

## ÍNDICE SISTEMÁTICO

<b>ABREVIATURAS</b> .....	29
<b>CAPÍTULO 1. TEORÍA GENERAL DE LA PRUEBA DIGITAL: CONCEPTO, MODALIDADES Y FASES EN TODOS LOS PROCESOS JUDICIALES.</b> .....	31
INTRODUCCIÓN: UNA TEORÍA GENERAL DE LA PRUEBA DIGITAL .....	33
1. SOBRE LA PRUEBA EN LA ERA DIGITAL .....	33
1.1. Justicia y sociedad de la información. ....	33
1.2. La prueba de hechos en la sociedad de la información. ....	36
1.3. Internet como fuente de prueba. ....	37
2. DELIMITACIÓN CONCEPTUAL DE LA PRUEBA DIGITAL ...	38
2.1. Concepto de prueba digital .....	40
2.2. Fuente y medio de prueba en el ámbito digital .....	41
2.3. Modalidades .....	42
2.4. Fases de la prueba digital .....	43
3. FASE DE OBTENCIÓN DE LA PRUEBA: LICITUD. ....	45
3.1. Acceso a datos contenidos en dispositivos electrónicos .....	45
3.1.1. Obtención de datos por la parte procesal ..	45
3.1.2. Obtención de datos por la autoridad pública competente en el proceso penal .....	46
3.2. Acceso a datos transmitidos por redes de comunicación. ....	47
3.3. Derechos fundamentales afectados en las distintas formas de obtención de la prueba digital. ....	48
4. FASE DE INCORPORACIÓN DE LA PRUEBA DIGITAL AL PROCESO. ....	49
4.1. Requisitos .....	49
4.2. La prueba digital puede ser incorporada al juicio por diferentes medios de prueba .....	51

4.3.	Documental en soporte papel . . . . .	52
4.4.	Documento electrónico. . . . .	53
4.4.1.	Concepto . . . . .	53
4.4.2.	Forma material de incorporación al proceso . . . . .	53
4.4.3.	Admisión del documento electrónico como prueba en los procedimientos de todos los órdenes jurisdiccionales . . . . .	55
4.4.4.	Régimen jurídico . . . . .	56
4.4.5.	Modalidades de documento electrónico. . . . .	56
	A. Documento electrónico público . . . . .	56
	B. Documento electrónico «oficial». . . . .	57
	C. Documento electrónico privado . . . . .	57
4.4.6.	Documentos judiciales electrónicos . . . . .	58
4.4.7.	Documento público notarial electrónico . . . . .	58
	A. Copia autorizada electrónica. . . . .	59
	B. Escritura matriz digital . . . . .	60
	C. Constatación fehaciente de hechos relacionados con soportes informático (mediante hash) . . . . .	60
4.4.8.	Registro de la Propiedad. . . . .	61
4.4.9.	Documento electrónico «oficial» . . . . .	61
4.4.10.	Facturas electrónicas . . . . .	62
4.4.11.	Los «pantallazos» . . . . .	64
4.5.	Prueba pericial . . . . .	64
4.5.1.	Concepto y caracteres de la prueba pericial informática. . . . .	64
4.5.2.	Modalidades de la pericial informática. . . . .	68
4.5.3.	La cadena de custodia en la pericial informática . . . . .	69
4.5.4.	Fases de la pericial informática. . . . .	69
	A. Obtención de los datos (acceso a la información) . . . . .	70
	B. Clonado de los datos y cálculo del hash. . . . .	70
	C. Elaboración del informe pericial . . . . .	72
	D. Presentación del dictamen pericial al tribunal . . . . .	72
	E. Valoración de la pericial informática. . . . .	72
4.6.	Reconocimiento judicial e inspección ocular . . . . .	73
4.7.	Anticipación o preconstitución de la prueba . . . . .	74
4.7.1.	Preconstitución extraprocésal de la prueba electrónica . . . . .	75

4.7.2.	Anticipación de la prueba digital en el proceso . . . . .	75
5.	VALORACIÓN DE LA PRUEBA DIGITAL . . . . .	75
5.1.	Libre valoración de la prueba . . . . .	76
5.1.1.	Regla general: libre valoración de la prueba electrónica . . . . .	77
5.1.2.	Valoración de las distintas modalidades de documentos electrónicos . . . . .	78
5.2.	Autenticidad e integridad de los datos . . . . .	80
5.2.1.	Autenticidad . . . . .	80
5.2.2.	Integridad . . . . .	81
5.2.3.	Garantías de autenticidad e integridad . . . . .	81
5.3.	Postura procesal de las partes . . . . .	82
5.3.1.	Impugnación . . . . .	82
5.3.2.	¿Reglas de distribución de la carga de la prueba? . . . . .	83
5.3.3.	Negación de presunción de ilegitimidad de actuaciones policiales . . . . .	86
5.4.	Valoración conjunta de la prueba . . . . .	86
5.4.1.	Concepto . . . . .	86
5.4.2.	Motivación de la valoración de la prueba . . . . .	87
5.5.	Efectos de la firma electrónica . . . . .	88
5.5.1.	Concepto . . . . .	88
5.5.2.	Modalidades de la firma electrónica . . . . .	90
5.5.3.	Valor probatorio de los documentos con firma electrónica . . . . .	92
5.6.	Terceros de confianza: Prestadores de Servicio de Confianza . . . . .	94
5.6.1.	Concepto y marco jurídico . . . . .	94
5.6.2.	Nuevo panorama tras el Reglamento UE 910/2014 . . . . .	95

## **CAPÍTULO 2. DERECHOS FUNDAMENTALES EN LA INVESTIGACIÓN TECNOLÓGICA. LA PRUEBA DIGITAL ILÍCITA . . . . .**

1.	DERECHO A LA INTIMIDAD . . . . .	99
1.1.	Protección de la intimidad como derecho fundamental . . . . .	99
1.1.1.	Contenido y destinatarios . . . . .	99
1.1.2.	Sobre la expectativa razonable de privacidad . . . . .	100
1.2.	La intimidad en la pareja y en la familia . . . . .	102
1.2.1.	Intimidad en la pareja . . . . .	102

