ÍNDICE SUMARIO

AUTORES 7
ÍNDICE GENERAL 13
Prólogo, por DANIELA DUPUY 15

PRIMERA PARTE

LA ERA DE LA CIVILIZACIÓN DIGITAL Y LOS CRÍMENES DEL SIGLO XXI

CAPÍTULO I

1. Civilización digital del siglo XXI: transformación sociotécnica y desafíos penales 19
2. El ciberespacio y los desafíos jurídicos y securitarios 26

SEGUNDA PARTE

DELINCUENCIA EN EL CIBERESPACIO Y JUSTICIA ELECTRÓNICA: TRANSFORMANDO EL DERECHO PENAL EN LA DIMENSIÓN DIGITAL

CAPÍTULO I

1. El ciberespacio como dominio virtual: concepto, naturaleza jurídica y actores 31

2. Soberanía nacional y ciberespacio. Introducción 34
2.1. Soberanía nacional y ciberespacio: consideraciones sobre la extraterritorialidad. 36
2.2. Soberanía nacional y jurisdicción en el ciberespacio 39
2.3. Soberanía estatal en el ámbito digital. 39
2.4. Carácter transnacional del ciberespacio y desafíos jurídicos . . . 40
2.5. Ejercicio de la soberanía digital por los Estados. 42
2.6. Jurisdicción extraterritorial en el ciberespacio y ciberdelitos. . . 43
2.7. Ciberataques, intervención estatal y soberanía más allá de las fronteras. 45
2.8. Ejemplos relevantes de extraterritorialidad digital. 48
2.9. Marco jurídico y cooperación internacional. 50
3. Hostilidades en el ciberespacio: ciberguerra, ciberdelitos y Derecho Internacional Humanitario. 53
4. Exposición a riesgos y seguridad en el ciberespacio: amenazas, vigilancia e infraestructuras críticas 56

CAPÍTULO II

1. Evolución de los ciberdelitos: un análisis político-criminal. 63
2. Ciberterrorismo 64
3. Amenazas cibernéticas a escala global: ciberataques a infraestructura crítica del Estado 68

CAPÍTULO III

1. El orden jurídico informático como bien jurídico 79
2. La protección penal del orden jurídico informático 80

CAPÍTULO IV

1. El ciberdelito o delito informático propio y delito informático impropio 83
2. Los delitos informáticos propios o ciberdelitos 84
3. Los delitos informáticos impropios. 85

CAPÍTULO V

1. La criminalidad informática en la pandemia de coronavirus (COVID-19). 87
2. El incremento de la criminalidad informática en la pandemia de coronavirus (COVID-19) 89
3. La necesidad de reforma e incorporación de nuevos tipos penales de delitos informáticos propios 91

TERCERA PARTE

ASPECTOS HISTÓRICOS Y MODIFICACIONES AL CÓDIGO PENAL NACIONAL POR LA LEY 26.388 SOBRE DELITOS INFORMÁTICOS

CAPÍTULO I

1. La necesidad de la reforma en materia de criminalidad informática 97
2. Debilidades actuales de la legislación nacional 98
3. Desafíos de la criminalidad informática 99

CAPÍTULO II

1. Antecedentes de la ley 26.388 de reforma en materia de criminalidad informática al Código Penal de la Nación 103
2. La ley 26.388 de reforma en materia de criminalidad informática al Código Penal de la Nación 105
3. Propuesta de reforma integral en materia de criminalidad informática al Código Penal de la Nación 110
   3.1. Atentados a través de medios informáticos 111
      3.1.1. Atentados mediante técnicas de manipulación informática 113
         3.1.1.1. Atentados mediante técnicas de manipulación informática 114
         3.1.1.2. Compilación, venta, ofrecimiento o intercambio de claves o datos sensibles. 115

