . . .	493
2.8.1.2.	Trazabilidad. . . . .	494
2.8.1.3.	Identificabilidad. . . . .	494
2.8.1.4.	Acceso algorítmico. . . . .	494
2.8.2.	Sistemas de caja negra . . . . .	495
2.9.	Confianza (fiabilidad) . . . . .	496
2.9.1.	Fiabilidad. . . . .	496
2.9.2.	Calidad de los datos. . . . .	497
2.10.	Responsabilidad y rendición de cuentas . . . . .	498
2.10.1.	Rendición de cuentas. . . . .	498
2.10.2.	Responsabilidad. . . . .	499
3.	REFLEXIONES FINALES . . . . .	499
4.	¿Y EN EL FUTURO? . . . . .	500
<b>CAPÍTULO 4. EL SISTEMA DE JUSTICIA EN EL REGLAMENTO EUROPEO DE INTELIGENCIA ARTIFICIAL . . . . .</b>		<b>503</b>
1.	CLASIFICACIÓN DE LOS SISTEMAS IA EN FUNCIÓN DEL RIESGO . . . . .	505
1.1.	Sistemas IA de alto riesgo . . . . .	505
1.1.1.	¿Cuáles son? . . . . .	506
1.1.2.	Sistemas de alto riesgo del Anexo III . . . . .	507
1.2.	Sistemas IA con riesgos mínimos. . . . .	510
1.3.	Sistemas IA con obligaciones de transparencia . . . . .	510

2.	SISTEMAS IA EN LA ADMINISTRACIÓN DE JUSTICIA. . . . .	511
2.1.	Sustitución del juez en el RIA: el juez robot . . . . .	511
2.2.	Sistemas IA de alto riesgo en la Administración de Justicia . . . . .	511
2.3.	Actividades sin riesgo o de riesgo mínimo en la Administración de Justicia . . . . .	512
2.3.1.	Fundamento. . . . .	512
2.3.2.	¿Qué actividades se pueden incluir en el ámbito excluido de la consideración de alto riesgo en el sistema de justicia?. . . . .	513
2.3.3.	Obligaciones . . . . .	515
2.3.4.	Fomento de códigos de conducta para la aplicación voluntaria de requisitos específicos. . . . .	515
3.	IA EN EL SISTEMA PENAL . . . . .	516
3.1.	Sistemas de IA de alto riesgo en garantía del cumplimiento del Derecho . . . . .	516
3.2.	Sistemas IA para evaluar el riesgo de comisión de delitos. . . . .	516
3.3.	Riesgo de suplantación o engaño: obligaciones de información y/o transparencia. . . . .	517
4.	BIOMETRÍA . . . . .	518
4.1.	Sobre los datos biométricos. . . . .	518
4.2.	Verificación biométrica. . . . .	520
4.3.	Identificación biométrica . . . . .	520
4.4.	Sistema de identificación remota en tiempo real en espacio de acceso público . . . . .	521
4.4.1.	Delimitación conceptual . . . . .	521
4.4.2.	Prohibición general con excepción del sistema penal. . . . .	523
4.4.3.	Supuestos en los que el Estado miembro puede autorizar su uso. . . . .	524
4.4.4.	Requisitos para su utilización por el sistema penal . . . . .	525
4.5.	Categorización biométrica . . . . .	528
4.5.1.	Concepto. . . . .	528

4.5.2.	Sistemas de categorización biométrica que clasifiquen individualmente a las personas . . . . .	528
4.5.3.	Requisitos de los sistemas de categorización biométrica permitidos . . . . .	529
4.6.	Reconocimiento de emociones . . . . .	530
4.6.1.	Concepto . . . . .	530
4.6.3.	Requisitos de los sistemas IA . . . . .	530
5.	CONSECUENCIAS DE LA CALIFICACIÓN COMO ALTO RIESGO . . . . .	530
5.1.	Requisitos . . . . .	531
5.2.	Evaluación de impacto relativa a los derechos fundamentales . . . . .	532
6.	ACTIVIDADES DE LAS AUTORIDADES DE VIGILANCIA DEL MERCADO Y RÉGIMEN SANCIONADOR EN RELACIÓN CON EL SISTEMA DE JUSTICIA . . . . .	534
6.1.	Designación de autoridad de vigilancia de mercado para los sistemas IA en la justicia . . . . .	535
6.2.	Respeto de la función judicial . . . . .	535
6.3.	Régimen sancionador . . . . .	535
6.3.1.	Régimen general . . . . .	535
6.3.2.	Sobre la posible responsabilidad de las entidades del sector público. . . . .	536

