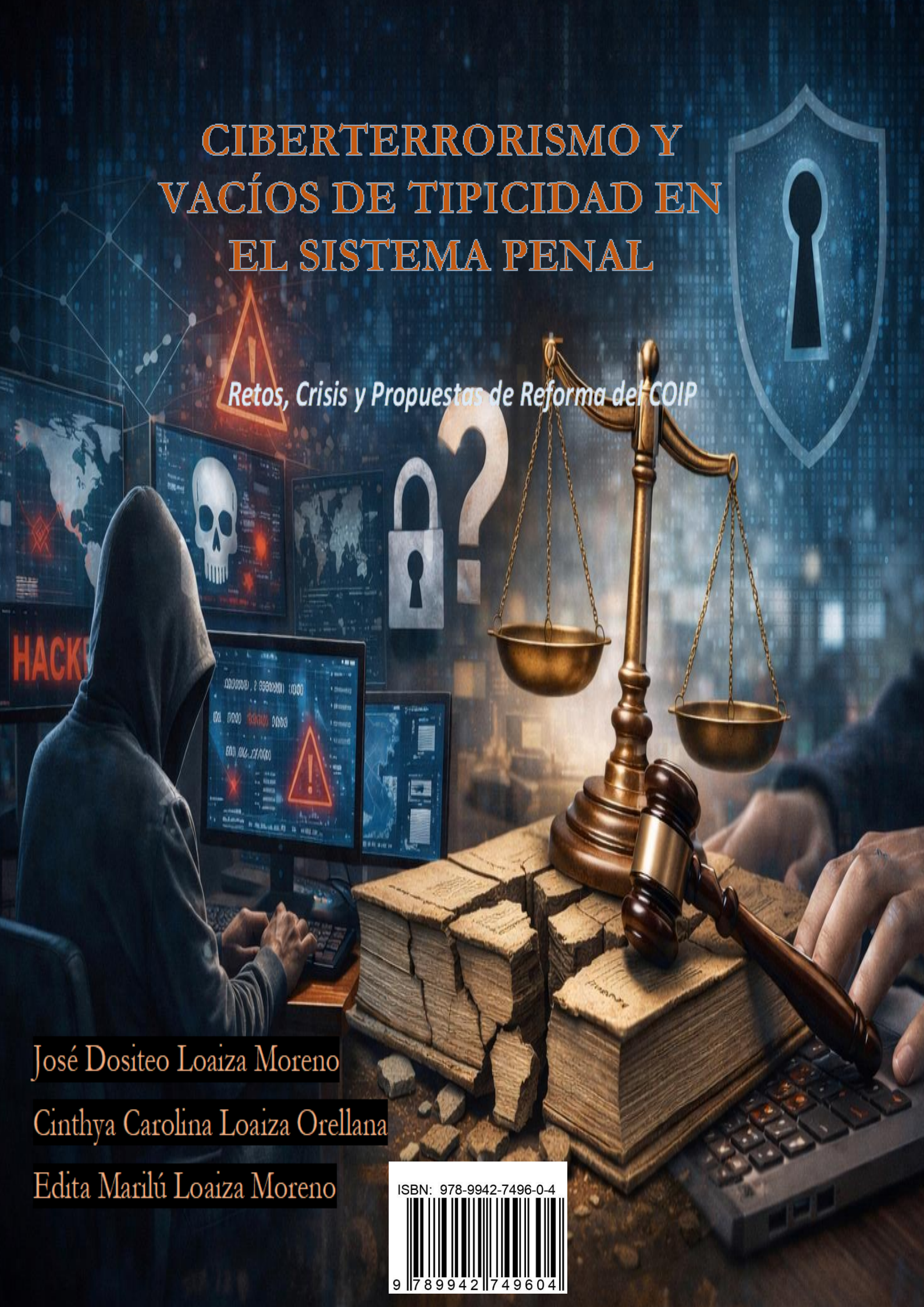
CIBERTERRORISMO Y VACÍOS DE TIPICIDAD EN EL SISTEMA PENAL