1.2.2.	Intimidad del menor de edad en el ámbito familiar. . . . .	103
1.2.3.	Uso familiar compartido de un equipo informático . . . . .	104
1.3.	Derecho a la intimidad en la sociedad de la información. . . . .	105
1.3.1.	Dispositivos electrónicos . . . . .	105
1.3.2.	Actividades en Internet. . . . .	106
	A. Principio general . . . . .	106
	B. Inserción de contenidos en Internet. . . . .	106
	C. Datos de navegación web . . . . .	107
1.4.	Requisitos para la injerencia . . . . .	109
2.	SECRETO DE LAS COMUNICACIONES . . . . .	109
2.1.	Sobre el derecho al secreto de comunicaciones. . . . .	109
2.1.1.	Concepto . . . . .	109
2.1.2.	Elementos del proceso de comunicación . . . . .	111
	A. Transmisión de información o contenido. . . . .	111
	B. Entre dos o más personas determinadas o determinables. . . . .	111
	C. Intermediación de tercero con obligación de confidencialidad. . . . .	112
2.2.	Datos asociados a comunicaciones electrónicas (DA-CE) . . . . .	114
2.2.1.	Sobre los datos externos de la comunicación . . . . .	114
2.2.2.	Datos externos en las fases del proceso comunicativo . . . . .	115
	A. Acceso a datos externos cuando la comunicación aún no se ha iniciado . . . . .	115
	B. Acceso a los datos externos de la comunicación cuando ésta está teniendo lugar. . . . .	115
	C. Acceso a datos externos de la comunicación cuando ésta ha terminado. . . . .	115
2.2.3.	Conservación de datos por operadoras . . . . .	117
2.3.	El secreto de comunicaciones en la prueba digital. . . . .	117
2.4.	Secreto de comunicaciones en procesos de comunicación por redes . . . . .	118
2.4.1.	Obtención por uno de los comunicantes . . . . .	118
	A. Conversación desvelada por uno de los comunicantes. . . . .	119

	B.	Grabación subrepticia de la propia conversación . . . . .	119
	C.	Comentario de la Sentencia Sala de lo Civil del Tribunal Supremo 678/2014 . . . . .	120
2.4.2.		Obtención por tercero no partícipe en la comunicación . . . . .	122
2.5.		Secreto de comunicaciones en la obtención de datos contenidos en dispositivos electrónicos . . . . .	123
2.5.1.		Planteamiento general: fases del proceso de comunicación a través de una red . . . . .	124
2.5.2.		Especial consideración de los procesos de comunicación terminados o consumados . . . . .	125
2.5.3.		Mensajes que se encuentran en poder del emisor . . . . .	128
2.6.		Restricción del secreto a las comunicaciones . . . . .	128
3.		<b>DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS PERSONALES RECONOCIDO EN EL ART. 18.4 CE . . . . .</b>	<b>129</b>
3.1.		El derecho fundamental del art. 18.4 CE . . . . .	129
3.2.		Regulación . . . . .	131
3.2.1.		Unión Europea . . . . .	131
3.2.2.		Normativa aplicable . . . . .	131
	A.	Reglamento 2016/679 . . . . .	131
	B.	Directiva 2016/680 . . . . .	132
	C.	Decreto-Ley 2018 . . . . .	132
3.3.		Licitud del tratamiento . . . . .	132
3.4.		Incorporación de datos personales al proceso judicial . . . . .	133
3.4.1.		Planteamiento general . . . . .	133
3.4.2.		Fuentes de la normativa de protección de datos en los procesos judiciales . . . . .	135
3.4.3.		Licitud del tratamiento de datos en un proceso judicial . . . . .	137
3.4.4.		La prueba digital con violación del derecho del artículo 18.4 CE . . . . .	139
3.5.		Protección de datos personales en el proceso penal . . . . .	140
3.5.1.		Planteamiento general y fuentes normativas . . . . .	140
3.5.2.		Principios aplicables al tratamiento de datos en el ámbito penal . . . . .	143
3.5.3.		Datos especialmente sensibles . . . . .	146
3.5.4.		Obtención del dato . . . . .	147
	A.	Aportación por la parte al proceso . . . . .	147
	B.	Obtención o recogida por el poder público . . . . .	147

3.5.5.	Cesión de datos personales en la investigación y prueba de los delitos . . . . .	150
	A. Legitimidad de la cesión . . . . .	150
	B. Obligatoriedad de la cesión de datos. . . . .	151
	C. Régimen jurídico de la cesión del dato. . . . .	151
3.5.6.	Categorías de interesados en el proceso . . . . .	152
3.5.7.	Protección de datos en la Orden Europea de Investigación . . . . .	153
3.6.	Tratamiento de los ficheros policiales . . . . .	154
	A. Categorías . . . . .	154
	B. Régimen jurídico especial de los ficheros policiales . . . . .	155
3.7.	Técnicas de análisis automatizado de datos y decisiones automatizadas: Big Data . . . . .	157
	3.7.1. Cruce y contraste de datos personales . . . . .	159
	3.7.2. Mecanismo de decisión individual automatizado y elaboración de perfiles . . . . .	160
3.8.	Delegado de protección de datos . . . . .	161
3.9.	Protección de datos personales en el ámbito laboral . . . . .	162
	3.9.1. Planteamiento general . . . . .	162
	3.9.2. Uso de las TIC para la función de control empresarial. . . . .	165
4.	LA PRUEBA DIGITAL ILÍCITA: RÉGIMEN JURÍDICO . . . . .	169
4.1.	Concepto y consecuencias de la prueba ilícita . . . . .	169
	4.1.1. Exclusionary rule en el Tribunal Supremo de EEUU. . . . .	170
	4.1.2. Sistema español . . . . .	171
	A. Nulidad de la prueba. . . . .	171
	B. Cauce procesal de la nulidad. . . . .	172
4.2.	Efectos sobre las pruebas derivadas: sobre la conexión de antijuridicidad . . . . .	175
	4.2.1. Regla general: nulidad . . . . .	175
	4.2.2. Excepción: validez de las pruebas derivadas carentes de conexión de antijuridicidad . . . . .	175
	A. Falta de conexión natural . . . . .	175
	B. Falta de conexión de antijuridicidad . . . . .	175
4.3.	Aportación al proceso de pruebas ilícitas obtenidas por un particular . . . . .	179
	4.3.1. Planteamiento general . . . . .	179
	4.3.2. Proceso penal. . . . .	180
	A. Gradación de la violación . . . . .	180
	B. Relación con la actividad del Estado . . . . .	181