## PARTE IX

### DIMENSIÓN INTERNACIONAL DE LA DIGITALIZACIÓN JUDICIAL

<b>CAPÍTULO 1. DIGITALIZACIÓN DE LA COOPERACIÓN JUDICIAL INTERNACIONAL. . . . .</b>	<b>541</b>
1. DIGITALIZACIÓN EN EL ESPACIO JUDICIAL EUROPEO. . .	543
1.1. El Espacio Judicial Europeo . . . . .	543
1.1.1. Mejora de la cooperación judicial . . . . .	544

1.1.2.	Mejora del acceso a la justicia en asuntos transfronterizos . . . . .	545
1.2.	La digitalización de la justicia en la UE. . . . .	546
1.2.1.	Comunicación de 2 de diciembre de 2020 . . . . .	546
1.2.2.	Ejes de la digitalización . . . . .	547
2.	REGLAMENTO (UE) 2023/2844, DE 13 DE DICIEMBRE DE 2023, SOBRE LA DIGITALIZACIÓN DE LA COOPERACIÓN JUDICIAL Y DEL ACCESO A LA JUSTICIA EN ASUNTOS TRANSFRONTERIZOS . . . . .	548
2.1.	Ejes del Reglamento . . . . .	548
2.2.	Comunicación electrónica entre autoridades competentes . . . . .	550
2.2.1.	Régimen jurídico . . . . .	550
2.2.2.	Utilización subsidiaria de otros sistemas de comunicación . . . . .	553
2.2.3.	Infraestructura para las comunicaciones entre autoridades . . . . .	554
2.3.	Comunicación entre personas físicas o jurídicas y las autoridades competentes en materia civil y mercantil. . . . .	556
2.3.1.	¿A qué órganos y/o personas afecta esta comunicación electrónica? . . . . .	556
2.3.2.	¿Qué es el punto de acceso electrónico europeo? . . . . .	556
2.3.3.	¿Para qué pueden utilizarse estas comunicaciones electrónicas? . . . . .	556
2.3.4.	¿En qué instrumentos jurídicos UE resulta aplicable? . . . . .	557
2.4.	Vistas por videoconferencia o por otro medio tecnológico de comunicación a distancia . . . . .	558
2.4.1.	Materia civil y mercantil . . . . .	558
2.4.2.	Materia penal. . . . .	559
2.5.	Garantizar la aplicación de los instrumentos de confianza digital del Reglamento eIDAS . . . . .	562
2.6.	Pago electrónico de tasas . . . . .	563

3.	SOBRE EL SISTEMA E-CODEX . . . . .	563
3.1.	Régimen jurídico del sistema e-CODEX: el Reglamento (UE) 2022/850 . . . . .	564
3.2.1.	¿Para qué? . . . . .	564
3.1.2.	¿Qué es y cómo se organiza? . . . . .	564
3.2.	Porta eDES . . . . .	566
4.	DIGITALIZACIÓN DE LA COOPERACIÓN JUDICIAL INTERNACIONAL EN IBEROAMÉRICA . . . . .	567
4.1.	Tratado de Medellín . . . . .	567
4.2.	Contenido . . . . .	567
4.2.1.	Transmisión de solicitudes de cooperación jurídica internacional entre Autoridades Centrales . . . . .	567
4.2.2.	Comunicación entre Puntos de Contacto y Enlaces de IberRed. . . . .	568
<b>CAPÍTULO 2. COOPERACIÓN JUDICIAL CONTRA LA CIBERDELINCUENCIA. . . . .</b>		<b>569</b>
1.	COMISIONES ROGATORIAS INTERNACIONALES. EL CONVENIO DE BUDAPEST. . . . .	572
1.1.	Asistencia mutua para medidas provisionales . . . . .	572
1.2.	Asistencia mutua para remisión de datos. . . . .	574
1.3.	Acceso transfronterizo a datos. . . . .	574
1.4.	Otras formas: obtención en tiempo real . . . . .	574
1.5.	Supuestos de urgencia. . . . .	575
2.	UNIÓN EUROPEA . . . . .	575
2.1.	Conservación rápida de datos . . . . .	575
2.1.1.	Régimen general . . . . .	575
2.1.2.	Dinamarca e Irlanda . . . . .	577
2.2.	Remisión de los datos . . . . .	577
2.2.1.	Emisión por órgano español. . . . .	577
2.2.2.	Ejecución en España . . . . .	579
3.	ESTADOS UNIDOS . . . . .	584
3.1.	Tratado bilateral . . . . .	584

