



**tirant**  
**monografías**  
**833**

# Nuevas amenazas a la Seguridad Nacional

Terrorismo, criminalidad  
organizada y tecnologías  
de la información y la  
comunicación

José Luis González Cussac  
María Luisa Cuerda Arnau  
(Directores)

Antonio Fernández Hernández  
(Coordinador)

# Índice

Presentación .....	17
El laberinto jurídico español.....	21
TOMÁS SALVADOR VIVES ANTÓN	
1. Introducción .....	21
2. El descrédito del derecho .....	21
3. Legitimidad, legitimación y dignidad .....	23
4. La autoridad de la legislación y algunos de sus problemas .....	28
4.1. El problema del concepto de ley.....	28
4.2. El problema de la realidad de la ley.....	32
4.2.1. El cambio en la posición de la ley .....	32
4.2.2. La devaluación de la ley.....	34
5. Sobre la autoridad de la jurisdicción .....	37
5.1. La concepción continental de la jurisdicción .....	37
5.2. La experiencia anglosajona .....	39
5.3. Algunos problemas básicos del sistema jurisdiccional español	41
6. ¿Un laberinto sin salida? .....	45
Adenda negrita .....	46
El insoportable anacronismo de los abusos policiales en el marco de la instrucción criminal a la luz de las nuevas técnicas de investigación .....	47
EMILIO CORTÉS BECHIARELLI	
1. Introducción. Algunos insoportables anacronismos.....	48
2. Un caso de técnica moderna: el ADN.....	56
3. Las labores de investigación policial previa al conocimiento judicial del presunto delito.....	59
4. Regulación legal del papel de la Policía en la investigación del delito .....	62
5. Exégesis propuesta del art. 284 DE LA Ley de Enjuiciamiento criminal .....	66
6. La afectación de los derechos fundamentales .....	74
Criminalidad organizada y las formas de investigación: el agente encubierto .....	79
AI EXIS COUTO DE BRITO	
Aproximación .....	80

1. De la responsabilidad criminal del agente infiltrado.....	80
1.1. En cuanto a la conducta típica.....	81
1.2. En cuanto a la antijuridicidad.....	84
1.1.1. La posibilidad del uso de la fuerza por parte del Estado y su poder de ordenar.....	85
1.1.2. El deber de obediencia del funcionario a la orden emanada del superior que posee base legal.....	86
1.2. En cuanto a la culpabilidad.....	87
1.3. En cuanto a la punibilidad.....	89
2. De la licitud o ilicitud de la prueba recolectada por el agente infiltrado.....	90
3. De la suficiencia de la acción controlada, de la interceptación telefónica y de la delación premiada o principio de oportunidad.....	99
4. Conclusión.....	100
Bibliografía.....	101
<b>Intervenciones prospectivas y secreto de las comunicaciones. Cuestiones pendientes.....</b>	<b>103</b>
M <sup>a</sup> LUISA CUERDA ARNAU	
1. Un nuevo escenario estratégico, criminológico y político criminal. Especial referencia al ciberespacio como nuevo ámbito de la criminalidad.....	104
2. Nuevos riesgos para el secreto de las comunicaciones.....	109
3. Algunas cuestiones pendientes en materia de interceptación prospectiva de las comunicaciones.....	121
3.1. Delimitación de supuestos: concepto de intervenciones prospectivas. Clases: A) intervenciones estratégicas de las comunicaciones; B) intervenciones prospectivas en el marco de un proceso: b') dirigidas a la comprobación del delito y la averiguación del delincuente; b'') intervenciones prospectivas como medidas preventivas de investigación: especial referencia a la captación del IP y el rastreo de sitios públicos como ejemplos de métodos lícitos.....	121
3.2. La ausencia de una delimitación del contenido constitucional del derecho a la intimidad y al secreto de las comunicaciones. Algunos ejemplos: la captación del IMEI e IMSI como medida preventiva de investigación; naturaleza jurídica de los listados de llamadas; el registro de teléfonos móviles; el registro de ordenadores.....	126
3.2.1. La captación del IMEI/IMSI.....	129
3.2.2. Los listados telefónicos.....	132
3.2.3. El registro de un teléfono móvil (o de su agenda).....	135

