

ÍNDICE

ABREVIATURAS.....	XVII
PRÓLOGO.....	XXI
PRESENTACIÓN.....	XXV

Capítulo I

LA INTEGRIDAD Y EL FUNCIONAMIENTO DE LOS SISTEMAS DE ALMACENAMIENTO Y TRATAMIENTO DE DATOS EN LA MODERNA SOCIEDAD DE LA INFORMACIÓN Y LAS TELECOMUNICACIONES

1. Introducción	1
2. Origen de las redes telemáticas.....	5
3. El cambio de paradigma en la tutela de los derechos de los ciudadanos a partir de la revolución informática.....	7
4. Características propias de la criminalidad informática.....	14
5. Desafíos de la globalización informática para el moderno Derecho Penal.....	28
a) Anonimato.....	31
b) Bajo costo	35
c) Vulnerabilidad de los sistemas y redes telemáticas....	36
d) La integridad, funcionalidad y confidencialidad de los sistemas informáticos como nuevos bienes jurídicos.....	37
e) Delitos a distancia y conflictos jurisdiccionales	41
6. La tutela de la información en el marco internacional. El Convenio sobre la Ciberdelincuencia (Budapest, 2001).....	58
7. Las políticas estratégicas en materia de ciberseguridad adoptadas por los Estados Unidos y el Reino Unido.....	62

8. La Organización de Cooperación de Shanghái (OCS) ..	64
9. La autodeterminación informativa como eje del nuevo Derecho informático	65
10. El concepto de "información"	72
11. Valoración provisoria	75

Capítulo II

PROBLEMÁTICA DE LOS DELITOS INFORMÁTICOS

1. Introducción	77
2. Problemas de la aplicación espacial de la ley penal: "Caso Yahoo!"	78
3. Participación de personas jurídicas en su comisión	88
4. Extradición	101
5. Los comportamientos abusivos cometidos a través de Internet	101
a) Fraudes cometidos a través de la manipulación de sistemas informáticos	103
b) Copia ilegal de <i>software</i> y espionaje informático....	105
c) Sabotaje informático	105
d) Uso ilegítimo de sistemas informáticos ajenos	106
e) Acceso a sistemas informáticos sin autorización (<i>Computerhacking</i>)	106

Capítulo III

INTERNET Y LIBERTAD DE EXPRESIÓN

1. Introducción	109
2. La libertad de prensa y las nuevas tecnologías de la información y la comunicación	110
3. La libertad de expresión en el mundo virtual	116
4. Limitaciones a la libertad de expresión en Internet ...	125
5. Valoración provisional	138

Capítulo IV

DELITOS CONTRA LA INTIMIDAD Y LA PRIVACIDAD *Acceso indebido a comunicaciones electrónicas, datos sensibles y sistemas informáticos*

1. Introducción	141
2. El marco constitucional de la tutela del ejercicio de la libertad	143

3. El delito de acceso ilegítimo a una comunicación electrónica.....	152
4. El acceso ilegítimo de comunicaciones electrónicas en el ámbito laboral.....	167
5. El delito de acceso no autorizado a un sistema o dato informático.....	177
6. El delito de publicación abusiva de correspondencia ...	187
7. El delito de revelación de secreto oficial y datos informáticos	189
8. Valoración provisoria	194

Capítulo V

LOS DELITOS DE DISTRIBUCIÓN DE IMÁGENES PORNOGRÁFICAS DE MENORES, ORGANIZACIÓN DE ESPECTÁCULOS PORNOGRÁFICOS CON MENORES DE EDAD, FACILITACIÓN DE ACCESO Y SUMINISTRO DE MATERIAL PORNOGRÁFICO

1. Introducción. La incidencia de los medios de comunicación masivos en la posibilidad de comisión de este delito	197
2. Bien jurídico.....	207
3. Tipicidad objetiva.....	209
3.1. Acciones típicas	209
3.2. Sujeto pasivo	222
3.3. Sujeto activo	222
3.4. Responsabilidad penal de los medios de comunicación	222
3.5. Responsabilidad penal del titular de la computadora	225
3.6. Responsabilidad penal de los padres, encargados o tutores de los menores de edad	225
3.7. Responsabilidad penal de las personas jurídicas....	226
4. El delito de organización de espectáculos en vivo con escenas pornográficas en las que participan menores de dieciocho años (art. 128, párrafo segundo, del Cód. Penal).....	227
5. El delito de facilitación de acceso a espectáculos pornográficos o suministro de material pornográfico a menores de catorce años (art. 128, párrafo tercero, Cód. Penal).....	228
6. Tipicidad subjetiva.....	230

7. Consumación y tentativa	230
8. Casos jurisprudenciales	232
9. Prescripción de la acción penal.....	235
10. Valoración provisoria	236

Capítulo VI

CONTACTO TELEMÁTICO CON MENORES DE EDAD CON FINES SEXUALES (*CHILD GROOMING*)

1. Introducción: El nuevo art. 131 del Código Penal argentino.....	237
2. Análisis dogmático del delito de contacto telemático de menores de edad con fines sexuales	241
3. Valoración provisoria.....	253

Capítulo VII

STALKING Y CYBERSTALKING: *El dominio de la víctima mediante terror psicológico como nueva expresión de atentado contra la libertad personal*