3.1.1.3. Atentados mediante técnicas de manipulación informática a un organismo público estatal . . . 116
3.2. Sustitución de identidad . . . 117
3.3. Publicación abusiva de imágenes con contenido sexual (pornovenganza) . . . 122
3.4. Daño informático agravado, ciberataques a infraestructura crítica del Estado y ciberataques generadores de una situación de peligro grave para la sociedad . . . 124
3.4.1. Daño informático simple . . . 124
3.4.2. Daño informático agravado . . . 125
3.4.3. Daño masivo a sistemas informáticos, a infraestructura crítica del Estado o como generador de situación de peligro grave para la sociedad . . . 126
3.4.3.1. Daño masivo (art. 496, inc. 1º o art. 478, inc. 1º) . . . 126
3.4.3.2. Daño a la infraestructura crítica del Estado (art. 496, inc. 2º o art. 478, inc. 2º) . . . 129
3.4.3.3. Daño como generador de una situación de peligro grave para la sociedad (art. 496, inc. 3º o art. 478, inc. 3º) . . . 133
3.4.4. Obstaculización o interrupción del normal funcionamiento del sistema informático . . . 134
3.4.5. Venta, distribución, puesta en circulación o introducción de programas destinados a causar daño . . 138
3.5. Hurto informático: "Hurto de información o apoderamiento de bienes intangibles" . . . 139
3.6. Acceso ilegítimo a un sistema informático agravado . . . 141
3.6.1. Acceso ilegítimo agravado por tratarse de un sistema informático público . . . 141
3.6.2. Acceso ilegítimo agravado por tratarse de sistemas informáticos de proveedores de servicios públicos, salud o financieros . . . 142
3.6.3. Acceso ilegítimo agravado por tratarse de un número indeterminado de víctimas . . . 142
3.6.4. Acceso ilegítimo agravado por obtención de información sensible para la Defensa Nacional . . . 143
3.7. Hurto agravado por la utilización de inhibidores de señal (art. 163, inc. 7º) . . . 144

3.8. Interrupción o entorpecimiento de las comunicaciones por empleo de inhibidores de señal (art. 197 bis). 147
3.9. *Doxing* o exposición de datos personales 148
3.9.1. Definición 148
3.9.2. Técnicas para la obtención de información y posterior revelación en la red. 151
3.9.3. *Doxing* y su adecuación típica en el Código Penal de la Nación 153
4. Síntesis de la propuesta de reforma en materia de criminalidad informática al Código Penal de la Nación 156

CAPÍTULO III

1. Análisis crítico de la ley 26.388 de reforma en materia de criminalidad informática al Código Penal de la Nación. Ventajas y desventajas de la ley 26.388 159
1.1. Ventajas. 159
1.2. Desventajas 161

CAPÍTULO IV

1. Análisis del artículo 77 del CPN. Terminología. 163
2. Antecedentes 163
3. El motivo de introducir la terminología 164
4. Repercusión de la terminología prevista en el artículo 77 del Código Penal de la Nación sobre otros tipos penales no comprendidos por la reforma de la ley 26.388 165

CAPÍTULO V

1. Análisis de los tipos penales en particular 169
1.1. Casos de material pornográfico infantil: tenencia, distribución y comercialización. 171
1.1.1. Acuerdos internacionales 175
1.1.2. Acuerdos internacionales, marco legal y principios tuitivos. 178

1.1.3. Producción, financiación, ofrecimiento, comercialización, publicación, facilitación, divulgación, distribución de material sexual infantil y organización de espectáculos en vivo en los que participen menores 189
1.1.3.1. Conducta típica. 189
1.1.3.2. Sujeto activo. 200
1.1.3.3. Sujeto pasivo 202
1.1.3.4. Tipo subjetivo. 202
1.1.3.5. Consumación y tentativa 203
1.1.3.6. Concursalidad 203
1.1.3.7. Pena. 203
1.1.4. "La tenencia simple de pornografía sexual infantil": aspectos objetivos y subjetivos del tipo 204
1.1.4.1. Elementos configurativos del delito 209
1.1.5. Tenencia de contenido pornográfico infantil para distribución o comercialización: elementos configurativos del delito. 210
1.1.6. Distribución de material pornográfico a menores por medios digitales: elementos configurativos del delito. 213
1.1.6.1. El tipo subjetivo. 215
1.1.7. Violencia sexual a menores mediante tecnología digital 215
1.1.7.1. Definiciones clave y violencia digital 215
1.1.7.2. Las víctimas 217
1.1.7.3. Principio del interés superior del niño 218
1.1.7.4. Perfil del acosador sexual en línea. 236
1.1.8. Acoso digital y odio en línea 275
1.1.8.1. Efectividad del acoso digital. 281
1.1.8.2. Cultura de la cancelación 283
1.1.9. Implicación de servicios de hosting y buscadores en la red 286
1.1.10. Almacenamiento en caché y distribución en redes 288
1.1.11. Convergencia de delitos 290

