

TEMAS

Delitos 2.0

Aspectos penales, procesales y de seguridad de los ciberdelitos

Moisés Barrio Andrés

■ LA LEY

[111339]

TEMAS

■ LA LEY



Delitos 2.0

Aspectos penales, procesales y de seguridad de los ciberdelitos

Moisés Barrio Andrés

SUPREMA CORTE DE JUSTICIA DE LA NACION
C.C.I.J. "SILVESTRE MORENO CORA"
BIBLIOTECA

3920.214
B3778
E.1

© Moisés Barrio Andrés, 2018
© Wolters Kluwer España, S.A.

Wolters Kluwer

C/ Collado Mediano, 9
28231 Las Rozas (Madrid)
Tel: 902 250 500 – Fax: 902 250 502
e-mail: clientes@wolterskluwer.com
http://www.wolterskluwer.es

Primera edición: septiembre 2018

Depósito Legal: M-23756-2018
ISBN versión impresa: 978-84-9020-743-7
ISBN versión electrónica: 978-84-9020-744-4

Diseño, Preimpresión e Impresión: Wolters Kluwer España, S.A.
Printed in Spain

© **Wolters Kluwer España, S.A.** Todos los derechos reservados. A los efectos del art. 32 del Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba la Ley de Propiedad Intelectual, Wolters Kluwer España, S.A., se opone expresamente a cualquier utilización del contenido de esta publicación sin su expresa autorización, lo cual incluye especialmente cualquier reproducción, modificación, registro, copia, explotación, distribución, comunicación, transmisión, envío, reutilización, publicación, tratamiento o cualquier otra utilización total o parcial en cualquier modo, medio o formato de esta publicación.

Cualquier forma de reproducción, distribución, comunicación pública o transformación de esta obra solo puede ser realizada con la autorización de sus titulares, salvo excepción prevista por la Ley. Dirijase a **Cedro** (Centro Español de Derechos Reprográficos, www.cedro.org) si necesita fotocopiar o escanear algún fragmento de esta obra.

El editor y los autores no aceptarán responsabilidades por las posibles consecuencias ocasionadas a las personas naturales o jurídicas que actúen o dejen de actuar como resultado de alguna información contenida en esta publicación.

Nota de la Editorial: El texto de las resoluciones judiciales contenido en las publicaciones y productos de **Wolters Kluwer España, S.A.**, es suministrado por el Centro de Documentación Judicial del Consejo General del Poder Judicial (Cendoj), excepto aquellas que puntualmente nos han sido proporcionadas por parte de los gabinetes de comunicación de los órganos judiciales colegiados. El Cendoj es el único organismo legalmente facultado para la recopilación de dichas resoluciones. El tratamiento de los datos de carácter personal contenidos en dichas resoluciones es realizado directamente por el citado organismo, desde julio de 2003, con sus propios criterios en cumplimiento de la normativa vigente sobre el particular, siendo por tanto de su exclusiva responsabilidad cualquier error o incidencia en esta materia.

2967 B

ÍNDICE SISTEMÁTICO

ABREVIATURAS	15
PRÓLOGO	17
CAPÍTULO I. INTRODUCCIÓN	25
CAPÍTULO II. DEL DELITO INFORMÁTICO AL CIBERDELITO ..	31
CAPÍTULO III. LOS PROBLEMAS JURÍDICO-PENALES DE LA CIBERDELINCUENCIA.	39
1. UN NUEVO GRUPO DE DELINCUENTES CIBERNÉTICOS ..	41
2. PROBLEMAS DE PERSECUCIÓN (I): EL ANONIMATO.	43
3. PROBLEMAS DE PERSECUCIÓN (II): DELITOS A DISTANCIA Y COMPETENCIA TERRITORIAL	50
4. OTROS PROBLEMAS	53
CAPÍTULO IV. DERECHO COMPARADO, INTERNACIONAL Y EUROPEO	55
1. DERECHO COMPARADO	57
2. DERECHO INTERNACIONAL	58
3. EL CONVENIO DE BUDAPEST SOBRE LA CIBERDELINCUENCIA	59
4. DERECHO DE LA UNIÓN EUROPEA	62
CAPÍTULO V. SU TRATAMIENTO EN EL DERECHO PENAL ESPAÑOL	65
CAPÍTULO VI. CIBERDELITOS CONTRA LA INTIMIDAD Y EL DERECHO A LA PROPIA IMAGEN	73
1. DESCUBRIMIENTO Y REVELACIÓN DE SECRETOS.	75

