

TEMAS

■ LA LEY

Investigación tecnológica y prueba digital en todas las jurisdicciones

Joaquín Delgado Martín

ÍNDICE SISTEMÁTICO

ABREVIATURAS.....	31
CAPÍTULO 1	
TEORÍA GENERAL DE LA PRUEBA DIGITAL: CONCEPTO, MODALIDADES Y FASES EN TODOS LOS PROCESOS JUDICIALES..	33
INTRODUCCIÓN: UNA TEORÍA GENERAL DE LA PRUEBA DIGITAL	35
1. SOBRE LA PRUEBA EN LA ERA DIGITAL.....	35
1.1. Justicia y sociedad de la información	35
1.2. La prueba de hechos en la sociedad de la información	38
1.3. Internet como fuente de prueba	39
2. DELIMITACIÓN CONCEPTUAL DE LA PRUEBA DIGITAL.....	40
2.1. Concepto de prueba digital	42
2.2. Fuente y medio de prueba en el ámbito digital.....	43
2.3. Modalidades	45
3. FASE DE OBTENCIÓN DE LA PRUEBA: LICITUD.....	47
3.1. Acceso a datos contenidos en dispositivos electrónicos	48
3.1.1. Obtención de datos por la parte procesal	48
3.1.2. Obtención de datos por la autoridad pública competente en el proceso penal	48
3.2. Acceso a datos transmitidos por redes de comunicación...	49
3.3. Derechos fundamentales afectados en las distintas formas de obtención de la prueba digital.....	50
4. FASE DE INCORPORACIÓN DE LA PRUEBA DIGITAL AL PROCESO	51

4.1.	Requisitos	51
4.2.	La prueba digital puede ser incorporada al juicio por diferentes medios de prueba	52
4.3.	Documental en soporte papel	54
4.4.	Documento electrónico	54
4.4.1.	Concepto	54
4.4.2.	Forma material de incorporación al proceso	55
4.4.3.	Admisión del documento electrónico como prueba en los procedimientos de todos los órdenes jurisdiccionales	56
4.4.4.	Régimen jurídico	57
4.4.5.	Modalidades de documento electrónico	58
A.	Documento electrónico público	58
B.	Documento electrónico «oficial»	58
C.	Documento electrónico privado	59
4.4.6.	Documento público notarial electrónico	59
A.	Copia autorizada electrónica	60
B.	Escritura matriz digital	60
C.	Constatación fehaciente de hechos relacionados con soportes informático (mediante hash)	61
4.4.7.	Registro de la Propiedad	61
4.4.8.	Documento electrónico «oficial»	62
4.4.9.	Facturas electrónicas	63
4.4.10.	Los «pantallazos»	64
4.5.	Prueba pericial	65
4.5.1.	Concepto y caracteres de la prueba pericial informática	65
4.5.2.	Modalidades de la pericial informática	68
4.5.3.	La cadena de custodia en la pericial informática ..	70
4.5.4.	Fases de la pericial informática	70
A.	Obtención de los datos (acceso a la información)	71
B.	Clonado de los datos y cálculo del hash	71
C.	Elaboración del informe pericial	73
D.	Presentación del dictamen pericial al tribunal	73
E.	Valoración de la pericial informática	74
4.6.	Reconocimiento judicial e inspección ocular	74
4.7.	Anticipación o preconstitución de la prueba	76

4.7.1.	Preconstitución extraprocésal de la prueba electrónica	76
4.7.2.	Anticipación de la prueba digital en el proceso	76
5.	VALORACIÓN DE LA PRUEBA DIGITAL	77
5.1.	Libre valoración de la prueba	78
5.1.1.	Regla general: libre valoración de la prueba electrónica	78
5.1.2.	Valoración de las distintas modalidades de documentos electrónicos	80
5.2.	Autenticidad e integridad de los datos	81
5.2.1.	Autenticidad	82
5.2.2.	Integridad	82
5.2.3.	Garantías de autenticidad e integridad	82
5.3.	Postura procesal de las partes	83
5.3.1.	Impugnación	83
5.3.2.	¿Reglas de distribución de la carga de la prueba? ..	84
5.4.	Valoración conjunta de la prueba	87
5.4.1.	Concepto	87
5.4.2.	Motivación de la valoración de la prueba	88
5.5.	Efectos de la firma electrónica	89
5.5.1.	Concepto	89
5.5.2.	Modalidades de la firma electrónica	91
5.5.3.	Valor probatorio de los documentos con firma electrónica	93
5.6.	Terceros de confianza: Prestadores de Servicio de Confianza	95
5.6.1.	Concepto y marco jurídico	95
5.6.2.	Nuevo panorama tras el Reglamento UE 910/2014 ..	96

CAPÍTULO 2

DERECHOS FUNDAMENTALES EN LA INVESTIGACIÓN TECNOLÓGICA. LA PRUEBA DIGITAL ILÍCITA	99
1. DERECHO A LA INTIMIDAD	101
1.1. Protección de la intimidad como derecho fundamental	101