Retos, Crisis y Propuestas de Reforma del COIP



José Dositeo Loaiza Moreno

Cinthya Carolina Loaiza Orellana

Edita Marilú Loaiza Moreno

ISBN: 978-9942-7496-0-4

ACACFESA SAS.
EDITORIAL
APOYANDO EL CRECIMIENTO PROFESIONAL Y EMPRESARIAL

CIBERTERRORISMO Y VACÍOS DE TIPICIDAD EN EL SISTEMA PENAL

Retos, Crisis y Propuestas de Reforma Del COIP

Autores:

José Dositeo, Loaiza Moreno

Orcid: https://orcid.org/0009-0003-6643-4442

Correo: abgjoseloaiza_loja11@hotmail.com

Filial: Autoría Propia

Cinthya Carolina, Loaiza Orellana

Orcid: https://orcid.org/0009-0003-3676-781X

Correo: cinthya.c.loaiza@gmail.com

Filial: Autoría Propia

Edita Marilú, Loaiza Moreno

Orcid: https://orcid.org/0009-0004-7994-6794

Correo: edita.loaiza@yahoo.es

Filial: Autoría Propia

Editorial “ACACFESA SAS”

La presente obra fue revisada por 2 pares académicos externos ciegos conforme al proceso editorial de ACACFESA SAS.

Los rigurosos procedimientos editoriales de ACACFESA SAS garantizan la selección de manuscritos por sus aportes significativos al conocimiento y cualidades científicas.

Editorial: ACACFESA SAS.

Sello editorial: 978-9942-7496

Teléfono: (+593) 998955446

Web: https://acacfesa.com/editorial/index.php/1

ISBN: 978-9942-7496-0-4

Doi: https://doi.org/10.70577/afd8x778/ACACFESA.EDITORIAL/2025

Año: Enero 2026

Aviso Legal

El contenido de esta obra, que incluye ilustraciones, textos, tablas, gráficos, cuadros y referencias bibliográficas, es responsabilidad única del autor o autores. Lo que se ha dicho, los criterios y los datos no reflejan necesariamente la posición institucional ni el pensamiento de la Editorial ACACFESA SAS.

Constancia de Arbitraje

La Editorial ACACFESA SAS, certifica que este libro es el resultado de un estudio llevado a cabo por los autores, el cual fue evaluado por jurados expertos bajo el sistema de doble ciego, tanto en contenido como en forma. Asimismo, se llevó a cabo un análisis del método de investigación, paradigma y enfoque; a partir de la matriz epistémica adoptada por los autores, utilizando las normas APA, Séptima Edición y el proceso de antiplagio en línea turnitinedu para asegurar que la obra fuera científica.

DESCRIPCIÓN DEL LIBRO

El libro examina cómo el avance acelerado de las tecnologías digitales, la inteligencia artificial, la infraestructura crítica conectada y las nuevas manifestaciones de criminalidad han superado la capacidad normativa del Código Orgánico Integral Penal. Esto ha generado crisis jurídicas, investigativas, probatorias y de persecución penal, especialmente en conductas que se aproximan al ciberterrorismo, pero que no están tipificadas o están reguladas de forma insuficiente. El texto propone además líneas de modernización penal, análisis comparado y modelos normativos para el Ecuador.

DEDICATORIA

A la Universidad Nacional de Loja, institución que ha formado generaciones comprometidas con el pensamiento crítico y la transformación social. A la Carrera de Derecho, espacio donde se forja la vocación de justicia y se cultiva el rigor intelectual.

Dedico también este libro a mis maestros, quienes con disciplina y ejemplo sembraron en mí la pasión por el estudio del Derecho; a mis compañeros y colegas, con quienes compartí debates, ideas y experiencias que enriquecieron mi visión jurídica; y a mis estudiantes, cuya curiosidad y energía renovada alimentan día a día mi compromiso académico.

De manera especial, dedico esta obra a mi madre Zulema Moreno, por su sabiduría, compañía y apoyo constante; a mi esposa Digna Orellana, mis hijos y mis hermanos, pilares fundamentales en cada proyecto emprendido y fuente inagotable de motivación.

PRESENTACIÓN DEL LIBRO

El presente libro aborda uno de los desafíos más complejos de la modernidad: la transformación del terrorismo en la era digital y la incapacidad de los sistemas penales tradicionales para responder a esta amenaza. En nuestro territorio, estas dificultades se ven agravadas por vacíos de tipicidad en el Código Orgánico Integral Penal (COIP), lo que ha generado crisis investigativas, probatorias, institucionales y de seguridad pública.