3.2.4. El registro de un ordenador: la STC 173/2011, de 7 de noviembre.....	137
4. Conclusiones.....	141
<b>Las TIC y las amenazas a la seguridad nacional; ciberseguridad.....</b>	<b>145</b>
FERNANDO DAVARA	
1. Introducción.....	146
2. TICs y Seguridad nacional.....	147
2.1. Nuevos riesgos; nuevas amenazas.....	148
2.1.1. Estrategias de Seguridad.....	148
2.1.2. Los nuevos Teatros de Operaciones.....	149
3. El Ciberespacio.....	151
3.1. Seguridad en el Ciberespacio.....	152
3.2. Estrategias nacionales y conjuntas.....	155
4. Reflexiones y Resumen de conclusiones.....	158
4.1. Reflexiones.....	158
4.2. Recomendaciones.....	159
4.3. Conclusiones.....	159
Bibliografía.....	160
<b>Ciberamenazas a la Seguridad Nacional.....</b>	<b>161</b>
ANTONIO FERNÁNDEZ HERNÁNDEZ	
1. Introducción.....	161
2. Seguridad Nacional.....	164
3. Las infraestructuras críticas y su protección.....	166
4. La protección de las IC en España.....	169
5. Nuevos retos.....	173
5.1. Cibercriminología.....	173
5.2. Ciberterrorismo.....	175
5.3. Ciberguerra.....	187
Bibliografía.....	189
<b>Tecnologías de información y comunicación, comercio electrónico, precios de transferencia y fraude fiscal.....</b>	<b>193</b>
JUAN CARLOS FERRÉ OLIVÉ	
1. Aproximación.....	193
2. Comercio electrónico y venta de servicios por vía electrónica.....	197
3. Los precios de transferencia.....	201
4. Conclusión.....	203

Tecnocrimen .....	205
JOSÉ L. GONZÁLEZ CUSSAC	
1. Nuevos escenarios, nuevas amenazas, nuevos enfoques.....	206
2. Un intento de categorización del crimen organizado: un híbrido de delito y amenaza .....	209
3. Las principales áreas de intervención punitiva .....	215
4. Las respuestas del derecho penal.....	219
4.1. Estrategias penales. El valor de las reglas de imputación .....	221
4.2. Las respuestas del Derecho penal al tecnocrimen .....	233
Documentos .....	240
Investigaciones prospectivas y secreto de las comunicaciones: respuestas jurídicas .....	243
ELENA M. GÓRRIZ ROYO	
1. Planteamiento.....	244
2. La jurisprudencia del TEDH como punto de partida.....	246
3. Posible tratamiento legal de las investigaciones prospectivas en el Ordenamiento jurídico español.....	260
3.1. Paralelismos entre el art. 8 TEDH y el art. 18 C.E.....	260
3.2. Delimitación entre los derechos fundamentales a la intimidad y al secreto de las comunicaciones del art. 18 C.E.....	262
4. Tratamiento de las investigaciones prospectivas en la jurisprudencia del Tribunal Constitucional y el Tribunal Supremo.....	274
5. Conclusiones.....	281
Bibliografía.....	282
Reflexiones en torno a la doctrina jurisprudencial sobre la legitimidad del acceso policial a información generada en el tráfico en internet, con motivo de investigaciones criminales .....	285
CRISTINA GUIASOLA LERMA	
1. Planteamiento .....	286
2. Doctrina jurisprudencial en relación a supuestos de acceso policial a equipos informáticos sin autorización judicial.....	287
2.1. Captación policial de las direcciones IP en supuestos de pornografía infantil a través de la red. Garantías de la intervención.....	287
2.1.1. El punto de partida: la naturaleza jurídica de la dirección IP .....	288
2.1.2. Algunas consideraciones en torno a los recientes pronunciamientos jurisprudenciales de la Sala II del Tri-	

