

ÍNDICE

CAPÍTULO I INTRODUCCIÓN AL CIBERCRIMEN

1.1. El fenómeno de la delincuencia digital y los problemas que encierra en la actualidad.....	23
1.2. Conceptos básicos.....	25
1.3. Conductas. Distinción de categorías.....	34

CAPÍTULO II LA REGULACIÓN DE LOS CIBERDELITOS EN NUESTRO PAÍS

2.1. Ley 26.388 de delitos informáticos y ciberseguridad.....	39
2.2. Ley 27.411: El Convenio de Ciberdelitos (Budapest) y sus protocolos adicionales	41
2.2.1. El Convenio.....	41
2.2.2. El Primer Protocolo Adicional	46
2.2.3. El Segundo Protocolo Adicional.....	48
2.2.4. Las Directrices o Notas orientativas del Comité.....	48
2.2.4.1. Nota de orientación sobre disposiciones del Convenio de Budapest aplicables a las botnets	49
2.2.4.2. Nota de orientación sobre los ataques de denegación de servicio distribuido (DDOS).....	50
2.2.4.3. Nota de orientación sobre usurpación de identidad y suplantación de identidad en relación con fraude.....	51
2.2.4.4. Nota de orientación sobre los ataques a infraestructuras críticas de información.....	55
2.2.4.5. Nota de orientación sobre nuevas formas de programas informáticos malintencionados (malware).....	55
2.2.4.6. Nota de orientación sobre el spam	57
2.2.4.7. Nota de orientación sobre el terrorismo	58

2.2.4.8. Nota de orientación sobre aspectos del ransomware cubiertos por el Convenio de Budapest	59
2.3. Otras normas complementarias	62
2.3.1. Ley 11.723 de Propiedad intelectual	62
2.3.2. Ley 23.592 de Actos discriminatorios	65
2.3.2.1. El agravante genérico	65
2.3.2.2. Participación en una organización o realización de propaganda con fines discriminatorios	66
2.3.2.3. Instigación o incitación al odio y la discriminación	67
2.3.3. Ley 25.326 de protección de los datos personales	67
2.3.4. Ley 26.904 de “grooming”	71
2.3.5. Ley 27.436 de Materiales de Explotación Sexual de Niños, Niñas y Adolescentes (pornografía infantil)	72
2.3.6. Ley 27.590 “Mica Ortega”	74

CAPÍTULO III LOS CIBERDELITOS EN EL SISTEMA PENAL ARGENTINO ANÁLISIS DE LAS CONDUCTAS TÍPICAS RELEVANTE

3.1. Introducción	75
3.2. Acceso indebido a comunicaciones, violación de correspondencia electrónica (art. 153 del CP)	81
3.2.1. Apertura o acceso indebido de correspondencia electrónica	82
3.2.2. Apoderamiento ilegítimo de correspondencia	83
3.2.3. Supresión o desvío indebido de correspondencia	85
3.2.4. Interceptación o captación indebida de comunicaciones	87
3.3. Acceso no autorizado a un sistema informático (art. 153 bis del CP)	88
3.4. Acceso ilegítimo a bancos de datos y violación de secretos (art. 157 bis del CP)	90
3.4.1. Acceso ilegítimo	91
3.4.2. Violación de secretos	91
3.4.3. Inserción de datos en un banco de datos	92

3.5. Estafas y defraudaciones relevantes (arts. 172 y 173, inc. 15 y 16 del CP)	93
3.5.1. Estafa general.....	94
3.5.2. Defraudación mediante uso de tarjeta o sus datos	96
3.5.3. Defraudación informática	97
3.6. Daño informático (art. 183, segundo párrafo del CP)	98
3.6.1. Daño informático	99
3.6.2. Abuso de dispositivos.....	101
3.6.3. Cuestiones de lesividad.....	102
3.6.4. Agravantes. Art. 184 del CP.....	107
3.7. Interrupción de las comunicaciones (arts. 194 y 197 del CP)	109
3.8. Violación de medios de prueba, registros o documentos (art. 255 del CP)	113
3.9. Ciberacoso sexual de menores. Grooming (art. 131 del CP)	115

CAPÍTULO IV CONDUCTAS LESIVAS EN ENTORNOS DIGITALES Y ENCUADRE TÍPICO

4.1. Introducción	117
4.2. Afectación a la integridad de datos y sistemas electrónicos.....	118
4.2.1. Daños informáticos.....	118
4.2.2. Malware	118
4.2.2.1 Concepto	118
4.2.2.2. Adecuación típica	119
4.2.2.3. Cuestiones de autoría.....	121
4.2.3. Virus informático	126
4.2.4. Gusanos.....	127
4.2.5. Troyanos.....	130
4.2.5.1 Introducción.....	130
4.2.5.2 Tipos de troyanos y adecuación típica	131

a) Puertas traseras (backdoors):	131
b) Keyloggers y ladrones de contraseñas:	132
c) Banqueros o Bancarios:	133
d) Descargadores:	134
e) Zombies y botnets:	134
f) Sustitutos / Proxy:	135
g) Dialer:	135
h) Cemetery:	136
4.2.6. Ransomware.....	136
4.2.6.1 Concepto	136
4.2.6.2. Adecuación típica	137
4.2.7. Defacement.....	140
4.2.8. Abuso de dispositivos.....	143
4.3. Afectaciones a la privacidad e intimidad	145
4.3.1. Accesos indebidos a sistemas informáticos	146
4.3.2. Interrupción de señales electrónicas. Jammers	149
4.3.3. Protección de datos	154
4.3.4. Relaciones laborales y sistemas informáticos	157
4.4. Afectaciones a la propiedad: casos de fraude y estafa informática ..	161
4.4.1. Phishing.....	161
4.4.2. Smishing y Vishing	168
4.4.3. Pharming.....	169
4.4.4. Skimming y clonning	172
4.4.5. Sim swap	172
4.4.6. Cibermulas: responsabilidad y participación criminal de los agentes intermedios.....	176
4.4.7. Responsabilidad por la difusión. El rol de los “ influencers ” y las figuras públicas.....	177
4.5. Conductas en ecosistemas de cryptoactivos	181