La obra nace de la necesidad de analizar, con rigurosidad académica y desde una perspectiva crítica, cómo la evolución tecnológica ha superado la capacidad normativa del Estado, provocando espacios de impunidad que ponen en riesgo la estabilidad institucional tanto pública como privada y la seguridad nacional.

El texto combina análisis doctrinario, jurisprudencial, marcos internacionales, experiencias latinoamericanas, debate constitucional, técnicas de investigación digital, y finalmente presenta propuestas concretas de reforma legislativa exclusivas para el COIP. Incluye además un aporte personal basado en la experiencia académica, reflexiva y profesional.

Este libro está pensado para juristas, legisladores, académicos, operadores de justicia y estudiantes, pero también para instituciones del Estado que requieren comprender las amenazas emergentes del mundo digital.

ÍNDICE

DEDICATORIA vii

PRESENTACIÓN DEL LIBRO viii

ÍNDICE ix

PRÓLOGO xvii

INTRODUCCIÓN 1

CAPÍTULO I Fundamentos del Ciberterrorismo 5

1.1. Introducción conceptual 5

1.1.1. Definición: 5

1.2. Diferencias entre terrorismo tradicional y ciberterrorismo 10

1.2.1. Territorialidad 11

1.2.2. Costos y recursos 11

1.2.3. Identificación de responsables 11

1.2.4. Potencial destructivo 12

1.2.5. Velocidad de propagación 12

1.3. Categorías del ciberterrorismo 13

1.3.1. Ataques a infraestructura 13

1.3.2. Sabotaje digital 14

1.3.3. Terrorismo financiero digital 14

1.3.4. Desinformación masiva y psicoterror digital 14

1.3.5. Ataques basados en IA 14

1.3.6. Deepfakes con fines terroristas 15

1.4. Actores del ciberterrorismo 15

1.4.1. Organizaciones terroristas tradicionales 15

1.4.2. Grupos extremistas descentralizados 15

1.4.3. Estados y actores paraestatales 16

1.4.4. Grupos criminales organizados 16
1.4.5. Hacktivistas radicalizados 16
1.5. Metodologías y medios tecnológicos del ciberterrorismo 17
1.6. Elementos jurídicos del ciberterrorismo 18
1.6.1. Elemento objetivo 18
1.6.2. Elemento subjetivo 18
1.6.3. Bien jurídico protegido 18
1.7. El ciberterrorismo en el derecho internacional 19
1.8. Impacto del ciberterrorismo en los Estados 20
1.9. Tipificar el Ciberterrorismo 21
CAPÍTULO II Marco Internacional y Derecho Comparado del Ciberterrorismo 23
2.1. Enfoque comparado 23
2.2. Marco Internacional 24
2.2.1. Organización de las Naciones Unidas (ONU) 24
2.2.2. Convención de Budapest (2001) – Consejo de Europa 25
2.2.3. OTAN y doctrina de defensa cibernética 26
2.3. Derecho comparado en América Latina 30
2.3.1. Ecuador: rezago regional 32
2.4. Modelos internacionales de tipificación del ciberterrorismo 33
2.4.1. Modelo amplificado 34
2.4.2. Modelo autónomo 34
2.4.3. Modelo mixto 34
2.5. Prácticas internacionales 35
2.6. Aprendizajes para Ecuador: 36
CAPÍTULO III El Sistema Penal Ecuatoriano ante las Nuevas Amenazas Digitales 38
3.1. Evolución del COIP desde 2014 39
3.2. Delitos informáticos existentes y sus limitaciones 41