bunal Supremo. ¿Hay proceso comunicativo en las redes de intercambio de archivo P2P? .....	293
2.1.3. La Ley 25/2007, de Conservación de Datos relativos a las comunicaciones electrónicas y a las Redes Públicas de Comunicaciones y sus repercusiones jurídicas en la investigación informática. Breve referencia a la Sentencia del Tribunal Constitucional Federal alemán de 2 de Marzo de 2010 .....	299
2.2. Legitimación constitucional al registro informático por razones de “urgencia y necesidad”: STC 7/11/11. Voto particular .....	304
3. A vueltas con la necesaria regulación de las medidas legales de investigación relacionadas con la informática: alcance y garantías .....	307
Bibliografía .....	315
El empleo de las TIC en la prevención e investigación del delito en México .....	319
PABLO HERNÁNDEZ-ROMO VALENCIA	
Ciberespionaje económico: Una amenaza real para la Seguridad Nacional en el siglo XXI .....	327
BEATRIZ LARRIBA HINOJAR	
1. Los grandes cambios del espionaje económico en el siglo XXI .....	328
2. Del espionaje económico al ciberespionaje económico .....	330
3. La expansión del ciberespionaje económico .....	335
4. Algunas reflexiones legales finales .....	339
Bibliografía .....	342
La investigación policial en los delitos de criminalidad organizada .....	345
VÍCTOR M. LÓPEZ TEMPORAL	
1. Introducción .....	346
2. Qué conocemos como criminalidad organizada .....	349
3. El fenómeno de la criminalidad organizada .....	350
4. Algunas organizaciones delictivas en particular .....	352
5. Evolución del crimen organizado en España .....	354
6. Las unidades de Inteligencia Policial contra el crimen organizado y su estructura .....	355
6.1. Estructura de las unidades del Servicio de Información y especializadas de la Policía Judicial .....	357
6.2. Organismos de apoyo en la lucha contra la criminalidad organizada .....	360
7. El Ciclo de Inteligencia .....	365

8. Las diligencias de investigación.....	367
8.1. La intervención de las comunicaciones telefónicas .....	367
9. Sistema Integrado de Interceptación Legal de Telecomunicaciones (SITEL). Sentencias que lo corroboran y operadores SITEL.....	371
9.1. Los medios técnicos y el secreto de las comunicaciones.....	371
9.2. Cobertura legal del sistema SITEL .....	371
9.3. El Sistema Integrado de Intervención Legal de las Telecomunicaciones (SITEL) .....	374
9.4. El sistema de trabajo SITEL.....	375
9.5. Sentencias favorables a la utilización de la red SITEL.....	375
Bibliografía.....	376

El efecto expansivo de los derechos fundamentales a la intimidad y al secreto de las comunicaciones telefónicas.....	379
ÁNGELA MATALLÍN EVANGELIO	

1. El derecho fundamental al secreto de las comunicaciones telefónicas .....	380
1.1. El concepto de comunicación como presupuesto de la protección constitucional.....	380
1.2. La limitación del derecho al secreto de las comunicaciones telefónicas.....	384
2. El derecho fundamental a la intimidad personal .....	386
2.1. El concepto de acto íntimo como presupuesto de la protección del derecho fundamental a la intimidad.....	386
2.2. Requisitos legales de la limitación del derecho .....	387
2.3. El carácter de los datos asociados a la compra de un terminal telefónico y/o a la contratación de un servicio.....	388
3. El derecho fundamental a la protección de datos de carácter personal) (artículo 18.4 C.E.) .....	390
3.1. Contenido y límites .....	390
3.2. Concepto y régimen jurídico de los datos de carácter personal .....	392
3.3. Tratamiento de los datos de carácter personal.....	392
3.4. Cesión de datos personales.....	393
3.5. Cesión de datos asociados a una comunicación.....	396
3.5.1. Delimitación conceptual: noción de comunicación protegida por el secreto de las comunicaciones.....	396
3.5.2. Cesión de datos asociados a una comunicación en sentido constitucional.....	398
3.5.2.1. Análisis de la normativa comunitaria .....	399
3.5.2.2. Obligaciones derivadas de la Ley 25/2007, de 18 de octubre .....	401
3.5.2.3. Conclusión .....	404