1.1.1.	Contenido y destinatarios	101
1.1.2.	Sobre la expectativa razonable de privacidad	102
1.2.	La intimidad en la pareja y en la familia.....	104
1.2.1.	Intimidad en la pareja.....	104
1.2.2.	Intimidad del menor de edad en el ámbito familiar	105
1.3.	Derecho a la intimidad en la sociedad de la información..	106
1.3.1.	Dispositivos electrónicos	106
1.3.2.	Actividades en Internet	107
	A. Principio general.....	107
	B. Inserción de contenidos en Internet.....	108
	C. Datos de navegación web.....	109
1.4.	Requisitos para la injerencia	111
2.	SECRETO DE LAS COMUNICACIONES	111
2.1.	Sobre el derecho al secreto de comunicaciones.....	111
2.1.1.	Concepto.....	111
2.1.2.	Elementos del proceso de comunicación.....	112
	A. Transmisión de información o contenido	113
	B. Entre dos o más personas determinadas o determinables.....	113
	C. Intermediación de tercero con obligación de confidencialidad.....	114
2.2.	Datos asociados a comunicaciones electrónicas (DACE)...	116
2.2.1.	Sobre los datos externos de la comunicación.....	116
2.2.2.	Datos externos en las fases del proceso comunicativo	117
	A. Acceso a datos externos cuando la comunicación aún no se ha iniciado.....	117
	B. Acceso a los datos externos de la comunicación cuando ésta está teniendo lugar	117
	C. Acceso a datos externos de la comunicación cuando ésta ha terminado.....	117
	C.1. ¿Afecta al secreto de comunicaciones?	117
	C.2. ¿Afecta al derecho a la intimidad?.....	118
2.2.3.	Conservación de datos por operadoras	119

2.3.	El secreto de comunicaciones en la prueba digital	119
2.4.	Secreto de comunicaciones en procesos de comunicación por redes.....	120
2.4.1.	Obtención por uno de los comunicantes	120
	A. Conversación desvelada por uno de los comunicantes	121
	B. Grabación subrepticia de la propia conversación	121
	C. Comentario de la Sentencia Sala de lo Civil del Tribunal Supremo 678/2014	122
2.4.2.	Obtención por tercero no partícipe en la comunicación	124
2.5.	Secreto de comunicaciones en la obtención de datos contenidos en dispositivos electrónicos	125
2.5.1.	Planteamiento general: fases del proceso de comunicación a través de una red.....	126
2.5.2.	Especial consideración de los procesos de comunicación terminados o consumados.....	128
2.5.3.	Mensajes que se encuentran en poder del emisor	130
2.6.	Restricción del secreto a las comunicaciones.....	131
3.	DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS PERSONALES RECONOCIDO EN EL ART. 18.4 CE.....	131
3.1.	El derecho fundamental del art. 18.4 CE	132
3.2.	Incorporación de datos personales al proceso.....	134
3.3.	Obtención de datos personales con violación del derecho fundamental del art. 18.4 CE.....	135
3.3.1.	Obtención con consentimiento.....	135
3.3.2.	Cesión de datos a tercero.....	137
	A. Comunicación de datos a un tercero.....	137
	B. Comunicación de datos entre Administraciones Públicas.....	139
3.3.3.	Efectos de la obtención del dato con violación del derecho del art. 18.4 CE	139
3.4.	Tratamiento del dato obtenido	142
3.4.1.	Obligaciones para los responsables del tratamiento del dato	142

3.4.2. Tratamiento del dato y prueba electrónica.....	143
3.5. Protección de datos personales en el proceso penal.....	144
3.5.1. Obtención del dato.....	144
A. Aportación por la parte al proceso	144
B. Obtención o recogida por el poder público....	145
B.1. Consentimiento no necesario	145
B.2. Principio de proporcionalidad.....	145
3.5.2. Cesión de datos personales en la investigación y prueba de los delitos	146
A. Legitimidad de la cesión	146
B. Obligatoriedad de la cesión de datos	147
C. Régimen jurídico de la cesión del dato	147
D. Cruce y contraste de datos personales	148
3.5.3. Tratamiento de los ficheros de órganos judiciales.	150
3.5.4. Tratamiento de los ficheros policiales	150
A. Categorías.....	150
B. Régimen jurídico especial de los ficheros policiales	150
4. LA PRUEBA DIGITAL ILÍCITA: RÉGIMEN JURÍDICO.....	155
4.1. Concepto y consecuencias de la prueba ilícita.....	155
4.1.1. Exclusionary rule en el Tribunal Supremo de EEUU	156
4.1.2. Sistema español	157
A. Nulidad de la prueba	157
B. Cauce procesal de la nulidad	159
B.1. De oficio por el Juez	159
B.2. A instancia de parte procesal	159
4.2. Efectos sobre las pruebas derivadas: sobre la conexión de antijuridicidad	160
4.2.1. Regla general: nulidad	160
4.2.2. Excepción: validez de las pruebas derivadas carentes de conexión de antijuridicidad.....	161
A. Falta de conexión natural.....	161
B. Falta de conexión de antijuridicidad	161