3.3. Problemas probatorios, cadena de custodia digital y evidencia volátil 43
3.4. La falta de especialización de operadores de justicia 46
3.5. Instituciones débiles: Policía Nacional, Fiscalía y peritos..... 47
CAPÍTULO IV Vacíos de Tipicidad y Crisis Penal..... 50
4.1. Análisis Jurídico de la Ausencia de Tipo Penal Específico de Ciberterrorismo.. 51
4.2. Sabotaje, ataques informáticos y terrorismo clásico delitos similares pero insuficientes: 53
4.3. Casos reales en Ecuador..... 55
4.4. Consecuencias jurídicas: impunidad, archivo de causas, reclasificación inadecuada 57
4.5. Riesgos para la seguridad nacional y la democracia..... 59
CAPÍTULO V Gobernanza Digital y Responsabilidad del Estado..... 61
5.1. Falta de estrategia nacional de ciberseguridad..... 62
5.2. Debilidades en la protección de datos y sistemas del Estado 64
5.3. Rol del Ministerio del Interior, CNT, ECU911, Fuerzas Armadas y Secretaría de Inteligencia..... 66
5.4. Relaciones entre ciberterrorismo y crimen organizado transnacional 69
CAPÍTULO VI Propuesta de Reforma al COIP..... 72
6.1. Redacción de un tipo penal autónomo de ciberterrorismo 73
6.2. Tipos penales complementarios..... 75
6.3. Reglas especiales de investigación 78
6.4. Incorporación de estándares del Convenio de Budapest (sin adhesión formal) .. 80
CAPÍTULO VII Análisis Crítico: Derecho Penal del Enemigo y Garantismo Digital . 82
7.1. ¿Debe endurecerse el derecho penal? 82
7.2. Riesgos de desnaturalizar garantías constitucionales 84
7.3. Ponderación entre derechos, seguridad y libertad digital 85
7.4. Propuesta de equilibrio 87
CAPÍTULO VIII Conclusiones Generales..... 90

8.1. Síntesis doctrinaria y jurídica 91
8.1.1. El ciberterrorismo como categoría autónoma 93
8.1.2. Insuficiencia del marco penal actual 94
8.1.3. El rol del garantismo digital 94
8.1.4. Responsabilidad del Estado en la gobernanza digital 95
8.1.5. Necesidad de una política criminal preventiva y especializada 95
8.2. Modelo de política criminal moderna para Ecuador 96
8.3. Necesidad jurídica y constitucional de un tipo penal autónomo 99
8.3.1. Naturaleza particular del ciberterrorismo 101
8.3.2. Derecho comparado y estándares internacionales 102
8.3.3. Justificación técnica desde la política criminal 103
8.3.4. Principio de legalidad y prohibición de analogía penal 104
8.4. Propuesta de texto normativo para el COIP 105
8.5. Inclusión en el COIP: impacto y beneficios 107
8.5.1. Profesionalización especializada 108
8.5.2. Infraestructura de ciberseguridad estatal 108
8.5.3. Política criminal preventiva 109
8.5.4. Gobernanza interinstitucional 109
8.6. Recomendaciones para jueces, fiscales, policías y legisladores 109
CAPÍTULO IX Delitos Complementarios al Tipo Penal De Ciberterrorismo 113
9.1. Necesidad de delitos complementarios: razones estructurales 113
9.2. Delito complementario: Sabotaje Digital Agravado 115
9.3. Delito complementario 2: Ataques a Infraestructura Crítica 118
9.4. Delito complementario 3: Manipulación Algorítmica o IA con Fines Terroristas 121
9.4.1. Fundamentación científica y técnica 121
9.4.2. Fundamentación jurídica 122

9.4.3. Propuesta de texto legal 123
9.5. Integración sistemática en el COIP 124
9.6. Beneficios jurídico-penales de incorporar estos tipos 125
CAPÍTULO X Reglas Especiales de Investigación Digital: Fundamentación Doctrinaria y Jurídica 126
10.1. Necesidad Constitucional y Legal de Reglas Especiales de Investigación Digital 126
10.1.1. Principio de eficacia del ius puniendi 126
10.2. Fundamentación para cada regla especial 128
10.2.1 Agentes encubiertos digitales 128
10.2.2 Retención y preservación de metadatos 130
10.2.3 Cooperación internacional inmediata 132
10.2.4 Otras reglas especiales que pueden incluirse 135
10.3. Principios garantistas para limitar estas medidas 135
CAPÍTULO XI Estándares del Convenio de Budapest Sobre Cibercrimen 137
11.1. Estándares sustantivos (tipos penales mínimos) 138
11.2. Estándares probatorios y procesales 140
11.3. Estándares de cooperación internacional 142
11.4. Principios transversales del convenio 143
11.5. Aplicación para la reforma del COIP 144
CAPÍTULO XII Los Ciberdelitos y el Marco Jurídico Internacional: Análisis del Convenio de Budapest (2001) 146
12.1. Introducción al fenómeno de los ciberdelitos 146
12.2. Conceptualización y tipología de los ciberdelitos 147
12.3. El Convenio de Budapest (2001): origen y alcance 149
12.4. Tipos penales sustantivos en el Convenio de Budapest 150
12.4.1. Acceso ilícito (Artículo 2) 150
12.4.2. Interceptación ilícita (Artículo 3) 150