3.1.1.	Preservación de datos . . . . .	584
3.1.2.	Entrega de datos. . . . .	587
3.1.3.	Entrega de datos en supuestos de urgencia	587
3.2.	Sistema Cloud Act. . . . .	587
3.2.1.	EEUU como parte activa . . . . .	587
3.2.2.	EEUU como parte pasiva . . . . .	588
4.	IBEROAMÉRICA: TRATADO DE MADRID. . . . .	589
4.1.	Estado actual del convenio . . . . .	589
4.2.	Contenido. . . . .	590
5.	RECOMENDACIONES PARA MEJORAR LA OBTENCIÓN INTERNACIONAL DE DATOS . . . . .	591
5.1.	Estrategia general . . . . .	591
5.1.1.	Agotar fuentes abiertas y recursos internos	591
5.1.2.	Solicitud internacional alternativa a la Comisión Rogatoria formal. . . . .	591
5.1.3.	Uso de la Asistencia Judicial Internacional	591
5.2.	Decálogo de recomendaciones para mejorar las solicitudes de cooperación judicial internacional. . . . .	592
5.3.	Acceso a datos abiertos al público . . . . .	593
5.3.1.	Identificar propietarios de nombres de dominio. . . . .	593
5.3.2.	Fuentes abiertas . . . . .	594
5.4.	Entrega voluntaria por el proveedor de servicios a requerimiento de la autoridad pública . . . . .	595
6.	COOPERACIÓN POLICIAL INTERNACIONAL. . . . .	596
6.1.	Canales de cooperación policial . . . . .	596
6.1.1.	Centro Europeo de Ciberdelincuencia (EC3) . . . . .	597
6.1.2.	Red 24/7 del Convenio de Budapest . . . . .	597
6.1.3.	Red 24/7 de Interpol . . . . .	597
6.2.	Intercambio espontáneo de información. . . . .	598
6.3.	Información transmitida por servicios policiales extranjeros . . . . .	599
7.	PANORAMA DE FUTURO. . . . .	601

---

8.	OBTENCIÓN DE DATOS EN PODER DE PROVEEDORES . . .	601
8.1.	Relevancia . . . . .	601
8.2.	Dificultades en la obtención de datos en poder de los proveedores de servicios . . . . .	603
8.2.1.	Peligro de pérdida de datos . . . . .	603
8.2.2.	Localización de los datos. . . . .	603
8.2.3.	Falta de un marco legal adecuado . . . . .	604
8.2.4.	Desafíos de las novedades tecnológicas. . . . .	605
8.2.5.	Dimensión internacional . . . . .	605
8.2.6.	Ineficiencias en la colaboración público-privada. . . . .	606
9.	INSTRUMENTOS PARA LA OBTENCIÓN DE DATOS EN PODER DE PROVEEDORES . . . . .	606
9.1.	Segundo Protocolo del Convenio de Budapest . . . . .	607
9.2.	Nuevo sistema en la UE: sistema E-Evidence. . . . .	609
10.	SOBRE EL REGLAMENTO E-EVIDENCE . . . . .	611
10.1.	Ámbito de aplicación . . . . .	611
10.1.1.	¿Cuál es el objeto? . . . . .	611
10.1.2.	¿Qué datos pueden ser objeto de una Orden? . . . . .	611
10.2.	Emisión de la Orden . . . . .	615
10.2.1.	¿Qué autoridades pueden emitir las órdenes? . . . . .	615
10.2.2.	¿Cuál es la forma de emisión? . . . . .	616
10.2.3.	¿Cuál es la forma de remisión? . . . . .	616
10.3.	Ejecución de la Orden . . . . .	616
10.3.1.	Orden de Conservación . . . . .	616
10.3.2.	Orden de Producción. . . . .	617

**PARTE X**

**RETIRADA DE CONTENIDOS ILÍCITOS Y COLABORACIÓN DE  
LOS PRESTADORES DE SERVICIOS. EL REGLAMENTO DE  
SERVICIOS DIGITALES**