CAPÍTULO 3

PRINCIPALES MODALIDADES DE FUENTES DE LA PRUEBA DIGITAL	165
INTRODUCCIÓN AL CAPÍTULO.....	167
1. CORREO ELECTRÓNICO	167
1.1. Concepto y funcionamiento.....	167
1.2. La prueba del mail en el proceso	168
1.2.1. Contenido del mail	169
1.2.2. Otros datos	169
1.2.3. Acceso a información de servidores.....	169
1.2.4. Acceso a información de los dispositivos del emisor y/o del receptor.....	171
1.2.5. Incorporación al proceso y valoración judicial	173
1.3. Afectación de derechos fundamentales	173
1.3.1. Acceso al mail antes de iniciado el proceso de comunicación	173
A. Mensaje en poder del emisor que no ha sido enviado.....	173
B. Software de control remoto.....	174
1.3.2. Acceso durante el proceso de comunicación.....	174
1.3.3. Acceso al mail una vez finalizado el proceso de comunicación.....	175
A. Datos conservados por operadoras.....	175
B. Contenidos de mails almacenados por la operadora	175
C. Datos contenidos en dispositivos electrónicos	176
C.1. Dispositivo electrónico del receptor.....	176
C.2. Dispositivo electrónico del emisor	176
2. SMS	176
2.1. Concepto y funcionamiento.....	176
2.2. Problemas en la prueba del SMS.....	177
3. WHATSAPP Y OTROS SISTEMAS DE MENSAJERÍA INSTANTÁNEA	179
3.1. Sobre el WhatsApp	179

3.1.1.	Notas características.....	180
3.1.2.	Información útil para el proceso penal.....	181
	A. Datos de tráfico generados durante la conversación de WhatsApp.....	181
	B. Contenido de la conversación de WhatsApp..	181
3.2.	Incorporación al proceso: medio probatorio utilizado.....	181
3.3.	Una visión práctica de la prueba del WhatsApp.....	182
	3.3.1. Peligros de manipulación o de suplantación.....	182
	3.3.2. La elección del medio probatorio	182
	3.3.3. Autoría del mensaje por el titular de la línea.....	184
	3.3.4. Conclusión	184
3.4.	Un ejemplo práctico	185
3.5.	Estado del WhatsApp.....	189
4.	LAS REDES SOCIALES.....	190
4.1.	Concepto y clases	190
	4.1.1. De la Web 1.0 a la Web 2.0. Delimitación conceptual	190
	4.1.2. Modalidades.....	191
	4.1.3. Probática y redes sociales	192
4.2.	Investigación y prueba de actos ilícitos en redes sociales..	193
	4.2.1. Investigación de la huella digital: volatilidad	194
	4.2.2. Investigación del autor de un contenido ilícito	195
	4.2.3. Localización de empresa prestadora del servicio fuera de España	196
	4.2.4. Derechos fundamentales afectados.....	197
4.3.	Información obtenida en redes sociales para la prueba en cualquier proceso	198
5.	OTROS ELEMENTOS WEB.....	199
5.1.	Página web	199
	5.1.1. Concepto y notas características	199
	5.1.2. Derechos fundamentales afectados en el acceso a una página web	200
	5.1.3. Prueba de una página web	200
5.2.	Navegación por Internet.....	202

CAPÍTULO 4

PRUEBA DIGITAL EN LOS PROCESOS CIVIL Y CONTENCIOSO-ADMINISTRATIVO.....	203	
1. PLANTEAMIENTO GENERAL DEL CAPÍTULO.....	205	
2. LA PRUEBA ELECTRÓNICA EN EL PROCESO CIVIL	205	
2.1. Fase de obtención.....	205	
2.1.1. Acceso a los datos. Información digital en poder de otro.....	206	
2.1.2. Diligencias preliminares	207	
2.1.3. Diligencias preliminares para la obtención de datos en propiedad intelectual o industrial	209	
2.1.4. Deber de exhibición documental	210	
	A. Entre partes	210
	B. Por terceros.....	211
	C. Por entidades oficiales	211
2.1.5. Medidas de aseguramiento de la prueba.....	211	
2.1.6. Medidas cautelares	212	
2.1.7. Art. 336.5 LEC.....	212	
2.2. La prueba digital ilícita en el proceso civil	213	
2.2.1. Licitud	213	
2.2.2. Nulidad de la prueba ilícita	214	
2.3. Fase de Incorporación al proceso a través de distintos medios probatorios.....	216	
2.3.1. El medio probatorio regulado en el art. 299.2 LEC	216	
2.3.2. Documento electrónico procedimiento probatorio en el proceso civil	217	
	A. Proposición.....	218
	B. Práctica.....	219
	C. Valoración de la prueba.....	220
2.4. La prueba de la contratación electrónica.....	220	
2.4.1. Consideraciones generales.....	220	
2.4.2. Contrato bancario electrónico	222	