12.4.4. Interferencia en sistemas (Artículo 5) 151
12.4.5. Uso indebido de dispositivos (Artículo 6) 151
12.4.6. Falsificación informática (Artículo 7) 151
12.4.7. Fraude informático (Artículo 8) 151
12.4.8. Delitos relacionados con contenidos ilegales (Artículos 9 y 10) 151
12.5. Medidas procesales del Convenio de Budapest 152
12.5.1. Preservación rápida de datos (Artículo 16) 152
12.5.2. Conservación y revelación de tráfico (Artículos 17 y 18) 152
12.5.3. Allanamiento digital (Artículo 19) 153
12.5.4. Recolección en tiempo real (Artículos 20 y 21) 153
12.5.5. Interceptación legal de datos digitales 153
12.6. Cooperación internacional inmediata 153
12.7. Estándares de derechos humanos y garantías procesales 154
12.8. Importancia del Convenio de Budapest para Ecuador 155
12.9. Propuesta de incorporación parcial del Convenio al COIP 156
12.10. Recomendaciones para jueces, fiscales, policías y legisladores 158
CAPÍTULO XIII Inteligencia Artificial y Ciberdelincuencia Avanzada 161
13.1. Introducción: la inteligencia artificial como nuevo escenario delictivo 161
13.2. La IA como herramienta criminal 162
13.2.1. IA como herramienta instrumental (asistencia al delincuente) 162
13.2.2. IA como agente semi-autónomo 163
13.2.3. IA como creadora de riesgo sistémico 163
13.3. Deepfakes, identidad digital y nueva formas de fraude 164
13.4. IA en ransomware y ataques avanzados 165
13.5. IA como arma de ciberterrorismo 165
13.5.1. Algoritmos utilizados para planificar ataques 166
13.5.2. Automatización del ataque 166

13.5.3. Propaganda algorítmica 166
13.6. Responsabilidad penal en delitos con IA 167
13.7. Necesidad de tipos penales especiales en el COIP 168
13.7.1. Manipulación algorítmica con fines delictivos 168
13.7.2. Uso de IA para ataques informáticos agravados 168
13.7.3. IA con fines terroristas 169
13.7.4. Deepfake ofensivo agravado 169
13.8. Medidas procesales para investigar delitos cometidos con IA 170
13.8.1. Peritaje especializado en IA 170
13.8.2. Auditoría algorítmica forense 170
13.8.3. Preservación de modelos y bases de datos 170
13.8.4. Orden de acceso a sistemas autónomos 171
13.8.5. Agentes encubiertos digitales con IA 171
13.9. Perspectiva de derechos fundamentales 171
13.10. Recomendaciones para Ecuador 172
CAPÍTULO XIV Derecho Penal del Enemigo Digital y la Desnaturalización de los Derechos Fundamentales 174
14.1. Introducción: la expansión del punitivismo digital 174
14.2. El concepto de “enemigo” en el espacio digital 175
14.3. Tecnologías como catalizadoras de un derecho penal excepcional 179
14.3.1. Vigilancia masiva y metadatos 179
14.3.2. Persecución extraterritorial 180
14.3.3. Algoritmos de vigilancia predictiva 180
14.4. La tendencia al debilitamiento de derechos fundamentales 181
14.4.1. Presunción de inocencia 181
14.4.2. Legalidad y tipicidad 181
14.4.3. Intimidad y protección de datos 182

