

ÍNDICE SUMARIO

ÍNDICE GENERAL	7
----------------------	---

CUARTA PARTE

CIBERDELINCUENCIA EN EL ESCENARIO INTERNACIONAL

CAPÍTULO I

1. Proemio a la dimensión internacional de los delitos informáticos	11
2. Ciberdelincuencia en el escenario internacional: transnacionalidad y cooperación global	12
3. El alcance internacional del crimen cibernético	15
4. Tratado sobre ciberdelincuencia del Consejo de Europa (Convenio de Budapest, 2001)	15
4.1. Integración de naciones extranjeras al tratado	19
4.2. Participación de entidades internacionales contra la ciberdelincuencia	20
5. Ciberdelincuencia organizada	20

CAPÍTULO II

1. Disposiciones fundamentales del tratado de ciberdelincuencia	25
2. Conceptualizaciones básicas	26

3. Adaptaciones legislativas internas	26
3.1. Jurisdicción, cooperación internacional y gobernanza penal del ciberespacio	29
3.2. Delitos contra la integridad de la información y sistemas computacionales.....	32
3.2.1. Acceso no autorizado	34
3.2.2. Interceptación no consentida	49
3.2.3. Daños a la integridad de datos y sistemas	57
3.2.4. Abuso de dispositivos de software	63
3.3. Tipificaciones de infracciones informáticas	67
3.3.1. Falsificación informática	68
3.3.2. Fraude informático	71
3.4. Infracciones sobre el contenido.....	80
3.4.1. Contenido de abuso sexual infantil en Internet	80
3.4.2. Infracciones contra la propiedad intelectual e industrial	81

CAPÍTULO III

1. Aspectos procesales del Convenio sobre la Ciberdelincuencia	83
2. Derechos y garantías constitucionales en el proceso de medidas judiciales	91
2.1. Principio de libertad probatoria y autoincriminación. Dispositivos electrónicos y su desbloqueo compulsivo en el marco de un proceso penal	91
2.2. Registro de un sistema informático. Doctrina de la <i>plain view</i>	97
2.3. Derecho a la eliminación de archivos, información y datos no relacionados con la investigación.....	103
2.4. Cadena de custodia, derecho a la inalterabilidad de la prueba y a su trazabilidad	104
2.5. Programas de caja cerrada para el análisis forense (algoritmos secretos) y el derecho a controlar la prueba (art. 18, CN)	108
2.6. Derecho a la intimidad. Doctrina del mosaico y utilización de herramientas novedosas de vigilancia.....	111
3. Medidas a adoptar relativas a pruebas informáticas	115
3.1. Conservación de datos informáticos almacenados.....	117

3.2. Conservación y divulgación inmediata de datos de tráfico . . .	120
3.3. Mandato de comunicación	120
3.4. Secuestro y decomiso de datos informáticos/recolección en tiempo real de datos informáticos	121
3.5. Interceptación de datos relativos al contenido en tiempo real . . .	124

CAPÍTULO IV

1. Cooperación internacional contra la ciberdelincuencia	125
2. Fundamentos de la colaboración internacional	127
3. Normativa sobre la extradición	128
4. Bases de la asistencia mutua	132
4.1. Información provisional	133
4.2. Gestión de solicitudes de cooperación sin acuerdos internacionales previos	133
4.3. Cooperación para medidas preventivas	134
4.4. Acceso transfronterizo a datos con consentimiento o libre acceso	135

CAPÍTULO V

1. Otros marcos internacionales relevantes	137
2. Protocolo Adicional contra la ciberxenofobia y el racismo	137
3. Tratado europeo para la protección de niños contra la explotación sexual	139
4. Protocolo contra la antifalsificación comercial	140

QUINTA PARTE

CIBERCRIMEN ORGANIZADO

CAPÍTULO I

1. Criminalidad organizada internacional y transnacional. A manera de introducción	145
1.1. Crímenes informáticos internacionales	150