4.3.3.	Algunos casos concretos abordados por la jurisprudencia penal. . . . .	182
<b>CAPÍTULO 3. PRINCIPALES MODALIDADES DE FUENTES DE LA PRUEBA DIGITAL. . . . .</b>		<b>185</b>
	INTRODUCCIÓN AL CAPÍTULO . . . . .	187
1.	CORREO ELECTRÓNICO. . . . .	187
1.1.	Concepto y funcionamiento . . . . .	187
1.2.	La prueba del mail en el proceso. . . . .	188
1.2.1.	Contenido del mail. . . . .	189
1.2.2.	Otros datos. . . . .	189
1.2.3.	Acceso a información de servidores . . . . .	189
1.2.4.	Acceso a información de los dispositivos del emisor y/o del receptor. . . . .	191
1.2.5.	Incorporación al proceso y valoración judicial. . . . .	193
1.3.	Afectación de derechos fundamentales . . . . .	193
1.3.1.	Acceso al mail antes de iniciado el proceso de comunicación . . . . .	193
A.	Mensaje en poder del emisor que no ha sido enviado . . . . .	193
B.	Software de control remoto . . . . .	194
1.3.2.	Acceso durante el proceso de comunicación . . . . .	194
1.3.3.	Acceso al mail una vez finalizado el proceso de comunicación . . . . .	195
A.	Datos conservados por operadoras . . . . .	195
B.	Contenidos de mails almacenados por la operadora . . . . .	195
C.	Datos contenidos en dispositivos electrónicos. . . . .	196
2.	SMS . . . . .	196
2.1.	Concepto y funcionamiento . . . . .	196
2.2.	Problemas en la prueba del SMS . . . . .	197
3.	WHATSAPP Y OTROS SISTEMAS DE MENSAJERÍA INSTANTÁNEA . . . . .	199
3.1.	Sobre el WhatsApp . . . . .	199
3.1.1.	Notas características. . . . .	199
3.1.2.	Información útil para el proceso penal . . . . .	200
A.	Datos de tráfico generados durante la conversación de WhatsApp. . . . .	200

	B. Contenido de la conversación de WhatsApp . . . . .	200
3.2.	Incorporación al proceso: medio probatorio utilizado	201
3.3.	Una visión práctica de la prueba del WhatsApp . . . .	201
	3.3.1. Peligros de manipulación o de suplantación	201
	3.3.2. La elección del medio probatorio . . . . .	202
	3.3.3. Autoría del mensaje por el titular de la línea . . . . .	204
	3.3.4. Conclusión . . . . .	204
3.4.	Un ejemplo práctico . . . . .	204
3.5.	Estado del WhatsApp . . . . .	208
4.	LAS REDES SOCIALES. . . . .	209
	4.1. Concepto y clases . . . . .	209
	4.1.1. De la Web 1.0 a la Web 2.0. Delimitación conceptual . . . . .	209
	4.1.2. Modalidades . . . . .	211
	4.1.3. Probática y redes sociales . . . . .	212
	4.2. Investigación y prueba de actos ilícitos en redes sociales . . . . .	212
	4.2.1. Investigación de la huella digital: volatilidad . . . . .	213
	4.2.2. Investigación del autor de un contenido ilícito . . . . .	214
	4.2.3. Localización de empresa prestadora del servicio fuera de España . . . . .	215
	4.2.4. Derechos fundamentales afectados . . . . .	216
	4.3. Información obtenida en redes sociales para la prueba en cualquier proceso . . . . .	217
5.	OTROS ELEMENTOS WEB . . . . .	218
	5.1. Página web . . . . .	218
	5.1.1. Concepto y notas características . . . . .	218
	5.1.2. Derechos fundamentales afectados en el acceso a una página web . . . . .	219
	5.1.3. Prueba de una página web . . . . .	219
	5.2. Navegación por Internet . . . . .	220
<b>CAPÍTULO 4. PRUEBA DIGITAL EN LOS PROCESOS CIVIL Y CONTENCIOSO-ADMINISTRATIVO . . . . .</b>		<b>223</b>
1.	PLANTEAMIENTO GENERAL DEL CAPÍTULO . . . . .	225
2.	LA PRUEBA ELECTRÓNICA EN EL PROCESO CIVIL . . . . .	225
	2.1. Fase de obtención . . . . .	226

2.1.1.	Acceso a los datos. Información digital en poder de otro . . . . .	226
2.1.2.	Diligencias preliminares . . . . .	227
2.1.3.	Diligencias preliminares para la obtención de datos en propiedad intelectual o industrial. . . . .	229
2.1.4.	Deber de exhibición documental . . . . .	230
	A. Entre partes . . . . .	230
	B. Por terceros . . . . .	231
	C. Por entidades oficiales. . . . .	231
2.1.5.	Medidas de aseguramiento de la prueba. . . . .	232
2.1.6.	Medidas cautelares. . . . .	232
2.1.7.	Art. 336.5 LEC . . . . .	233
2.2.	La prueba digital ilícita en el proceso civil. . . . .	233
2.2.1.	Licitud . . . . .	233
2.2.2.	Nulidad de la prueba ilícita . . . . .	235
2.3.	Fase de Incorporación al proceso a través de distintos medios probatorios . . . . .	236
2.3.1.	El medio probatorio regulado en el art. 299.2 LEC. . . . .	236
2.3.2.	Documento electrónico; procedimiento probatorio en el proceso civil. . . . .	238
	A. Proposición . . . . .	239
	B. Práctica . . . . .	239
	C. Valoración de la prueba . . . . .	240
2.4.	La prueba de la contratación electrónica. . . . .	241
2.4.1.	Consideraciones generales . . . . .	241
2.4.2.	Contrato bancario electrónico . . . . .	243
2.5.	Procesos concursales: restricción de derechos fundamentales del concursado . . . . .	244
3.	LA PRUEBA ELECTRÓNICA EN EL PROCEDIMIENTO CONTENCIOSO-ADMINISTRATIVO . . . . .	245
3.1.	Licitud de la prueba electrónica . . . . .	245
3.2.	Incorporación al proceso: Procedimiento probatorio . . . . .	246
3.3.	Documento electrónico: Aplicación subsidiaria del régimen de la Ley de Enjuiciamiento Civil. . . . .	246
3.4.	Medios electrónicos en el procedimiento administrativo . . . . .	247
3.4.1.	Expediente administrativo electrónico: remisión a la jurisdicción contenciosa-administrativa. . . . .	247
3.4.2.	Documento administrativo electrónico. Copias electrónicas. . . . .	248