<b>CAPÍTULO 1. COLABORACIÓN CON LAS AUTORIDADES PE- NALES EN EL REGLAMENTO DE SERVICIOS DIGITALES (DSA) .</b>	<b>623</b>
1. SOBRE EL DSA . . . . .	625
1.1.  Ámbito de aplicación: prestadores de servicios afectados. . . . .	625
1.2.  Colaboración voluntaria . . . . .	627
1.2.1.  Relevancia . . . . .	627
1.2.2.  Afectación a derechos fundamentales . . .	628
1.2.3.  Modalidades . . . . .	629
1.3.  Obligaciones de colaboración para la persecución de delitos . . . . .	631
2.  ÓRDENES DE ENTREGA DE INFORMACIÓN . . . . .	631
2.1.  Elementos de la orden. . . . .	631
2.1.1.  Autoridades emisoras. . . . .	631
2.1.2.  Destinatarios de la orden . . . . .	631
2.1.3.  Información objeto de la orden . . . . .	632
2.1.4.  Contenido mínimo de la orden . . . . .	632
2.2.  Procedimiento. . . . .	633
2.2.1.  Remisión al prestador de servicios e infor- mación por éste sobre el curso dado a la orden. . . . .	633
2.2.2.  Información al coordinador digital. . . . .	633
2.2.3.  Información al destinatario del servicio . .	634
3.  NOTIFICACIÓN DE SOSPECHAS DE DELITOS . . . . .	634
3.1.  ¿En qué supuestos nace la obligación de notificar sospechas? . . . . .	635
3.2.  ¿Qué información se ha de remitir?. . . . .	635
3.3.  ¿A qué Estado debe notificarse la sospecha? . . . . .	635

<b>CAPÍTULO 2. MEDIDAS FRENTE A CONTENIDOS CONSTITUTIVOS DE DELITO EN INTERNET . . . . .</b>	<b>637</b>
1. ORDEN DE RETIRADA DE CONFORMIDAD CON EL DERECHO ESPAÑOL . . . . .	639
1.1. Medidas para todos los delitos cometidos a través de las tecnologías de la información o de la comunicación . . . . .	640
1.2. Medidas para determinados delitos . . . . .	641
1.2.1. Pornografía infantil . . . . .	641
1.2.2. Delitos relativos a la propiedad intelectual . . . . .	641
1.2.3. Delitos de incitación al odio . . . . .	642
1.2.4. Determinados delitos de terrorismo . . . . .	642
1.2.4.1. Delito de enaltecimiento del terrorismo . . . . .	642
1.2.4.2. Delito de incitación al terrorismo . . . . .	643
1.3. Presupuestos para la adopción de la orden de retirada . . . . .	643
1.3.1. Apariencia de buen derecho . . . . .	644
1.3.2. Periculum in mora . . . . .	644
1.3.3. Proporcionalidad . . . . .	644
1.3.4. Motivación . . . . .	645
2. ÓRDENES DE RETIRADA EN EL REGLAMENTO DE SERVICIOS DIGITALES (DSA) . . . . .	646
2.1. Comunicación directa del prestador de servicios con las autoridades nacionales . . . . .	647
2.2. Condiciones y requisitos comunes . . . . .	648
3. ÓRDENES DE RETIRADA FRENTE A CONTENIDOS TERRORISTAS EN LÍNEA . . . . .	652
3.1. Ámbito de aplicación . . . . .	652
3.2. Órdenes de retirada . . . . .	654
3.3. Autoridad competente para las órdenes de retirada . . . . .	657
3.4. Tutela judicial . . . . .	658

3.5.	Otras obligaciones . . . . .	658
3.5.1.	Deber de informar a las autoridades penales . . . . .	658
3.5.2.	Medidas que deben adoptar los proveedores expuestos a contenidos terroristas. . . . .	659
4.	RETIRADA O ELIMINACIÓN DE MATERIAL ILÍCITO EN VIOLENCIA CONTRA LAS MUJERES Y VIOLENCIA DOMÉSTICA: DIRECTIVA 2024/1385 . . . . .	661
4.1.	Directiva (UE) 2024/1385 sobre la lucha contra la violencia contra las mujeres y la violencia doméstica . . . . .	661
4.2.	Órdenes de retirada de material ilícito . . . . .	662