1.2. Delitos transnacionales o transfronterizos	154
1.2.1. Delitos informáticos transnacionales	156
1.2.2. Internet y el entorno digital distribuido y su favorecimiento a la transnacionalidad del delito	158
2. Crimen organizado internacional	159
2.1. Algunas tipificaciones específicas del crimen organizado	161
2.1.1. Pornografía infantil y grooming	162
2.1.1.1. Estándares internacionales sobre protección digital de niñas, niños y adolescentes	164
2.1.1.2. Aspectos procesales	167
2.1.1.3. Interacción con el sistema penal juvenil	179
2.1.1.4. Criminalidad organizada en el Anteproyecto de reforma penal (resolución 25/2024)	183
2.1.1.5. Cuadro comparativo: instrumentos y propuestas sobre ciberdelincuencia transnacional	186

CAPÍTULO II

1. El lavado de activos como pilar del crimen organizado internacional	189
2. Conceptualización jurídica, bien jurídico protegido y fases del blanqueo de capitales	191

CAPÍTULO III

1. Paraísos digitales, ciberdelito y obstáculos a la justicia	195
1.1. Concepto y evolución	195
1.2. Diferencias con los paraísos fiscales y factores facilitadores	197
1.3. Rol en la preparación y monetización de ciberataques	199
1.4. Obstáculos a la persecución penal en entornos digitales transnacionales	201

CAPÍTULO IV

1. Blockchain, criptoactivos y crimen organizado.
Perspectiva técnica y jurídico-penal. Fundamentos
técnicos de blockchain y criptomonedas. 205

CAPÍTULO V

1. Necesidad de normativas penales
específicas para criptomonedas. 209
 - 1.1. Infracciones monetarias y la soberanía de la
moneda nacional afectada por criptomonedas 210
 - 1.2. Riesgos para la seguridad nacional. 211
 - 1.3. Desafíos judiciales en la penalización
de delitos con criptomonedas 212
2. Legislación sobre delitos asociados al uso de criptomonedas 212
 - 2.1. Adaptación de la legislación
sobre falsificación monetaria. 213
 - 2.2. Modificaciones en la legislación sobre
la tenencia y uso de moneda falsa 213

CAPÍTULO VI

1. Ciberdelincuencia organizada de datos espaciales 215
2. Datos geoespaciales y sistemas satelitales:
tipologías, usos y actores institucionales 216
 - 2.1. Teledetección y observación de la Tierra. 218
 - 2.2. Misiones internacionales 218
 - 2.3. Sistemas de comunicaciones y geolocalización 219
 - 2.4. Datos geoespaciales: usos y valor jurídico. 220
3. Cooperación internacional espacial 220
4. Desarrollo espacial argentino 222
5. Ciberdelincuencia en el espacio ultraterrestre 228
 - 5.1. Ataque a la red KA-SAT de Viasat (2022). 228
 - 5.2. Accesos no autorizados a Landsat 7 y Terra (2007-2008). 229

5.3. Uso ilegítimo de imágenes satelitales en Asia Central (2013)	230
6. Consideraciones finales.....	230

SEXTA PARTE

DERECHO PROCESAL PENAL: INVESTIGACIÓN Y EVIDENCIA

CAPÍTULO I

1. Introducción	235
2. Indagación y recolección de pruebas en delitos complejos con base en evidencia digital para combatir la criminalidad organizada.....	236
3. La complejidad procesal como categoría estructural del sistema penal	239
4. Código Procesal Penal Federal	246
5. Figuras especiales de investigación	250
5.1. Agente encubierto.....	252
5.1.1. El agente encubierto en el ciberespacio y sus implicaciones.....	253
5.1.2. Falta de regulación específica en Argentina.....	255
5.1.3. Infiltración en redes: impacto en derechos constitucionales	260
5.1.4. Vigilancia en línea y uso de alias.....	261
5.2. El agente provocador.....	263
5.3. Agente revelador	265
5.4. Algunas consideraciones sobre el testigo de identidad reservada.....	268
5.5. Informante.....	272
5.6. Colaborador arrepentido.....	273
5.7. La “entrega vigilada”. Postergación de la detención y del secuestro de bienes.....	277
5.8. Interceptación de comunicaciones.....	280
5.9. Vigilancia electrónica y tecnologías de seguimiento.....	283