<b>CAPÍTULO 5. INVESTIGACIÓN Y PRUEBA DIGITAL EN EL PROCESO LABORAL</b> .....	251
1. LA PRUEBA ELECTRÓNICA EN EL PROCESO LABORAL . . . .	253
1.1. El entorno digital de la relación laboral .....	253
1.2. Fase de obtención: derechos fundamentales en el proceso laboral .....	254
1.2.1. Ámbitos afectados .....	254
1.2.2. Derechos fundamentales en el uso de medios informáticos proporcionados por la empresa al trabajador .....	255
1.2.3. Resumen de la STC 170/2013, de 7 de octubre. ....	258
1.2.4. Nulidad de la prueba electrónica ilícita en el proceso laboral. ....	261
1.3. Fase de Incorporación al proceso a través de distintos medios probatorios .....	263
1.4. Fase de valoración de la prueba electrónica .....	264
2. REGISTRO DE DISPOSITIVOS INFORMÁTICOS O ELECTRÓNICOS DEL TRABAJADOR. ....	264
2.1. Contenidos ajenos al ámbito personal del trabajador. ....	265
2.1.1. Principio general .....	265
2.1.2. Las búsquedas ciegas y las técnicas heurísticas .....	265
2.2. Contenidos propios del ámbito personal del trabajador .....	267
2.2.1. Consentimiento del trabajador .....	267
2.2.2. Supuestos particulares destacables .....	269
A. Reparación por técnico informático. .	269
B. Empleo de ordenador ajeno. ....	269
C. Ordenador del trabajador no protegido por contraseña .....	269
2.2.3. Ejercicio de las facultades de control empresarial de los medios facilitados para la prestación del trabajo .....	270
A. Principio general .....	270
B. Supuestos en los que el empresario puede realizar el registro del equipo informático o dispositivo electrónico del trabajador .....	271
C. Principio de proporcionalidad .....	273

	D.	Debate jurisprudencial sobre el deber de la empresa de informar a los trabajadores de los controles instaurados. .	274
	E.	BYOD (Bring your Own Device) . . . .	276
3.		COMUNICACIONES ELECTRÓNICAS DEL TRABAJADOR. . .	277
	3.1.	Contenido de la comunicación . . . . .	277
	3.2.	Relación con el proceso penal. . . . .	282
		3.2.1. Análisis del caso concreto . . . . .	282
		A. Jurisdicción social . . . . .	282
		B. Jurisdicción penal . . . . .	283
		3.2.2. Cuestiones planteadas desde la dimensión penal . . . . .	285
	3.3.	Datos externos de la comunicación. . . . .	287
4.		USO DE INTERNET POR EL TRABAJADOR . . . . .	288
	4.1.	Navegación por Internet . . . . .	288
	4.2.	El trabajador en las redes sociales . . . . .	289
		4.2.1. Prueba de la autoría . . . . .	290
		4.2.2. Derechos fundamentales afectados. . . . .	290
		A. Comunicación en canal cerrado . . . .	290
		B. Fuentes abiertas. . . . .	290
5.		USO DE CÁMARAS DE VIDEOVIGILANCIA EN LA EMPRESA	291
	5.1.	Derecho a la protección de datos . . . . .	292
		5.1.1. No necesidad de consentimiento . . . . .	292
		5.1.2. Plena aplicación del deber de información. . . . .	292
		5.1.3. Calidad de datos y principio de proporcionalidad. . . . .	294
	5.2.	Derecho a la intimidad: principio de proporcionalidad . . . . .	295
<b>CAPÍTULO 6. CIBERDELINCUENCIA E INVESTIGACIÓN TECNOLÓGICA EN EL PROCESO PENAL . . . . .</b>			<b>297</b>
1.		DOBLE ÁMBITO DE LA INVESTIGACIÓN TECNOLÓGICA EN EL PROCESO PENAL. . . . .	299
2.		LA CIBERDELINCUENCIA . . . . .	300
	2.1.	Concepto: de los delitos informáticos a los delitos en redes informáticas . . . . .	300
	2.2.	Notas características de los ciberdelitos. . . . .	300
		2.2.1. Facilidad de comisión . . . . .	300
		2.2.2. Alta capacidad de lesión . . . . .	301
		2.2.3. Elevada impunidad. . . . .	302
		2.2.4. Dificultades de investigación y prueba . . . .	303
		2.2.5. Necesidad de colaboración público/privada	304