4. Toma de postura: cesión de la información relativa a la titularidad de un terminal de teléfono o de un número determinado desvinculada de un proceso de comunicación.....	405
Bibliografía.....	407
<b>Terrorismo, crimen organizado y guerras en un mundo cibernético; Los retos para los Estados Unidos y la respuesta gubernamental .....</b>	<b>409</b>
LUIS SALAS CALERO	
1. Antecedentes.....	411
2. Ciberterrorismo .....	412
2.1. ¿Qué cosa es el ciberterrorismo? .....	414
2.2. Diferenciación entre cibercrimen y ciberterrorismo.....	416
2.3. Problemas de jurisdicción y competencia .....	417
3. La ciberguerra.....	418
4. Ciberespionaje.....	423
5. Hacktivismo .....	424
5.1. WikiLeaks.....	425
5.2. Anonymous.....	430
5.3. Lulzsec.....	435
6. La respuesta normativa.....	437
6.1. Obtención de información de la seguridad nacional.....	440
6.2. Acceso ilegal a un ordenador o a una red informática del gobierno .....	440
6.3. Causar daños a un ordenador o a la información que éste contiene .....	440
6.4. Tráfico de contraseñas.....	441
6.5. Amenazar con daños a un ordenador o red.....	441
6.6. Decomiso .....	441
6.7. Acceso ilícito a comunicaciones almacenadas.....	441
6.8. Resumen de la normativa.....	442
7. La seguridad cibernética y las políticas públicas.....	444
<b>Nuevas tecnologías y nuevos desafíos para el Derecho Penal. (Especial referencia al estado de la cuestión en Brasil).....</b>	<b>449</b>
WILLIAM TERRA DE OLIVEIRA	
1. Introducción .....	450
2. La amplitud del problema.....	452
3. El estado de la cuestión en Brasil .....	453
3.1. El terrorismo y su financiación.....	454
3.2. Las estructuras públicas .....	457
3.3. Aspectos procesales y el problema de la prueba .....	460



3.4. La participación en el debate internacional .....	461
4. La legislación brasileña .....	462
4.1. La legislación en vigor en Brasil .....	465
4.1.1. El artículo 325, § 1º del Código Penal de Brasil tiene relación con el Artículo 2 de la Convención de Budapest cuando esta cuida del acceso ilícito a sistemas informáticos .....	465
4.1.2. Por su parte el artículo 10 de la Ley nº 9.296/96 que criminaliza la interceptación no autorizada de transmisión de datos guarda relación con lo dispuesto en el artículo 3 de la Convención de Budapest .....	466
4.1.3. La Ley nº 9.983/2000 ha alterado el propio Código Penal, cambiando fundamentalmente los artículos: 153, 168-A, 296, 297, 313-A, 313-B, 327 y 337-A ....	466
4.1.4. Otros delitos están previstos en la legislación electoral	467
4.1.5. Por su parte, los artículos 6 y 7 de la Convención de Budapest no encuentran en la legislación de Brasil una perfecta traducción legislativa.....	467
4.1.6. En lo que se refiere a los documentos y las conductas que impliquen en su falsificación .....	468
4.1.7. Muy importantes son las correspondencias entre la Convención de Budapest y la legislación brasileña en el tema de la <i>pornografía infantil y los delitos sexuales</i> .....	469
4.1.8. Finalmente, es necesaria una especial referencia a los derechos de autor. El tema tiene enorme importancia en la actualidad, pues guarda relación con el mundo de la economía, el arte y las ciencias .....	471
5. Conclusiones.....	473
Anexo 1: Proyecto de Ley sobre delitos informáticos (la nueva Ley de Ciberseguridad en Brasil) .....	476
Anexo 2: Decreto 3505 de 13 de junio de 2000. (Establece la Política de Seguridad de la Información en los órganos y entidades de la Administración Pública Federal) .....	483
Anexo 3: Estructura del Centro Nacional de Seguridad de la Información.....	487
 Delincuencia organizada y medios tecnológicos avanzados: el subtipo agravado previsto en relación con organizaciones y grupos criminales .....	 489
CATY VIDALES RODRÍGUEZ	
1. Introducción .....	490
2. La agravante de disposición de medios tecnológicos avanzados de comunicación o transporte.....	492

Índice	15
2.1. Precisiones terminológicas.....	492
2.2. La mera disposición de los medios tecnológicos avanzados de comunicación o transporte.....	494
2.3. La especial aptitud de los medios tecnológicos avanzados para facilitar la ejecución de los delitos o la impunidad de los culpables.....	496
2.3.1. Medios tecnológicos avanzados de comunicación o transporte especialmente aptos para facilitar la ejecución de los delitos.....	496
2.3.2. Medios tecnológicos avanzados de comunicación o transporte para facilitar la impunidad de los culpables.....	498
3. Problemas concursales.....	500
4. Conclusión.....	502
Bibliografía.....	503
Glosario de términos de seguridad informática.....	507
MANUEL MOLLAR VILLANUEVA	