2.5. Procesos concursales: restricción de derechos fundamentales del concursado	223
3. LA PRUEBA ELECTRÓNICA EN EL PROCEDIMIENTO CONTENCIOSO-ADMINISTRATIVO	225
3.1. Licitud de la prueba electrónica	225
3.2. Incorporación al proceso: Procedimiento probatorio.....	226
3.3. Documento electrónico: Aplicación subsidiaria del régimen de la Ley de Enjuiciamiento Civil	226
3.4. Medios electrónicos en el procedimiento administrativo...	227
3.4.1. Expediente administrativo electrónico: remisión a la jurisdicción contenciosa-administrativa	227
3.4.2. Documento administrativo electrónico. Copias electrónicas	228
CAPÍTULO 5	
INVESTIGACIÓN Y PRUEBA DIGITAL EN EL PROCESO LABORAL...	231
1. LA PRUEBA ELECTRÓNICA EN EL PROCESO LABORAL	233
1.1. El entorno digital de la relación laboral.....	233
1.2. Fase de obtención: derechos fundamentales en el proceso laboral	234
1.2.1. Ámbitos afectados	234
1.2.2. Derechos fundamentales en el uso de medios informáticos proporcionados por la empresa al trabajador	235
1.2.3. Resumen de la STC 170/2013, de 7 de octubre	237
1.2.4. Nulidad de la prueba electrónica ilícita en el proceso laboral	240
1.3. Fase de Incorporación al proceso a través de distintos medios probatorios.....	243
1.4. Fase de valoración de la prueba electrónica.....	244
2. REGISTRO DE DISPOSITIVOS INFORMÁTICOS O ELECTRÓNICOS DEL TRABAJADOR	244
2.1. Contenidos ajenos al ámbito personal del trabajador	245
2.1.1. Principio general	245
2.1.2. Las búsquedas ciegas y las técnicas heurísticas.....	245

2.2. Contenidos propios del ámbito personal del trabajador.....	247
2.2.1. Consentimiento del trabajador	248
2.2.2. Supuestos particulares destacables.....	249
A. Reparación por técnico informático	249
B. Empleo de ordenador ajeno	250
C. Ordenador del trabajador no protegido por contraseña	250
2.2.3. Ejercicio de las facultades de control empresarial de los medios facilitados para la prestación del trabajo	250
A. Principio general.....	250
B. Supuestos en los que el empresario puede realizar el registro del equipo informático o dispositivo electrónico del trabajador.....	251
C. Principio de proporcionalidad.....	253
D. Debate jurisprudencial sobre el deber de la empresa de informar a los trabajadores de los controles instaurados	255
E. BYOD (Bring your Own Device).....	256
3. COMUNICACIONES ELECTRÓNICAS DEL TRABAJADOR	258
3.1. Contenido de la comunicación	258
3.2. Relación con el proceso penal	262
3.2.1. Análisis del caso concreto	262
A. Jurisdicción social.....	262
B. Jurisdicción penal.....	263
3.2.2. Cuestiones planteadas desde la dimensión penal..	265
3.3. Datos externos de la comunicación	267
4. USO DE INTERNET POR EL TRABAJADOR	268
4.1. Navegación por Internet.....	268
4.2. El trabajador en las redes sociales	270
4.2.1. Prueba de la autoría.....	270
4.2.2. Derechos fundamentales afectados.....	270
A. Comunicación en canal cerrado	270
B. Fuentes abiertas.....	271

5.	USO DE CÁMARAS DE VIDEOVIGILANCIA EN LA EMPRESA...	272
5.1.	Derecho a la protección de datos.....	272
5.1.1.	No necesidad de consentimiento.....	272
5.1.2.	Plena aplicación del deber de información.....	273
5.1.3.	Calidad de datos y principio de proporcionalidad	274
5.2.	Derecho a la intimidad: principio de proporcionalidad	274

CAPÍTULO 6

CIBERDELINCUENCIA E INVESTIGACIÓN TECNOLÓGICA EN EL PROCESO PENAL.....

1.	DOBLE ÁMBITO DE LA INVESTIGACIÓN TECNOLÓGICA EN EL PROCESO PENAL.....	279
2.	LA CIBERDELINCUENCIA.....	280
2.1.	Concepto: de los delitos informáticos a los delitos en redes informáticas.....	280
2.2.	Notas características de los ciberdelitos	281
2.2.1.	Facilidad de comisión.....	281
2.2.2.	Alta capacidad de lesión.....	281
2.2.3.	Elevada impunidad	282
2.2.4.	Dificultades de investigación y prueba	283
2.2.5.	Necesidad de colaboración público/privada.....	284
2.2.6.	Conclusión: disposición de medios adecuados por el sistema penal	285
2.3.	La ciberdelincuencia en España	285
2.4.	¿Prioridades en la lucha contra la ciberdelincuencia?	287
3.	PRINCIPALES ÁMBITOS DE LA CIBERDELINCUENCIA	287
3.1.	Delitos contra la integridad, confidencialidad y disponibilidad de datos, equipos o sistemas informáticos.....	288
3.1.1.	Acceso ilegal a los sistemas de información	288
3.1.2.	Interferencia ilegal en los sistemas de información	288
3.1.3.	Interceptación ilegal	289
3.1.4.	Punibilidad de ciertas formas preparatorias de determinados ciberdelitos.....	289
3.2.	Estafas y fraudes cometidos a través de la web.....	290