1.1.	Tipo básico de descubrimiento y revelación de secretos	75
1.1.1.	Tipo básico.	75
1.1.2.	Tipo objetivo	76
1.1.3.	Tipo subjetivo.	78
1.1.4.	Penas	78
1.2.	Protección penal de datos personales	78
1.2.1.	Tipo básico.	78
1.2.2.	Tipo objetivo	84
1.2.3.	Tipo subjetivo.	87
1.2.4.	Penas	88
1.3.	Revelación de secretos de origen ilícito.	88
1.4.	Tipos agravados.	89
2.	INTRUSISMO INFORMÁTICO E INTERCEPTACIÓN DE LAS COMUNICACIONES (HACKING).	89
2.1.	Intrusismo informático.	91
2.1.1.	Tipo básico.	91
2.1.2.	Tipo objetivo	92
2.1.3.	Tipo subjetivo.	94
2.1.4.	Penas	95
2.2.	Interceptación ilegal de comunicaciones entre sistemas de información.	95
2.2.1.	Tipo básico.	95
2.2.2.	Pena.	97
2.3.	Delito de facilitación de herramientas informáticas dañinas	97
3.	UTILIZACIÓN NO AUTORIZADA DE IMÁGENES PREVIAMENTE OBTENIDAS CON EL CONSENTIMIENTO DE LA VÍCTIMA EN UN LUGAR PRIVADO (SEXTING Y REVENGE PORN)	98
4.	CAUSAS DE JUSTIFICACIÓN	101
CAPÍTULO VII. CIBERDELITOS DE DAÑOS Y SABOTAJES (CRACKING).		105
1.	DAÑOS INFORMÁTICOS Y SABOTAJES (CRACKING).	108
1.1.	Tipo básico de daños informáticos	109
1.1.1.	Tipo básico.	109
1.1.2.	Tipo objetivo	109
1.1.3.	Tipo subjetivo.	113
1.1.4.	Pena	113
1.2.	Tipos agravados.	114

2.	OBSTACULIZACIÓN O INTERRUPCIÓN DE UN SISTEMA INFORMÁTICO	115
3.	DELITO DE FACILITACIÓN DE HERRAMIENTAS INFORMÁTICAS DAÑINAS	116
CAPÍTULO VIII. CIBERDELITOS CONTRA EL PATRIMONIO		119
1.	ESTAFA.....	122
1.1.	Estafa genérica.....	122
1.2.	Estafa informática	124
1.2.1.	Tipo básico.....	124
1.2.2.	Tipo objetivo	125
1.2.3.	Tipo subjetivo.....	129
1.3.	Estafa mediante utilización fraudulenta de tarjetas de crédito o débito, o cheques de viaje	129
2.	ABUSO DE SISTEMAS INFORMÁTICOS (<i>PHREAKING</i>)	130
CAPÍTULO IX. CIBERDELITOS CONTRA EL HONOR Y LA LIBERTAD PERSONAL		133
1.	CALUMNIAS E INJURIAS	136
1.1.	Calumnia.....	138
1.2.	Injuria	139
2.	CIBERACOSO (<i>CYBERSTALKING</i>).....	141
CAPÍTULO X. CIBERDELITOS CONTRA LA LIBERTAD E INDEMNIDAD SEXUALES		149
1.	PORNOGRAFÍA INFANTIL.....	151
2.	DELITO DE ACERCAMIENTO Y EMBAUCAMIENTO POR MEDIO DE TECNOLOGÍAS DE LA COMUNICACIÓN (<i>CHILDGROOMING</i>)	152
2.1.	Acercamiento	154
2.2.	Embaucamiento para la obtención o exhibición de material pornográfico	154
CAPÍTULO XI. CIBERDELITOS CONTRA LA PROPIEDAD INTELECTUAL Y DERECHOS CONEXOS		157
1.	DELITOS CONTRA LA PROPIEDAD INTELECTUAL.....	160
1.1.	Tipo básico	162
1.1.1.	Tipo básico.....	162
1.1.2.	Tipo objetivo	164