4.5.1. Conceptos básicos del ecosistema crypto	181
4.5.2. Diversos mecanismos de sustracción	186
4.5.3. Captación mediante engaño	190
4.5.4. Responsabilidad de exchanges y administradores	191
4.5.5. Agiotaje. Pump & dump, rug-pull y otras maniobras similares	193
4.5.6. Lavado de activos.....	195
4.5.6.1. Características del delito	195
4.5.6.2. El lavado de activos mediante criptomonedas	198
4.5.6.3. Precedentes locales de lavado con cryptoactivos	199
a) El caso “Bovinas Blancas”.....	199
b) el caso Comando Vermelho – Operación Crypto.....	202
c) El caso Fortecar y las cibermulas.....	203
4.6. Afectaciones a la propiedad intelectual y derechos afines	204
4.6.1. Scrapping	204
4.6.1.1. ¿Qué es el scraping?	204
4.6.1.2. Inteligencia Artificial: Entrenamiento por web scraping, datos personales y propiedad intelectual	205
4.6.2. Piratería. Difusión ilícita de material protegido	209
4.6.2.1. Propiedad intelectual en internet.....	209
4.6.2.2. Piratería digital. Desafíos y objetivos de la persecución.....	212
a) MagisTV	213
b) Al Angulo TV	213
c) Red de venta de accesos a packs premium	214
d) Red de piratería digital dinámica por TVBox.....	214
4.6.3. IA generativa y deepfakes	215
4.6.3.1. Introducción.....	215
4.6.3.2. Peligros y regulación de los riesgos en el derecho extranjero.....	216
4.6.3.3. Deepfakes y vulnerabilidades de identificación por biometría	219

4.6.4. Ciberocupación - Cybersquatting	222
4.6.4.1. Concepto y modalidades	222
4.6.4.2. Secuestro inverso de nombres de dominio. Reverse domain name hijacking	225
4.7. Afectaciones a la libertad e integridad física y/o sexual	226
4.7.1. Grooming	226
4.7.2. Materiales de explotación sexual de niños, niñas y adolescentes” (MESNNA)	228
4.7.2.1. Difusión, distribución, publicación, etc.....	228
4.7.2.2. Los desafíos de la IA generativa	231
a) Sharenting y web scraping.....	231
b) Deepfakes y MESNNA.....	233
4.7.3. Corrupción, explotación y trata de personas en internet	238
4.8. Conductas en conflicto con la libertad de expresión	240
4.8.1. Algunas consideraciones generales sobre la libertad de expresión	240
4.8.1.1. Alcances del derecho a la libertad de expresión.....	242
4.8.1.2. Los límites a la libertad de expresión. Los discursos prohibidos	244
4.8.1.3. Medidas restrictivas, sanciones penales y efecto indirecto (chilling effect).....	247
4.8.2. Identidad digital y anonimato. Patrones de comportamiento en redes sociales	248
4.8.3. Amenazas	251
4.8.3.1. Las amenazas en entornos digitales.....	251
4.8.3.2 Un ejemplo paradigmático: el caso “Durand”	253
4.8.4. Intimidación pública.....	256
4.8.4.1. Caso Prestofelippo	258
4.8.4.2. Caso de Asesores Legislativos	259
4.8.5. Incitación al odio y la discriminación	260
4.8.5.1. El caso Tévez.....	261

4.8.5.2. El caso Bodart.....	262
4.8.5.3. El caso Biasi.....	263
4.8.6. Doxxeo.....	267
4.9. Conductas atípicas. Los ciberdelitos impunes en argentina.....	269
4.9.1. Ataques de denegación de servicio DDOS.....	269
4.9.1.1. Concepto.....	269
a) Ataque de capa de aplicación (application layer attack).....	272
b) Ataque de protocolo (protocol attack).....	272
c) El ataque volumétrico (volumetric attack).....	274
4.9.1.2. Adecuación típica.....	275
a) Daño informático.....	277
b) Interrupción de las comunicaciones.....	280
c) Acceso no autorizado.....	283
d) Conclusiones.....	283
4.9.2. Usurpación, robo y/o suplantación de identidad digital.....	285
4.9.3. Acción coordinada de trolls, granjas, botnets y/o ciberejercitos.....	287
4.9.4. Difusión de imágenes íntimas no consentida: Pornovenganza, sexting y sextorsión.....	288
4.9.5. Violación a la intimidad digital.....	295
4.9.6. Daño al honor en Internet y “derecho al olvido”.....	296
4.9.7. Responsabilidad de las compañías tecnológicas.....	299
4.9.8. Hurto informático.....	303
4.9.9. Captación y/o venta ilegítima de datos.....	305
4.9.10. Hostigamiento digital.....	307
4.9.10.1. Ciberacoso (stalking).....	307
4.9.10.2. Violencia y agresiones sistemáticas (cyberbullying).....	310
4.9.11. Catfishing.....	312

BIBLIOGRAFÍA