3.3.	Delitos de contenido: creación, publicación y distribución de contenidos que sean constitutivos de delito	291
3.4.	Delitos contra la propiedad intelectual e industrial	292
4.	LIBERTAD DE EXPRESIÓN Y DELITO EN LA SOCIEDAD DE LA INFORMACIÓN.....	294
4.1.	Libertad de expresión y de información en Internet	294
4.2.	Límites a la libertad de expresión en la web.....	295
4.3.	Delitos contra el honor	295
4.4.	Delitos de odio	298
4.4.1.	Delimitación conceptual: Hate Crime.....	298
4.4.2.	Conductas punibles	299
4.4.3.	Ciberodio	300
4.4.4.	Protocolo sobre penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos	301
5.	LA USURPACIÓN DE LA IDENTIDAD VIRTUAL	302
5.1.	Análisis de los diferentes supuestos	302
5.2.	Utilización de datos de la víctima	303
5.3.	Delito de usurpación del estado civil	305
5.4.	Comunicación al administrador de la red social.....	306
6.	VIOLENCIA DE GÉNERO COMETIDA A TRAVÉS DE MEDIOS TECNOLÓGICOS DE INFORMACIÓN Y DE COMUNICACIÓN	307
6.1.	Notas características	307
6.1.1.	Gravedad del fenómeno	307
6.1.2.	Delitos mediante instrumentos tecnológicos de comunicación	309
6.2.	Delitos contra la intimidad en la pareja.....	310
6.2.1.	La intimidad en la pareja	310
A.	Consideraciones generales	310
B.	Análisis de la STS 872/2001	310
C.	Consentimiento y expectativa razonable de privacidad.....	311
D.	Utilización de datos de intimidad compartida	312
6.2.2.	Hacking: espionaje dentro de la pareja.....	313
6.2.3.	Delito de descubrimiento y revelación de secretos	314

A. Descubrimiento de secretos documentales.....	314
B. Instrumentos para interceptar comunicaciones o para grabar imagen y/o sonido.....	316
B.1. Interceptación de comunicaciones.....	316
B.2. Instrumentos para captación de imagen y/o sonidos	317
C. Tutela penal de los datos personales en soporte electrónico.....	318
6.2.4. Sexting	321
A. Concepto	321
B. Respuesta penal	322
6.2.5. Sextorsión.....	325
A. Concepto	325
B. Respuesta penal	325
6.3. Ciberacoso en la pareja.....	325
6.3.1. Características	325
6.3.2. Criminalización del acoso	326
6.3.3. Modalidades del ciberacoso en la pareja.....	327
6.4. Cyberstalking	327
6.4.1. Concepto: acecho a través de medios telemáticos	327
6.4.2. Respuesta penal.....	328
A. Art. 172 ter CP: tipo básico	328
B. Acoso en violencia de género	329
6.5. Cyberbullying	331
6.5.1. Delimitación conceptual: acoso moral o psicológico.....	331
6.5.2. Cyberbullying en violencia de género	332
6.5.3. Respuesta penal al cyberbullying.....	334
6.5.4. Delito de maltrato habitual y medios digitales de comunicación.....	335
6.6. Una reflexión final sobre la e-violencia de género	335

CAPÍTULO 7

RÉGIMEN JURÍDICO COMÚN DE LAS MEDIDAS DE INVESTIGACIÓN TECNOLÓGICA.....	337
1. FUENTES DE LAS MEDIDAS DE INVESTIGACIÓN BASADAS EN TECNOLOGÍA DIGITAL	339
2. REGULACIÓN DE LA PRUEBA ELECTRÓNICA EN EL PROCESO PENAL	340
2.1. Fases.....	340
2.1.1. Fase de obtención de prueba	340
2.1.2. Fase de incorporación al proceso	340
2.1.3. Fase de valoración judicial de la prueba.....	341
2.2. Reforma 2015 de la Ley de Enjuiciamiento Criminal.....	341
3. RÉGIMEN JURÍDICO DE LAS MEDIDAS DE INVESTIGACIÓN TECNOLÓGICA RESTRICTIVAS DE DERECHOS FUNDAMENTALES	342
3.1. Principios rectores.....	342
3.2. Sobre el principio de proporcionalidad	344
3.3. Procedimiento de adopción	345
3.3.1. Inicio.....	346
3.3.2. Audiencia del Ministerio Fiscal.....	346
3.3.3. Decisión judicial	346
A. Existencia de indicios suficientes	348
B. Idoneidad	349
C. Necesidad (subsidiariedad)	350
D. Gravedad de la conducta investigada. Proporcionalidad en sentido estricto	350
3.3.4. La ecuación de la proporcionalidad.....	351
3.3.5. Motivación	351
3.4. Ejecución de la medida.....	353
3.4.1. Pieza separada y secreta.....	353
3.4.2. Duración	353
3.4.3. Control judicial de la medida	354
A. Auto autorizante	355
B. Control durante la duración de la medida	355