1.1.12. Fallos importantes 293
1.1.12.1. Caso “Carignano, F. D. s/Producción de material pornográfico de menores” 293
1.1.12.2. Caso “Russo, R. según art. 128, CP” 294
1.1.12.3. Caso “Luna s/Coacción” 295
1.1.13. Difusión no autorizada de material sexual privado 296
1.1.13.1. Sexting, sextorsión y difusión no consentida de material privado con fines difamatorios. Generalidades 296
1.1.13.2. Sexting 303
1.1.13.3. Sextorsión 306
1.1.13.4. Análisis de jurisprudencia 307
1.1.13.5. Precedente del Código Penal español 323
1.1.13.6. Propuesta de modificación de los artículos 155 y 169 del Código Penal 325
1.1.13.7. Justicia con perspectiva de género 328
1.1.14. Protección de datos personales en investigaciones penales: un nuevo enfoque sobre la privacidad 329
1.1.14.1. Contexto histórico normativo 330
1.1.14.2. Alcance de los datos personales 333
1.1.14.3. Responsabilidad de empresas privadas y titulares de datos 334
1.1.14.4. Interacción entre empresas privadas y el Estado 335
1.1.14.5. Anonimato y “máscaras digitales” en la sociedad *data-driven* 337
1.1.14.6. Reconceptualización del bien jurídico protegido a la luz de la ley 26.388 339
1.1.14.7. Violación de correspondencia electrónica 340
1.1.15. Acceso no autorizado a sistemas informáticos (hacking ilícito) 343
1.1.15.1. Bien jurídico protegido 344
1.1.15.2. Elementos configurativos del delito en su faz objetiva y subjetiva 346
1.1.15.3. Instalación de keyloggers y dispositivos espía 347

1.1.15.4. Explotación de contraseñas por defecto en dispositivos IoT. 348
1.1.15.5. *Credential stuffing* y reutilización masiva de credenciales robadas. 349
1.1.15.6. Venta y alquiler de botnets 349
1.1.15.7. Uso de spyware o malware como forma de acceso. Responsabilidad penal del autor del malware 350
1.1.15.8. Instalación de cookies web y recolección de datos 351
1.1.15.9. Hacking ético y pruebas de penetración. . . . 352
1.1.15.10. Acceso del empleador a sistemas de su empresa. 353
1.1.15.11. Ingeniería inversa y protecciones DRM 354
1.1.15.12. Computación en la nube (*cloud computing*) 355
1.1.15.13. Criptojacking y minería ilícita de criptomonedas 356
1.1.15.14. Derecho Comparado. 358
1.1.16. Divulgación indebida de correspondencia y comunicaciones electrónicas 359
1.1.17. Revelación de secretos. Violación de secretos profesionales o funcionales 363
1.1.18. Infracciones a la protección de datos personales. Fundamento, evolución normativa y tipicidad penal . . . 372
1.1.18.1. Captación ilegal de datos, imágenes y sonidos 378
1.1.19. Impacto de la inteligencia artificial en la protección de datos y el cibercrimen 381
1.1.20. Ciberdelincuencia en el marco de la Web3 y blockchain 383
1.1.21. Estafas informáticas 387
1.1.21.1. Historia 388
1.1.21.2. Modalidades de fraude digital 388
1.1.21.3. Jurisdicción y competencia 401
1.1.21.4. Delitos informáticos en el ámbito financiero y económico 402

1.1.22. Daños informáticos 403
1.1.23. Interrupción o sabotaje de comunicaciones 412
1.1.24. Alteración y destrucción de medios de prueba digitales. 415
1.1.24.1. En el Anteproyecto de Código Penal, Comisión 2024 419
1.1.24.2. Directrices de la Unesco para fiscales sobre la recopilación de pruebas digitales 420

CAPÍTULO VI

1. Reformas legislativas en materia de criminalidad informática. 425
2. Tratamiento normativo en los Anteproyectos de Reforma 429
3. Parte general y desafíos estructurales 438
4. Parte especial. Nuevas formas de lesividad y bienes jurídicos difusos 439
5. Propuestas de mejora, cooperación y formación 440
5.1. Ejes para una transformación estructural del sistema de administración de justicia. 442
5.1.1. La infraestructura tecnológica como base para una justicia penal digitalmente competente 443
5.1.2. Capacitación judicial especializada: un desafío transversal y continuo 444
5.1.3. Cooperación internacional: necesidad ineludible en el combate al cibercrimen transnacional 444