1. Introducción.....	255
2. Análisis dogmático de la figura de <i>stalking</i>	267
3. ¿Necesidad político-criminal de esta figura?	283
4. Sentido y alcance del <i>cyberstalking</i>	288
5. Valoración provisoria	291

Capítulo VIII

DELITOS CONTRA LA PROPIEDAD (I): ESTAFA Y FRAUDES INFORMÁTICOS

1. Introducción.....	293
2. El bien jurídico patrimonio. Concepto y alcance.....	298
3. Utilización fraudulenta de tarjeta de compra, crédito o débito	302
3.1. Modalidad de falsificación de tarjetas para su uso fraudulento.....	310
4. Fraude o estafa informático (<i>Computerbetrug</i>)	314
a) <i>Phishing</i>	326
b) <i>Pharming</i>	335
5. Aspectos generales del fraude informático.....	336
5.1. Ausencia de consentimiento	336
5.2. Sujeto pasivo	336

5.3. Perjuicio patrimonial	337
5.4. Autoría y participación.....	342
5.5. Tipicidad subjetiva	344
5.6. Consumación y tentativa	345
6. Otras formas de presuntos fraudes informáticos.....	346
7. Valoración provisoria	348

Capítulo IX

DELITOS CONTRA LA PROPIEDAD (II): DAÑO INFORMÁTICO, EXTORSIÓN *ONLINE* Y PROPIEDAD INTELECTUAL

1. Introducción.....	351
2. Daño o sabotaje informático	353
2.1. Delito de facilitación de programas dañinos	363
2.2. Daño informático cualificado.....	371
3. Extorsión <i>online</i> (" <i>online extortion</i> ")	371
4. Derecho comparado.....	372
5. Delitos contra la propiedad intelectual.....	374
6. Valoración provisoria	378

Capítulo X

DELITOS CONTRA LA FE PÚBLICA. FALSIFICACIÓN ELECTRÓNICA

1. Introducción.....	381
2. Bien jurídico tutelado	384
3. El delito de falsificación de documentos en el Código Penal argentino.....	389
4. Falsificación de prueba en un proceso	395
5. Falsificación de medios de pago	399
6. Valoración provisoria	400

Capítulo XI

CIBERTERRORISMO: ¿REALIDAD O FICCIÓN?

1. Introducción	401
2. Concepto y alcance del ciberterrorismo.....	407
3. Características particulares del terrorismo cibernético.....	409
4. Respuestas desde el Derecho Penal contra el ciberterrorismo.....	418
5. Valoración provisoria	422

Capítulo XII

RESPONSABILIDAD PENAL DE LOS
PROVEEDORES DEL SERVICIO DE INTERNET

1. Introducción	425
2. La autodeterminación informativa y el derecho "al olvido" en Internet	426
3. La responsabilidad de los proveedores de servicio en la sociedad de la información a través de la jurisprudencia	432
3.1. "Cubby Inc. v. CompuServe Inc." (1991)	433
3.2. "Zeran v. America Online Inc." (1997)	434
3.3. Caso "CompuServer Deutschland" (1998)	438
3.4. Críticas al fallo del AG München en el caso "CompuServer Deutschland"	441
3.5. "United States vs. Thomas"	444
4. Creación de un link o enlace para la comisión de delitos	445
5. Las leyes 25.690, 26.032 y 27.078	446
6. La responsabilidad de los proveedores intermediarios de servicios en la jurisprudencia argentina	448
7. La responsabilidad de los proveedores intermediarios de servicios en la jurisprudencia comunitaria: Google Spain, S.L. y Google Inc./Agencia Española de Protección de Datos (AEPD) y Mario Costeja González (2014)	450
8. Aplicación de las reglas de participación criminal a los proveedores de servicio de Internet	454
9. El conocimiento fehaciente como presupuesto normativo de responsabilidad	467
10. Responsabilidad de los establecimientos comerciales que brindan servicio de Internet	470
11. Valoración provisoria	471

Capítulo XIII

TÉCNICAS DE INVESTIGACIÓN Y VIGILANCIA
ELECTRÓNICAS EN EL PROCESO PENAL Y EL DERECHO
A LA PRIVACIDAD EN LA MODERNA SOCIEDAD
DE LA INFORMACIÓN

1. Introducción	475
2. Concepto de Derecho Penal informático	487

3. Monitoreo online (<i>Durchsuchung</i> , §§ 102 a 110 del Código Procesal Penal alemán)	489
4. Almacenamiento temporario de comunicaciones	501
5. Videovigilancia y supervisión electrónica (videocámaras y GPS)	508
6. Interceptación y monitoreo de comunicaciones telefónicas y telemáticas	516
7. La inviolabilidad de datos sensibles almacenados en dispositivos electrónicos por la autoridad pública (el caso de la telefonía celular)	526
8. Vigilancia electrónica aplicada como medio sustitutivo al encierro	534
9. Pedido de información a los proveedores de servicio en Internet en el marco del proceso penal	536
10. Almacenamiento y tratamiento de datos relativos al procedimiento penal y registro de condenas por delitos sexuales	539
11. ¿Qué queda en pie del derecho a la privacidad?	540
12. Conclusiones	548

Capítulo XIV

CONCLUSIONES

Conclusiones	553
BIBLIOGRAFÍA	567