C. Control ex post por el órgano judicial sentenciador	355
3.4.4. Utilización de la información en otro procedimiento distinto.....	356
3.4.5. Hallazgos casuales	357
3.4.6. Cese de la medida	358
3.4.7. Destrucción de los registros.....	358
4. TRATAMIENTO DE LA PRUEBA ELECTRÓNICA ILÍCITA EN EL PROCESO PENAL	359
4.1. Procedimiento abreviado, juicio rápido y proceso penal de menores.....	360
4.2. Proceso ante tribunal de jurado.....	360
4.3. Proceso ordinario por delito y juicio por delito leve.....	360
CAPÍTULO 8	
REGISTRO DE DISPOSITIVOS Y REGISTROS REMOTOS.....	361
1. OBTENCIÓN DE LA PRUEBA DIGITAL EN LA INVESTIGACIÓN DEL DELITO: DATOS CONTENIDOS EN DISPOSITIVOS ELECTRÓNICOS	363
1.1. Entorno digital o virtual.....	363
1.2. Principio de legalidad.....	366
2. NOTAS GENERALES DE LA NUEVA REGULACIÓN DEL REGISTRO DE DISPOSITIVOS.....	367
2.1. Objeto: registro de dispositivos en la investigación de delitos	367
2.1.1. Registro	367
2.1.2. Dispositivos	367
2.1.3. En la investigación de delitos.....	369
2.2. Aprehensión/registro	369
2.3. Modalidades	369
2.4. Licitud del acceso a dispositivos electrónicos.....	370
3. ACCESO A DATOS CONTENIDOS EN DISPOSITIVOS APREHENDIDOS.....	372
3.1. Supuesto ordinario: autorización judicial	372
3.2. Supuesto extraordinario: intervención policial urgente.....	372
3.2.1. Presupuestos.....	373

3.2.2. Ratificación o revocación judicial.....	375
3.3. Consentimiento del afectado.....	375
3.3.1. Consentimiento en el acceso a dispositivos	375
3.3.2. Requisitos del consentimiento	376
4. APREHENSIÓN DE DISPOSITIVO FUERA DE DOMICILIO.....	377
5. REGISTRO DEL SISTEMA INFORMÁTICO QUE SE ENCUENTRA EN LUGAR CERRADO.....	378
5.1. Régimen de la entrada y registro en lugar cerrado.....	378
5.2. Registro del dispositivo	380
6. REGISTRO DE DATOS ALMACENADOS EN LA NUBE.....	382
6.1. Modalidades: servidores internos y externos	382
6.2. Régimen jurídico del registro de información accesible.....	384
7. REGISTROS REMOTOS. TROYANOS	385
7.1. Concepto y utilidad para la investigación.....	385
7.2. Régimen jurídico.....	385
7.3. Objeto	386
7.3.1. Acceso a distancia	386
7.3.2. Modalidades.....	386
A. Datos de identificación y códigos	386
B. Instalación de software. Troyanos.....	387
C. Keylogger.....	388
7.4. Presupuestos	389
8. REGISTROS TRANSFRONTERIZOS.....	390
8.1. Fuente abierta. Consentimiento.....	391
8.2. Cooperación judicial internacional	391
9. CLAVES DE ACCESO Y DEBER DE COLABORACIÓN	392
9.1. ¿Existe obligación de colaborar?.....	392
9.2. Régimen jurídico de esta obligación tras la reforma de la LECRIM 2015	393
9.2.1. Registros de dispositivos de almacenamiento.....	393
9.2.2. Registros remotos.....	394
10. PRESERVACIÓN Y COPIA DE LOS DATOS	395

10.1. Cadena de custodia en el registro de dispositivos.....	396
10.2. Volcado o copia de los datos	397

CAPÍTULO 9

INTERCEPTACIÓN DE COMUNICACIONES TELEMÁTICAS. INVESTIGACIONES EN INTERNET.....	401
1. PROCEDIMIENTO DE INTERCEPTACIÓN DE LAS COMUNICACIONES.....	403
1.1. Presupuestos	403
1.2. Necesaria autorización judicial.....	404
1.3. Comunicaciones en tiempo real.....	404
1.4. Procedimiento de interceptación de comunicaciones	405
1.4.1. Ámbito subjetivo	405
A. Sujeto activo	405
B. Sujetos pasivos.....	405
C. Utilización maliciosa por terceros. Routers. Ordenadores zombies.....	406
1.4.2. Ámbito objetivo.....	407
A. ¿Qué delitos pueden ser investigados?	407
B. Qué dispositivos pueden ser intervenidos?	407
C. ¿A qué información puede accederse?	407
1.4.3. Procedimiento	408
A. Solicitud de autorización judicial.....	408
B. Requisitos temporales.....	408
1.4.4. Ejecución de la medida	409
1.4.5. Acceso de las partes a las grabaciones	410
A. Entrega de la integridad	410
B. Entrega de una parte	410
1.4.6. Notificación a terceros afectados que no sean parte [art. 588 ter i)].....	410
A. Notificación.....	410
B. Entrega de copia a instancia de persona afectada	411
1.4.7. Régimen de los hallazgos casuales	411