	2.2.6.	Conclusión: disposición de medios adecuados por el sistema penal . . . . .	304
	2.3.	La ciberdelincuencia en España. . . . .	305
	2.4.	¿Prioridades en la lucha contra la ciberdelincuencia? . . . . .	306
3.		PRINCIPALES ÁMBITOS DE LA CIBERDELINCUENCIA . . . . .	307
	3.1.	Delitos contra la integridad, confidencialidad y disponibilidad de datos, equipos o sistemas informáticos . . . . .	307
	3.1.1.	Acceso ilegal a los sistemas de información . . . . .	307
	3.1.2.	Interferencia ilegal en los sistemas de información. . . . .	308
	3.1.3.	Interceptación ilegal. . . . .	308
	3.1.4.	Punibilidad de ciertas formas preparatorias de determinados ciberdelitos . . . . .	308
	3.2.	Estafas y fraudes cometidos a través de la web. . . . .	309
	3.3.	Delitos de contenido: creación, publicación y distribución de contenidos que sean constitutivos de delito. . . . .	310
	3.4.	Delitos contra la propiedad intelectual e industrial . . . . .	311
4.		LIBERTAD DE EXPRESIÓN Y DELITO EN LA SOCIEDAD DE LA INFORMACIÓN . . . . .	313
	4.1.	Libertad de expresión y de información en Internet . . . . .	313
	4.2.	Límites a la libertad de expresión en la web . . . . .	314
	4.3.	Delitos contra el honor . . . . .	314
	4.4.	Delitos de odio . . . . .	317
	4.4.1.	Delimitación conceptual: Hate Crime . . . . .	317
	4.4.2.	Conductas punibles . . . . .	318
	4.4.3.	Ciberodio . . . . .	319
	4.4.4.	Protocolo sobre penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos . . . . .	320
5.		LA USURPACIÓN DE LA IDENTIDAD VIRTUAL . . . . .	320
	5.1.	Análisis de los diferentes supuestos . . . . .	321
	5.2.	Utilización de datos de la víctima . . . . .	321
	5.3.	Delito de usurpación del estado civil. . . . .	323
	5.4.	Comunicación al administrador de la red social . . . . .	324
6.		VIOLENCIA DE GÉNERO COMETIDA A TRAVÉS DE MEDIOS TECNOLÓGICOS DE INFORMACIÓN Y DE COMUNICACIÓN . . . . .	325
	6.1.	Notas características . . . . .	325
	6.1.1.	Gravedad del fenómeno. . . . .	325
	6.1.2.	Delitos mediante instrumentos tecnológicos de comunicación . . . . .	327
	6.2.	Delitos contra la intimidad en la pareja. . . . .	328

6.2.1.	La intimidad en la pareja . . . . .	328
	A. Consideraciones generales. . . . .	328
	B. Análisis de la STS 872/2001. . . . .	328
	C. Consentimiento y expectativa razonable de privacidad. . . . .	329
	D. Utilización de datos de intimidad compartida . . . . .	330
6.2.2.	<i>Hacking</i> : espionaje dentro de la pareja. . . . .	331
6.2.3.	Delito de descubrimiento y revelación de secretos . . . . .	332
	A. Descubrimiento de secretos documentales . . . . .	332
	B. Instrumentos para interceptar comunicaciones o para grabar imagen y/o sonido. . . . .	333
	C. Tutela penal de los datos personales en soporte electrónico. . . . .	336
6.2.4.	<i>Sexting</i> . . . . .	338
	A. Concepto. . . . .	338
	B. Respuesta penal. . . . .	339
6.2.5.	<i>Sextorsión</i> . . . . .	342
	A. Concepto. . . . .	342
	B. Respuesta penal. . . . .	343
6.3.	Ciberacoso en la pareja . . . . .	345
	6.3.1. Características . . . . .	345
	6.3.2. Criminalización del acoso . . . . .	345
	6.3.3. Modalidades del ciberacoso en la pareja . . . . .	346
6.4.	<i>Cyberstalking</i> . . . . .	347
	6.4.1. Concepto: acecho a través de medios telemáticos. . . . .	347
	6.4.2. Respuesta penal . . . . .	347
	A. Art. 172 ter CP: tipo básico . . . . .	347
	B. Acoso en violencia de género . . . . .	350
6.5.	<i>Cyberbullying</i> . . . . .	352
	6.5.1. Delimitación conceptual: acoso moral o psicológico. . . . .	352
	6.5.2. <i>Cyberbullying</i> en violencia de género. . . . .	353
	6.5.3. Respuesta penal al <i>cyberbullying</i> . . . . .	355
	6.5.4. Delito de maltrato habitual y medios digitales de comunicación . . . . .	355
6.6.	Una reflexión final sobre la e-violencia de género. . . . .	356

<b>CAPÍTULO 7. RÉGIMEN JURÍDICO COMÚN DE LAS MEDIDAS DE INVESTIGACIÓN TECNOLÓGICA</b> .....	<b>359</b>
1. FUENTES DE LAS MEDIDAS DE INVESTIGACIÓN BASADAS EN TECNOLOGÍA DIGITAL .....	361
2. REGULACIÓN DE LA PRUEBA ELECTRÓNICA EN EL PROCESO PENAL .....	362
2.1. Fases .....	362
2.1.1. Fase de obtención de prueba .....	362
2.1.2. Fase de incorporación al proceso .....	362
2.1.3. Fase de valoración judicial de la prueba. . .	363
2.2. Reforma 2015 de la Ley de Enjuiciamiento Criminal .	363
3. RÉGIMEN JURÍDICO DE LAS MEDIDAS DE INVESTIGACIÓN TECNOLÓGICA RESTRINGIDAS DE DERECHOS FUNDAMENTALES .....	364
3.1. Principios rectores .....	364
3.2. Sobre el principio de proporcionalidad .....	366
3.3. Procedimiento de adopción .....	367
3.3.1. Inicio .....	367
3.3.2. Audiencia del Ministerio Fiscal .....	368
3.3.3. Decisión judicial .....	368
A. Existencia de indicios suficientes . . .	370
B. Idoneidad .....	371
C. Necesidad (subsidiariedad) .....	371
D. Gravedad de la conducta investigada. Proporcionalidad en sentido estricto .	371
3.3.4. La ecuación de la proporcionalidad .....	372
3.3.5. Motivación .....	373
3.4. Ejecución de la medida .....	374
3.4.1. Pieza separada y secreta .....	374
3.4.2. Duración .....	374
3.4.3. Control judicial de la medida .....	375
A. Auto autorizante .....	376
B. Control durante la duración de la medida .....	376
C. Control <i>ex post</i> por el órgano judicial sentenciador .....	376
3.4.4. Utilización de la información en otro procedimiento distinto .....	377
3.4.5. Hallazgos casuales .....	378
3.4.6. Cese de la medida .....	380
3.4.7. Destrucción de los registros .....	380