5.10. Ciberpatrullaje (vigilancia en fuentes abiertas en Internet)...	285
5.11. Rastreo de activos ilícitos	288
6. Riesgos y límites de las técnicas especiales	290
6.1. El Estado de Derecho y las técnicas especiales de investigación	294
6.2. Principios fundamentales del Estado de Derecho	296
6.2.1. Principio de legalidad.....	297
6.2.2. Principio de retribución penal	300
6.2.3. Principio de lesividad.....	301
6.2.4. Principio de proporcionalidad	302
6.2.5. Principio de culpabilidad	305
6.2.6. Principio de jurisdiccionalidad.....	306
6.2.7. Principio acusatorio.....	306
6.2.8. Principio de carga de la prueba.....	306
6.2.9. Derecho a la defensa en juicio	308
6.2.10. Principio de subsidiariedad.....	309
6.2.11. Presunción de inocencia	310
6.3. Teoría de los frutos del árbol envenenado.....	316
6.4. Conflicto de derechos y garantías.....	320
6.4.1. La puja de derechos	320
6.4.2. Perspectiva del garantismo penal:	
colisión de derechos y principios	327
6.4.2.1. Derecho a la intimidad	327
6.4.2.2. Derecho a la autodeterminación	
informativa	332
6.4.2.3. Derecho a la no autoincriminación.....	336
6.5. Punto de vista sobre la colisión de derechos.....	340

CAPÍTULO II

1. Prueba y evaluación de la evidencia	
recogida por agentes encubiertos	343
2. Principio de “libertad probatoria”	345
3. La búsqueda de la verdad en el proceso penal	348
4. Facultades coercitivas	351
5. Carga de la prueba	352

6. Sistemas de valoración de la prueba	355
7. La actividad probatoria a partir de la implementación del sistema acusatorio según las previsiones del CPPF	358
8. Prueba digital.	361
8.1. Conceptos informáticos esenciales	361
8.2. Obtención, preconstitución, peritaje, conservación	366

CAPÍTULO III

1. Vigilancia electrónica, proyectos normativos, uso de drones y tecnologías emergentes	371
2. Allanamientos remotos sobre dispositivos informáticos	381
3. Uso de drones y robots en la investigación penal.	386
3.1. Drones en allanamientos remotos y recolección de pruebas	387
4. Métodos de vigilancia electrónica en proyectos de reforma.	390
5. Experiencia comparada: España	394

CAPÍTULO IV

1. El “troyano judicial” como medida investigativa y sus implicancias	399
2. Cuestiones de constitucionalidad: privacidad, intimidad y confidencialidad de comunicaciones.	399

CAPÍTULO V

1. Directrices para la investigación en casos de femicidios y desapariciones	405
1.1. Protocolos y guías de actuación	406
1.2. Desarrollo de hipótesis delictivas	407
1.3. Colaboración interdisciplinaria y comunicación.	407
1.4. Selección de evidencia.	408
1.4.1. Evidencia digital	408
1.4.2. Principio de libertad probatoria.	410

2. Investigación en fuentes abiertas (<i>Open source intelligence, Osint</i>) . . .	411
3. Utilización de cámaras de seguridad.	412
4. Análisis de teléfonos celulares	412
4.1. Datos de titularidad	413
4.2. Datos de tráfico	413
4.3. Datos de contenido.	414
5. Investigación en plataformas digitales	414
6. Análisis de correos electrónicos	415
7. Cadena de custodia y cálculo hash	416

SÉPTIMA PARTE

EL FUTURO DEL DERECHO PENAL Y LA ADMINISTRACIÓN DE JUSTICIA: INTELIGENCIA ARTIFICIAL Y NEUROCIENCIAS COMO IMPULSORAS DE INNOVACIÓN

CAPÍTULO I

1. Modernización tecnológica de la justicia y acceso digital a derechos. Infraestructura tecnológica en la administración de justicia	421
2. La ley 26.685 y la implementación del expediente digital	422
3. Computación en la nube como herramienta para la justicia.	422
4. Nuevas tecnologías y el acceso a Internet como derechos humanos emergentes	423
5. Estrategia gubernamental frente al cibercrimen. Prevención más allá de la sanción penal.	424

CAPÍTULO II

1. Hacia un ciberespacio seguro: inteligencia artificial, neuroderechos y desafíos tecnológicos	427
1.1. La inteligencia artificial como nuevo habitante del ciberespacio.	427
1.2. Derecho a un ciberespacio seguro (DAFS)	428