2. EJECUCIÓN DE LA MEDIDA DE INTERCEPTACIÓN: SITEL.....	411
2.1. Funcionamiento del sistema SITEL	412
2.2. Principales problemas de SITEL.....	413
2.2.1. Capacidad para asegurar la coincidencia entre lo grabado en el DVD y las conversaciones mantenidas.....	413
2.2.2. Riesgo de automatización y correspondiente extensión a todos los datos	414
2.2.3. Destino de las grabaciones tras finalizar su utilización en el proceso: destrucción	415
3. DATOS ELECTRÓNICOS DE TRÁFICO O ASOCIADOS	415
3.1. Datos externos conservados y secretos de comunicaciones.	415
3.1.1. Distintas modalidades de datos conservados	416
3.1.2. Régimen del art. 588 ter j)	416
3.2. Datos conservados al amparo de la Ley 25/2007	417
3.2.1. Relevancia y marco jurídico	417
3.2.2. Régimen jurídico de la Ley 25/2007	418
3.2.3. Efectos de la STJUE de 8 de abril de 2014.....	419
3.2.4. Interpretación de la exigencia de delito grave.....	420
A. Planteamiento del problema	420
B. Postura personal.....	422
C. Algunos ejemplos en la práctica judicial.....	425
3.3. Averiguación policial del IMSI e IMEI	427
3.3.1. Notas definidoras.....	427
3.3.2. Derechos fundamentales afectados.....	428
3.3.3. Régimen jurídico tras la reforma de la LECRIM 2015	430
3.4. Datos de titularidad o identificación de un dispositivo	431
3.5. Obtención de las direcciones IP de equipos informáticos..	432
3.5.1. La prueba de la autoría a través de IP	432
A. Conexiones dinámicas	433
B. Servidor Proxy.....	433
C. Conexiones wifi	433
D. Cybercafés.....	434
E. La tecnología NAT.....	434

3.5.2.	Régimen del art. 588 ter k) LECRIM	435
3.5.3.	Comunicaciones entre equipos informáticos. Datos conservados por las operadoras.....	436
3.5.4.	Comunicación entre usuarios a través de una red P2P: rastreos policiales	437
3.6.	Orden de conservación de datos.....	440
4.	OBTENCIÓN DE LA PRUEBA DIGITAL EN LA INVESTIGACIÓN DEL DELITO: INVESTIGACIONES POLICIALES EN INTERNET...	442
4.1.	Modalidades	442
4.2.	Investigaciones en Internet: acceso a fuentes abiertas.....	442
4.2.1.	Principio general	442
4.2.2.	Rastreos informáticos en redes P2P.....	444
4.3.	Contactos con el investigado: infiltración policial en la web	444
4.4.	El agente encubierto en Internet.....	447
4.4.1.	Concepto y utilidad	447
4.4.2.	Régimen jurídico	448
4.4.3.	Ámbito objetivo: canales cerrados de comunicación	448
4.4.4.	Ámbito objetivo: delitos que pueden ser investigados	449
4.4.5.	Utilización de archivos ilícitos por el agente encubierto.....	450
4.4.6.	Grabación de encuentros.....	452
4.5.	Deep Web-Dark Net-Red Tor.....	452

CAPÍTULO 10

OTROS MEDIOS DE INVESTIGACIÓN TECNOLÓGICA EN EL PROCESO PENAL.....		455
1.	CAPTACIÓN Y GRABACIÓN DE COMUNICACIONES ORALES DIRECTAS.....	457
1.1.	Modalidades y derechos fundamentales	457
1.1.1.	Utilización de dispositivos técnicos	457
1.1.2.	Derechos fundamentales afectados.....	458
1.2.	Régimen jurídico tras la reforma LECRIM 2015.....	459
1.2.1.	Objeto.....	459

1.2.2.	Régimen de la autorización judicial.....	459
A.	Presupuestos [art. 588 quater b)]	459
B.	Contenido de la resolución judicial [art. 588 quater c)]	460
C.	Exigencia de vinculación con encuentros concretos.....	460
C.1.	Tiempo del encuentro o encuentros.....	461
C.2.	Lugar del encuentro o encuentros.....	461
D.	Ejecución de la medida	462
D.1.	Control de la medida [art. 588 quater d)]	462
D.2.	Cese [art. 588 quater e)]	462
D.3.	Otros aspectos de la ejecución	462
1.3.	Cuadro resumen de los supuestos de autorización judicial	463
2.	CAPTACIÓN DE LA IMAGEN	464
2.1.	Derechos fundamentales afectados. El derecho a la propia imagen.....	464
2.2.	Obtención de imágenes por la Policía en sus funciones de prevención del delito.....	466
2.3.	Obtención de imágenes por la Policía en sus funciones de investigación y prueba del delito	467
2.3.1.	En espacios públicos.....	467
2.3.2.	En espacios no públicos.....	468
3.	CAPTACIÓN Y GRABACIÓN POR PARTICULARES.....	469
3.1.	Grabación con cámara oculta.....	469
3.1.1.	Doctrina del TC sobre reportajes periodísticos con cámara oculta en el proceso civil	469
3.1.2.	Grabaciones con cámara oculta en el proceso penal	470
3.1.3.	Doctrina jurisprudencial del Tribunal Supremo	470
3.2.	Grabación subrepticia de conversación por interlocutor....	472
3.2.1.	Derecho al secreto de comunicaciones.	472
3.2.2.	Derecho a la intimidad.....	473
3.2.3.	Utilización por persona vinculada directa o indirectamente con el Estado: prueba ilícita.....	474