4.	TRATAMIENTO DE LA PRUEBA ELECTRÓNICA ILÍCITA EN EL PROCESO PENAL .....	381
4.1.	Procedimiento abreviado, juicio rápido y proceso penal de menores .....	381
4.2.	Proceso ante tribunal de jurado .....	381
4.3.	Proceso ordinario por delito y juicio por delito leve ..	382
<b>CAPÍTULO 8. REGISTRO DE DISPOSITIVOS Y REGISTROS REMOTOS.....</b>		<b>383</b>
1.	OBTENCIÓN DE LA PRUEBA DIGITAL EN LA INVESTIGACIÓN DEL DELITO: DATOS CONTENIDOS EN DISPOSITIVOS ELECTRÓNICOS.....	385
1.1.	Entorno digital o virtual .....	385
1.2.	Principio de legalidad .....	388
2.	NOTAS GENERALES DE LA NUEVA REGULACIÓN DEL REGISTRO DE DISPOSITIVOS .....	389
2.1.	Objeto: registro de dispositivos en la investigación de delitos .....	389
2.1.1.	Registro .....	389
2.1.2.	Dispositivos .....	389
2.1.3.	En la investigación de delitos .....	390
2.2.	Aprehensión/registro .....	391
2.3.	Modalidades .....	391
2.4.	Licitud del acceso a dispositivos electrónicos .....	392
3.	ACCESO A DATOS CONTENIDOS EN DISPOSITIVOS APREHENDIDOS .....	393
3.1.	Supuesto ordinario: autorización judicial .....	393
3.2.	Supuesto extraordinario: intervención policial urgente.....	394
3.2.1.	Presupuestos.....	394
3.2.2.	Ratificación o revocación judicial .....	396
3.3.	Consentimiento del afectado .....	397
3.3.1.	Consentimiento en el acceso a dispositivos .....	397
3.3.2.	Requisitos del consentimiento .....	397
4.	APREHENSIÓN DE DISPOSITIVO FUERA DE DOMICILIO ..	398
5.	REGISTRO DEL SISTEMA INFORMÁTICO QUE SE ENCUENTRA EN LUGAR CERRADO .....	400
5.1.	Régimen de la entrada y registro en lugar cerrado ..	400
5.2.	Registro del dispositivo .....	402
6.	REGISTRO DE DATOS ALMACENADOS EN LA NUBE .....	403
6.1.	Modalidades: servidores internos y externos .....	404

6.2.	Régimen jurídico del registro de información accesible. ....	407
7.	REGISTROS REMOTOS. TROYANOS. ....	408
7.1.	Concepto y utilidad para la investigación. ....	408
7.2.	Régimen jurídico. ....	408
7.3.	Objeto. ....	409
7.3.1.	Acceso a distancia. ....	409
7.3.2.	Modalidades. ....	410
	A. Datos de identificación y códigos. ....	410
	B. Instalación de <i>software</i> . Troyanos. ....	410
	C. <i>Keylogger</i> . ....	411
7.4.	Presupuestos. ....	412
8.	REGISTROS TRANSFRONTERIZOS. ....	413
8.1.	Fuente abierta. Consentimiento. ....	413
8.2.	Cooperación judicial internacional. ....	414
9.	CLAVES DE ACCESO Y DEBER DE COLABORACIÓN. ....	415
9.1.	¿Existe obligación de colaborar? ....	415
9.2.	Régimen jurídico de esta obligación tras la reforma de la LECRIM 2015. ....	415
9.2.1.	Registros de dispositivos de almacenamiento. ....	415
9.2.2.	Registros remotos. ....	417
10.	PRESERVACIÓN Y COPIA DE LOS DATOS. ....	418
10.1.	Cadena de custodia en el registro de dispositivos. ....	418
10.2.	Volcado o copia de los datos. ....	420
<b>CAPÍTULO 9. INTERCEPTACIÓN DE COMUNICACIONES TELE-MÁTICAS. INVESTIGACIONES EN INTERNET. ....</b>		<b>423</b>
1.	PROCEDIMIENTO DE INTERCEPTACIÓN DE LAS COMUNI-CACIONES. ....	425
1.1.	Presupuestos. ....	425
1.2.	Necesaria autorización judicial. ....	426
1.3.	Comunicaciones en tiempo real. ....	426
1.4.	Procedimiento de interceptación de comunicaciones. ....	427
1.4.1.	Ámbito subjetivo. ....	427
	A. Sujeto activo. ....	427
	B. Sujetos pasivos. ....	427
	C. Utilización maliciosa por terceros. Routers. Ordenadores zombies. ....	428
1.4.2.	Ámbito objetivo. ....	429
	A. ¿Qué delitos pueden ser investigados? ....	429

	B.	¿Qué dispositivos pueden ser intervenidos? . . . . .	429
	C.	¿A qué información puede accederse? . . . . .	429
1.4.3.		Procedimiento . . . . .	430
	A.	Solicitud de autorización judicial . . . . .	430
	B.	Requisitos temporales . . . . .	430
1.4.4.		Ejecución de la medida . . . . .	431
1.4.5.		Acceso de las partes a las grabaciones . . . . .	432
	A.	Entrega de la integridad . . . . .	432
	B.	Entrega de una parte . . . . .	432
1.4.6.		Notificación a terceros afectados que no sean parte [art. 588 ter i)] . . . . .	433
	A.	Notificación . . . . .	433
	B.	Entrega de copia a instancia de persona afectada . . . . .	433
1.4.7.		Régimen de los hallazgos casuales . . . . .	433
2.		EJECUCIÓN DE LA MEDIDA DE INTERCEPTACIÓN: SITEL . . . . .	433
2.1.		Funcionamiento del sistema SITEL . . . . .	434
2.2.		Principales problemas de SITEL . . . . .	436
	2.2.1.	Capacidad para asegurar la coincidencia entre lo grabado en el DVD y las conversaciones mantenidas . . . . .	436
	2.2.2.	Riesgo de automatización y correspondiente extensión a todos los datos . . . . .	437
	2.2.3.	Destino de las grabaciones tras finalizar su utilización en el proceso: destrucción . . . . .	437
3.		DATOS ELECTRÓNICOS DE TRÁFICO O ASOCIADOS . . . . .	438
3.1.		Datos externos conservados y secretos de comunicaciones . . . . .	438
	3.1.1.	Distintas modalidades de datos conservados . . . . .	438
	3.1.2.	Régimen del art. 588 ter j) . . . . .	439
3.2.		Datos conservados al amparo de la Ley 25/2007 . . . . .	440
	3.2.1.	Relevancia y marco jurídico . . . . .	440
	3.2.2.	Régimen jurídico de la Ley 25/2007 . . . . .	441
	3.2.3.	Efectos de la STJUE de 8 de abril de 2014 . . . . .	442
	3.2.4.	Interpretación de la exigencia de delito grave . . . . .	444
	A.	Planteamiento del problema . . . . .	444
	B.	Postura personal . . . . .	445
	C.	STJUE de 8 de octubre de 2018 . . . . .	448
	D.	Algunos ejemplos en la práctica judicial . . . . .	449