2. Implementación práctica de la IA en casos de violencia de género (Proyecto Ialab)	429
3. Los neuroderechos como salvaguarda ante la manipulación mental	431
4. Aplicaciones tecnológicas en ciberseguridad: transhumanismo, manipulación psicológica, protección avanzada, blockchain y privacidad diferencial.	432

CAPÍTULO III

DELITOS INFORMÁTICOS EN EL ANTEPROYECTO DEL CÓDIGO PENAL ARGENTINO (ARTÍCULOS 801 A 816)

1. Texto completo de los artículos 801 a 816 del Anteproyecto	439
2. Aspectos generales de la nueva regulación contenida en el Título XXVI del Anteproyecto de Código Penal.	443
2.1. Breves reflexiones	445
3. Armonización internacional: Convenio de Budapest y Convención de Palermo	445

ANEXOS

ACUERDOS Y RESOLUCIONES JUDICIALES (SCJ DE MENDOZA, CABA)

Acordada N° 29.363/2019 (Suprema Corte de Justicia de Mendoza). Terminología sobre material de abuso sexual infantil.	453
Resolución Presidencia CM CABA 954/2024. Nomenclador de delitos	453

CONVENCIÓN DE LAS NACIONES UNIDAS SOBRE LOS DERECHOS DEL NIÑO (1989)

.	455
-----------	-----

<p style="text-align: center;">CONVENIO SOBRE LA CIBERDELINCUENCIA (CONSEJO DE EUROPA, BUDAPEST, 2001)</p> <p>.....</p> <p style="text-align: center;">CONVENIO DEL CONSEJO DE EUROPA PARA LA PROTECCIÓN DE LOS NIÑOS CONTRA LA EXPLOTACIÓN Y EL ABUSO SEXUAL (CONVENIO DE LANZAROTE, 2007)</p> <p>.....</p> <p style="text-align: center;">DECISIÓN MARCO 2004/68/JAI DEL CONSEJO DE LA UE (22-12-2003) RELATIVA A LA LUCHA CONTRA LA EXPLOTACIÓN SEXUAL DE NIÑOS/AS Y LA PORNOGRAFÍA INFANTIL</p> <p>.....</p> <p style="text-align: center;">PROTOCOLO FACULTATIVO DE LA CONVENCIÓN SOBRE LOS DERECHOS DEL NIÑO RELATIVO A LA VENTA DE NIÑOS, LA PROSTITUCIÓN INFANTIL Y LA UTILIZACIÓN DE NIÑOS EN LA PORNOGRAFÍA (2000)</p> <p>.....</p> <p style="text-align: center;">RESOLUCIONES NORMATIVAS DE ARGENTINA</p> <p>Dispositivos de Vigilancia Electrónica (2016). Resolución MJyDH 808/2016 (Ministerio de Justicia y Derechos Humanos de la Nación, 13-9-2016)</p> <p>Resolución MJySGC 484/2016 (Ministerio de Justicia y Seguridad, Gobierno de la Ciudad de Buenos Aires, 19-7-2016).....</p> <p>Resolución SSJUS 285/2016 (Subsecretaría de Justicia, GCBA, 2-8-2016)</p> <p style="text-align: center;">TRATADO DE ASISTENCIA JURÍDICA MUTUA EN ASUNTOS PENALES ENTRE LA REPÚBLICA ARGENTINA Y LOS ESTADOS UNIDOS DE AMÉRICA (MLAT 1991)</p> <p>.....</p>	<p>465</p> <p>473</p> <p>479</p> <p>487</p> <p>495</p> <p>495</p> <p>497</p> <p>499</p> <p>587</p>
---	--

<p>TRATADO DE EXTRADICIÓN ENTRE LA REPÚBLICA ARGENTINA Y LOS ESTADOS UNIDOS (1972)</p> <p>.....</p>	501
<p>BOLETÍN OFICIAL DE LA PROVINCIA DE BUENOS AIRES</p> <p>.....</p>	505
<p>ANÁLISIS TÉCNICO-JURÍDICO DEL DDL S.1146-B (LEY 132/2025 SOBRE INTELIGENCIA ARTIFICIAL)</p> <p>.....</p>	511
<p>BIBLIOGRAFÍA</p>	559