4.	DISPOSITIVOS DE SEGUIMIENTO Y LOCALIZACIÓN.....	474
4.1.	Concepto y modalidades de geolocalización	474
4.1.1.	Geolocalización de dispositivos electrónicos de comunicación	475
4.1.2.	Geolocalización mediante dispositivos de seguimiento y de localización (balizas).....	475
4.2.	Derechos fundamentales afectados en la utilización de mecanismos de seguimiento y localización	476
4.3.	Normativa reguladora de la utilización de dispositivos de seguimiento y de localización en la LECRIM.....	479
4.3.1.	Ámbito objetivo.....	479
4.3.2.	Régimen ordinario: autorización y control judicial	480
	A. Presupuestos	480
	B. Descripción del medio técnico.....	480
4.3.3.	Supuesto de urgencia policial con control judicial posterior	481
4.3.4.	Duración de la medida	481
4.3.5.	Ejecución de la medida	481
	A. Instalación y explotación del mecanismo.....	481
	B. Deber de colaboración.....	482
	C. Custodia y destino de los soportes.....	482
5.	PRISMÁTICOS Y DRONES.....	482
5.1.	Observación del interior de un domicilio mediante el uso de prismáticos y similares	482
5.2.	Drones	484
6.	LA UTILIZACIÓN DE MEDIDAS TECNOLÓGICAS EN LA ACTIVIDAD DEL AGENTE ENCUBIERTO.....	485
6.1.	Sobre la figura del agente encubierto	485
6.1.1.	Concepto y régimen jurídico	485
6.1.2.	Finalidad inmediata: proporcionar elementos de investigación	487
6.2.	Medidas de investigación tecnológica limitativas de derechos fundamentales utilizadas en la actividad del agente encubierto	487

6.3.	Grabaciones de la actividad del agente encubierto	488
6.3.1.	Grabación de encuentros en los que participe el agente encubierto	488
6.3.2.	Grabaciones en video.....	490
6.3.3.	Entrada en domicilio por invitación	491
6.4.	Medidas tecnológicas para la seguridad del agente encubierto	493

CAPÍTULO 11

LA DIMENSIÓN INTERNACIONAL DE LA PRUEBA DIGITAL.....	495
1. DIMENSIÓN INTERNACIONAL DE LA INVESTIGACIÓN TECNOLÓGICA Y LA PRUEBA DIGITAL	497
2. COOPERACIÓN JUDICIAL INTERNACIONAL.....	498
2.1. Convenio de Budapest	499
2.2. Unión Europea.....	499
3. COOPERACIÓN POLICIAL INTERNACIONAL.....	500
4. PREVENCIÓN Y SOLUCIÓN DE CONFLICTOS DE JURISDICCIÓN EN LA CIBERDELINCUENCIA.....	503
4.1. Prevención de conflictos.....	503
4.2. Soluciones a un conflicto de jurisdicción	504

CAPÍTULO 12

COOPERACIÓN JUDICIAL INTERNACIONAL EN LA INVESTIGACIÓN TECNOLÓGICA Y PRUEBA DIGITAL.....	507
1. LA COOPERACIÓN JUDICIAL PENAL SOBRE OBTENCIÓN DE LA PRUEBA DIGITAL.....	509
1.1. Intervención transfronteriza de comunicaciones	509
1.1.1. Fases.....	509
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.....	511
A. Con asistencia técnica del Estado requerido (art. 18).....	511
B. Intervención por medio de proveedores de servicio.....	511

C.	Sin asistencia técnica del Estado requerido	511
1.1.3.	Directiva 2014/41/CE, sobre Orden Europea de Investigación Penal.....	512
1.2.	Remisión por otro Estado de datos electrónicos o digitales relevantes para el proceso penal	512
1.2.1.	Sistema del Convenio de Budapest	512
A.	Asistencia mutua para medidas provisionales.	513
B.	Asistencia mutua para remisión de datos.....	513
C.	Acceso transfronterizo a datos.....	513
D.	Otras formas: obtención en tiempo real	514
E.	Supuestos de urgencia	514
1.2.2.	Unión Europea	514
A.	Conservación rápida de datos	514
B.	Remisión de los datos.....	515
C.	Nueva regulación: Directiva 2014/41/CE sobre Orden Europea de Investigación en materia Penal (OEI).....	516
1.3.	Información transmitida por servicios policiales extranjeros	516
1.4.	Valor en España de la prueba electrónica internacional ...	517
2.	PRUEBA ELECTRÓNICA Y COOPERACIÓN JUDICIAL INTERNACIONAL EN OTRAS JURISDICCIONES.....	517
2.1.	Unión Europea.....	518
2.2.	Instrumentos de cooperación en otros ámbitos territoriales	518
3.	MECANISMOS PARA FACILITAR LA COOPERACIÓN JUDICIAL INTERNACIONAL.....	518
3.1.	Instituciones.....	518
3.2.	Catálogo de instrumentos web de apoyo a la asistencia judicial	520
4.	COOPERACIÓN CON EEUU EN LA OBTENCIÓN DE DATOS PARA LA INVESTIGACIÓN Y PRUEBA DEL DELITO.....	521
4.1.	Preservación de datos	522
4.2.	Entrega de datos.....	524
4.3.	Entrega de datos en supuestos de urgencia.....	525