1.1.3.	Tipo subjetivo.....	169
1.1.4.	Penas.....	170
1.2.	Exportación e importación.....	171
1.3.	Tipo atenuado de distribución al por menor.....	171
1.4.	Tipo agravado.....	172
2.	PÁGINAS WEB DE ENLACES.....	172
3.	SUPRESIÓN DE LAS MEDIDAS DE PROTECCIÓN.....	174
CAPÍTULO XII. CIBERTERRORISMO.....		177
1.	DELITOS DE TERRORISMO.....	180
2.	CIBERTERRORISMO.....	182
CAPÍTULO XIII. ASPECTOS PROCESALES Y POLICIALES.....		185
1.	DISPOSICIONES COMUNES A LOS NUEVOS ACTOS DE INVESTIGACIÓN TECNOLÓGICA.....	191
1.1.	Principios rectores.....	192
1.2.	Presupuestos habilitantes.....	195
1.3.	Solicitud.....	196
1.4.	Resolución judicial.....	199
1.5.	Secreto de las actuaciones.....	208
1.6.	Duración de la medida.....	209
1.7.	Prórroga.....	210
1.8.	Control.....	210
1.9.	Extensión a terceros.....	211
1.10.	Utilización de la información obtenida en un procedimiento distinto y descubrimientos casuales.....	211
1.11.	Cese de la medida.....	216
1.12.	Destrucción de los registros.....	216
2.	FUERZAS Y CUERPOS DE SEGURIDAD ESPECIALIZADOS ..	218
2.1.	Ámbito internacional.....	218
2.2.	Ámbito europeo.....	220
2.3.	Ámbito nacional.....	222
2.3.1.	Unidad de Investigación Tecnológica de la Policía Nacional.....	222
2.3.2.	Grupo de Delitos Telemáticos de la Guardia Civil.....	223
3.	LÍNEAS DE EVOLUCIÓN FUTURA.....	224

CAPÍTULO XIV. LAS DISTINTAS MEDIDAS DE INVESTIGACIÓN TECNOLÓGICA PARA LOS CIBERDELITOS	229
1. LAS DILIGENCIAS DE INVESTIGACIÓN TECNOLÓGICA EN PARTICULAR	232
1.1. Interceptación de las comunicaciones telefónicas y telemáticas	233
1.1.1. Régimen general.	236
A) Requisitos constitucionales.	237
B) Requisitos de legalidad ordinaria	240
C) Práctica de la prueba	256
D) Necesidad de oír en el juicio oral lo grabado.	261
1.1.2. Incorporación al proceso de datos electrónicos de tráfico o asociados	262
1.1.3. Acceso a los datos necesarios para la identificación de usuarios, terminales y dispositivos de conectividad	263
A) Dirección IP	264
B) Identificación de los terminales mediante captación de códigos de identificación del aparato o de sus componentes	265
C) Identificación de titulares o terminales o dispositivos de conectividad.	267
1.1.4. Supuestos problemáticos	268
A) PIN de un teléfono móvil	268
B) Obtención de los listados de llamadas ...	269
C) Acceso a mensajes del móvil	269
D) Registro de la agenda del teléfono móvil ..	270
1.2. Captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos .	271
1.3. Utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización	287
1.3.1. Captación de imágenes en lugares o espacios públicos	288
1.3.2. Utilización de dispositivos o medios técnicos de seguimiento y localización	290
1.3.3. Videovigilancia	294
1.4. Registro de dispositivos de almacenamiento masivo de información	298
1.5. Registros remotos sobre equipos informáticos	312
1.6. Agente encubierto informático	316

2.	MEDIDAS DE ASEGURAMIENTO.	324
CAPÍTULO XV. CIBERSEGURIDAD		325
1.	DERECHO EUROPEO.	328
1.1.	Directiva NIS.	329
1.2.	Reglamento de Ejecución de la Directiva NIS	333
1.3.	Evolución futura: el próximo Reglamento Europeo de Ciberseguridad	335
2.	DERECHO ESPAÑOL	336
2.1.	Protección de infraestructuras críticas	337
2.2.	Seguridad Nacional	339
2.3.	Transposición de la Directiva NIS	341
2.4.	La Estrategia de Ciberseguridad Nacional	343
CAPÍTULO XVI. LA RESPONSABILIDAD DE LOS PROVEEDORES Y PLATAFORMAS DE INTERNET		349
1.	RÉGIMEN LEGAL	353
2.	RÉGIMEN DE EXCLUSIÓN DE RESPONSABILIDAD DE LOS INTERMEDIARIOS	354
2.1.	Introducción y rasgos generales.	354
2.2.	Operadores de telecomunicaciones y proveedores de acceso.	356
2.3.	Proveedores de copia temporal de datos	357
2.4.	Proveedores de alojamiento de datos	358
2.5.	Proveedores de búsquedas o enlaces.	360
2.6.	El requisito del conocimiento efectivo.	361
3.	PROHIBICIÓN DE IMPONER OBLIGACIONES GENERALES DE SUPERVISIÓN.	362
4.	EVOLUCIÓN FUTURA.	364
CONCLUSIONES		367
ANEXO		375
BIBLIOGRAFÍA		415