3.3.	Averiguación policial del IMSI e IMEI . . . . .	451
3.3.1.	Notas definidoras . . . . .	451
3.3.2.	Derechos fundamentales afectados. . . . .	452
3.3.3.	Régimen jurídico tras la reforma de la LECRIM 2015. . . . .	454
3.4.	Datos de titularidad o identificación de un dispositivo . . . . .	456
3.5.	Obtención de las direcciones IP de equipos informáticos . . . . .	456
3.5.1.	La prueba de la autoría a través de IP. . . . .	456
	A. Conexiones dinámicas. . . . .	457
	B. Servidor Proxy . . . . .	458
	C. Conexiones wifi. . . . .	458
	D. Cibercafés . . . . .	458
	E. La tecnología NAT. . . . .	458
3.5.2.	Régimen del art. 588 ter k) LECRIM . . . . .	459
3.5.3.	Comunicaciones entre equipos informáticos. Datos conservados por las operadoras. . . . .	461
3.5.4.	Comunicación entre usuarios a través de una red P2P: rastros policiales . . . . .	462
3.6.	Orden de conservación de datos . . . . .	465
4.	OBTENCIÓN DE LA PRUEBA DIGITAL EN LA INVESTIGACIÓN DEL DELITO: INVESTIGACIONES POLICIALES EN INTERNET . . . . .	466
4.1.	Modalidades . . . . .	466
4.2.	Investigaciones en Internet: acceso a fuentes abiertas . . . . .	467
4.2.1.	Principio general . . . . .	467
4.2.2.	Uso de nickname supuesto. . . . .	468
4.2.3.	Rastros informáticos en redes P2P. . . . .	469
4.3.	Contactos con el investigado: infiltración policial en la web . . . . .	469
4.4.	El agente encubierto en Internet . . . . .	475
4.4.1.	Concepto y utilidad . . . . .	475
4.4.2.	Régimen jurídico . . . . .	475
4.4.3.	Ámbito objetivo: canales cerrados de comunicación . . . . .	476
4.4.4.	Ámbito objetivo: delitos que pueden ser investigados. . . . .	476
4.4.5.	Utilización de archivos ilícitos por el agente encubierto . . . . .	477
4.4.6.	Conversión de agente encubierto virtual en agente encubierto «físico» . . . . .	479

4.4.7.	Infraestructura de apoyo al agente encubierto virtual. . . . .	480
4.4.8.	Peligro de provocación delictiva . . . . .	480
4.4.9.	Grabación de encuentros . . . . .	481
4.5.	<i>Deep Web-Dark Net-Red Tor</i> . . . . .	481
<b>CAPÍTULO 10. OTROS MEDIOS DE INVESTIGACIÓN TECNOLÓGICA EN EL PROCESO PENAL . . . . .</b>		<b>483</b>
1.	CAPTACIÓN Y GRABACIÓN DE COMUNICACIONES ORALES DIRECTAS . . . . .	485
1.1.	Modalidades y derechos fundamentales . . . . .	485
1.1.1.	Utilización de dispositivos técnicos . . . . .	485
1.1.2.	Derechos fundamentales afectados. . . . .	486
1.2.	Régimen jurídico tras la reforma LECRIM 2015 . . . . .	487
1.2.1.	Objeto . . . . .	487
1.2.2.	Régimen de la autorización judicial . . . . .	487
	A. Presupuestos [art. 588 quater b)] . . . . .	487
	B. Contenido de la resolución judicial [art. 588 quater c)]. . . . .	488
	C. Exigencia de vinculación con encuentros concretos . . . . .	488
	D. Ejecución de la medida . . . . .	490
1.3.	Cuadro resumen de los supuestos de autorización judicial. . . . .	491
2.	CAPTACIÓN DE LA IMAGEN. . . . .	492
2.1.	Derechos fundamentales afectados. El derecho a la propia imagen . . . . .	492
2.2.	Obtención de imágenes por la Policía en sus funciones de prevención del delito . . . . .	493
2.3.	Obtención de imágenes por la Policía en sus funciones de investigación y prueba del delito . . . . .	495
2.3.1.	En espacios públicos . . . . .	495
2.3.2.	En espacios no públicos . . . . .	496
2.3.3.	Incorporación de las imágenes al proceso . . . . .	496
3.	CAPTACIÓN Y GRABACIÓN POR PARTICULARES. . . . .	497
3.1.	Grabación con cámara oculta . . . . .	497
3.1.1.	Doctrina del TC sobre reportajes periodísticos con cámara oculta en el proceso civil . . . . .	497
3.1.2.	Grabaciones con cámara oculta en el proceso penal . . . . .	498
3.1.3.	Doctrina jurisprudencial del Tribunal Supremo. . . . .	498

3.2.	Grabación subrepticia de conversación por interlocutor . . . . .	501
3.2.1.	Derecho al secreto de comunicaciones . . . . .	501
3.2.2.	Derecho a la intimidad . . . . .	502
3.2.3.	Derecho a no declarar contra sí mismo y a no declararse culpable . . . . .	503
3.2.4.	Derecho a un proceso con todas las garantías . . . . .	504
3.2.5.	Utilización por persona vinculada directa o indirectamente con el Estado: prueba ilícita . . . . .	505
4.	DISPOSITIVOS DE SEGUIMIENTO Y LOCALIZACIÓN . . . . .	505
4.1.	Concepto y modalidades de geolocalización . . . . .	505
4.1.1.	Geolocalización de dispositivos electrónicos de comunicación . . . . .	506
4.1.2.	Geolocalización mediante dispositivos de seguimiento y de localización (balizas) . . . . .	506
4.2.	Derechos fundamentales afectados en la utilización de mecanismos de seguimiento y localización . . . . .	507
4.3.	Normativa reguladora de la utilización de dispositivos de seguimiento y de localización en la LECRIM . . . . .	509
4.3.1.	Ámbito objetivo . . . . .	510
4.3.2.	Régimen ordinario: autorización y control judicial . . . . .	511
	A. Presupuestos . . . . .	511
	B. Descripción del medio técnico . . . . .	511
4.3.3.	Supuesto de urgencia policial con control judicial posterior . . . . .	511
4.3.4.	Duración de la medida . . . . .	512
4.3.5.	Ejecución de la medida . . . . .	512
	A. Instalación y explotación del mecanismo . . . . .	512
	B. Deber de colaboración . . . . .	512
	C. Custodia y destino de los soportes . . . . .	513
5.	PRISMÁTICOS Y DRONES . . . . .	513
5.1.	Observación del interior de un domicilio mediante el uso de prismáticos y similares . . . . .	513
5.2.	Drones . . . . .	515
6.	LA UTILIZACIÓN DE MEDIDAS TECNOLÓGICAS EN LA ACTIVIDAD DEL AGENTE ENCUBIERTO . . . . .	517
6.1.	Sobre la figura del agente encubierto . . . . .	517
6.1.1.	Concepto y régimen jurídico . . . . .	517
6.1.2.	Finalidad inmediata: proporcionar elementos de investigación . . . . .	518

6.2.	Medidas de investigación tecnológica limitativas de derechos fundamentales utilizadas en la actividad del agente encubierto . . . . .	519
6.3.	Grabaciones de la actividad del agente encubierto . . . . .	519
6.3.1.	Grabación de encuentros en los que participe el agente encubierto . . . . .	519
6.3.2.	Grabaciones en video. . . . .	521
6.3.3.	Entrada en domicilio por invitación . . . . .	522
6.4.	Medidas tecnológicas para la seguridad del agente encubierto . . . . .	524
<b>CAPÍTULO 11. LA DIMENSIÓN INTERNACIONAL DE LA PRUEBA DIGITAL . . . . .</b>		<b>525</b>
1.	DIMENSIÓN INTERNACIONAL DE LA INVESTIGACIÓN TECNOLÓGICA Y LA PRUEBA DIGITAL . . . . .	527
2.	COOPERACIÓN JUDICIAL INTERNACIONAL . . . . .	528
2.1.	Convenio de Budapest. . . . .	529
2.2.	Unión Europea . . . . .	529
3.	COOPERACIÓN POLICIAL INTERNACIONAL . . . . .	530
4.	PREVENCIÓN Y SOLUCIÓN DE CONFLICTOS DE JURISDICCIÓN EN LA CIBERDELINCUENCIA. . . . .	533
4.1.	Prevención de conflictos . . . . .	533
4.2.	Soluciones a un conflicto de jurisdicción . . . . .	534
<b>CAPÍTULO 12. COOPERACIÓN JUDICIAL INTERNACIONAL EN LA INVESTIGACIÓN TECNOLÓGICA Y PRUEBA DIGITAL . . . . .</b>		<b>537</b>
1.	LA COOPERACIÓN JUDICIAL PENAL SOBRE OBTENCIÓN DE LA PRUEBA DIGITAL . . . . .	539
1.1.	Intervención transfronteriza de comunicaciones . . . . .	539
1.1.1.	Fases . . . . .	539
1.1.2.	Unión Europea: Convenio de 29 de mayo de 2000, relativo a la asistencia judicial en materia penal entre los Estados miembros de la Unión Europea. . . . .	541
A.	Con asistencia técnica del Estado requerido (art. 18). . . . .	541
B.	Intervención por medio de proveedores de servicio . . . . .	541
C.	Sin asistencia técnica del Estado requerido . . . . .	541

1.1.3.	Directiva 2014/41/CE, sobre Orden Europea de Investigación Penal . . . . .	542
1.2.	Remisión por otro Estado de datos electrónicos o digitales relevantes para el proceso penal . . . . .	542
1.2.1.	Sistema del Convenio de Budapest . . . . .	542
	A. Asistencia mutua para medidas provisionales . . . . .	543
	B. Asistencia mutua para remisión de datos . . . . .	543
	C. Acceso transfronterizo a datos . . . . .	543
	D. Otras formas: obtención en tiempo real . . . . .	544
	E. Supuestos de urgencia . . . . .	544
1.2.2.	Unión Europea . . . . .	544
	A. Conservación rápida de datos . . . . .	544
	B. Remisión de los datos . . . . .	545
	C. Futura regulación . . . . .	545
1.3.	Información transmitida por servicios policiales extranjeros . . . . .	546
1.4.	Valor en España de la prueba electrónica internacional . . . . .	547
2.	PRUEBA ELECTRÓNICA Y COOPERACIÓN JUDICIAL INTERNACIONAL EN OTRAS JURISDICCIONES . . . . .	547
2.1.	Unión Europea . . . . .	548
2.2.	Instrumentos de cooperación en otros ámbitos territoriales . . . . .	548
3.	MECANISMOS PARA FACILITAR LA COOPERACIÓN JUDICIAL INTERNACIONAL . . . . .	548
3.1.	Instituciones . . . . .	548
3.2.	Catálogo de instrumentos web de apoyo a la asistencia judicial . . . . .	550
4.	COOPERACIÓN CON EEUU EN LA OBTENCIÓN DE DATOS PARA LA INVESTIGACIÓN Y PRUEBA DEL DELITO . . . . .	551
4.1.	Preservación de datos . . . . .	551
4.2.	Entrega de datos . . . . .	554
4.3.	Entrega de datos en supuestos de urgencia . . . . .	554
4.4.	Cloud Act . . . . .	554