14.4.4. Debido proceso 182
14.4.5. Libertad de expresión 182
14.5. ¿Ciberterroristas como enemigos? Crítica desde el garantismo 183
14.6. Propuestas de equilibrio: seguridad digital con garantías 184
14.6.1. Tipos penales tecnológicos claros y específicos 184
14.6.2. Controles estrictos a las facultades excepcionales 184
14.6.3. Transparencia algorítmica 185
14.6.4. Capacitación especializada 185
14.6.5. Instituciones fuertes y controladas 186
CAPÍTULO XV Metaverso, Ciberespacio Expandido y Nuevos Desafíos para el Derecho Penal 189
15.1. Introducción: del ciberespacio al metaverso 189
15.2. Naturaleza jurídica del metaverso como "espacio penalmente relevante" 190
15.3. Ciberdelitos y nuevas tipologías criminales en entornos inmersivos. 192
15.4. Metaverso y ciberterrorismo 194
15.5. Brecha normativa en Ecuador frente al metaverso. 195
15.6. Criterios de política criminal para regular el metaverso. 196
15.7. Riesgos de desnaturalización de derechos fundamentales en el metaverso 197
ANEXOS 200
GLOSARIO DE CIBERDELITOS 200
FLUJOGRAMA DE INVESTIGACIÓN DIGITAL PENAL 209
BIBLIOGRAFÍA 219

PRÓLOGO

La sociedad contemporánea vive una transición acelerada hacia lo digital. Las relaciones humanas, económicas, estatales y criminales se han trasladado al ciberespacio, un entorno donde el Derecho avanza más lento que la realidad. El ciberterrorismo constituye la expresión más peligrosa de esta transformación: un fenómeno transnacional, descentralizado, anónimo y potencialmente devastador.

En Ecuador, las amenazas digitales no son un asunto hipotético. Los ataques a páginas gubernamentales, filtraciones masivas de datos, accesos no autorizados a sistemas estatales, intentos de afectar infraestructura crítica y operaciones de espionaje digital han revelado una vulnerabilidad profunda. Sin embargo, el país carece de un tipo penal específico de ciberterrorismo, lo que obliga a fiscales y jueces a forzar la aplicación de figuras insuficientes o desactualizadas del COIP.

El resultado es una lucha desigual entre un Estado con herramientas normativas de la era analógica y organizaciones con recursos tecnológicos de altísima sofisticación.

Esta obra es un llamado a repensar la política criminal ecuatoriana. No se trata de recurrir a un derecho penal del enemigo, sino de equilibrar adecuadamente la seguridad digital, los derechos fundamentales y las garantías constitucionales. La tecnología no debe convertirse en un terreno sin ley, pero tampoco en un pretexto para restringir libertades.

El libro que el lector tiene en sus manos busca contribuir a este debate, proporcionando un análisis exhaustivo, didáctico y propositivo.

INTRODUCCIÓN

El Ecuador enfrenta una doble crisis:

1. Una transformación acelerada del delito hacia entornos digitales que el Estado no domina.
2. Un marco penal insuficiente, con vacíos de tipicidad que impiden perseguir y sancionar conductas altamente lesivas.

El Código Orgánico Integral Penal (COIP), publicado el 10 de febrero 2014 y entra en plena vigencia el 10 de agosto del mismo año, fue una innovación en su época, pero no fue diseñado para enfrentar fenómenos cibernéticos por cuanto aun no existían este tipo de delitos en el común de la gente:

- Ataques coordinados a infraestructura crítica;
- Manipulación algorítmica con fines disruptivos;
- Uso de inteligencia artificial para ataques a sistemas públicos;
- Extorsiones digitales masivas;
- Amenazas geopolíticas en el ciberespacio;

- Terrorismo financiero digital;
- Desinformación automatizada con fines desestabilizadores.

Estas conductas superan las herramientas típicas del derecho penal clásico.

El terrorismo del siglo XXI no necesita bombas ni secuestrar aviones. Basta con vulnerar un sistema eléctrico, paralizar una red bancaria, borrar registros estatales o manipular algoritmos que controlan recursos esenciales.

El ciberterrorismo se caracteriza por:

- Anonimato,
- Alcance global,
- Costos bajos,
- Potencial destructivo elevado,
- Capacidad para afectar servicios públicos esenciales,
- Posibilidad de operar desde cualquier país,
- Uso de IA y automatización para amplificar daños.

Su impacto puede ser tan grave como un ataque físico, pero sin dejar huellas tradicionales que permitan su persecución penal.

El análisis de este libro nace de una preocupación acumulada durante años: la distancia entre la realidad digital y la estructura penal. Desde la experiencia docente, académica y profesional he constatado que:

- Los operadores de justicia carecen de formación especializada.
- Las instituciones tienen recursos limitados para investigar delitos tecnológicos.
- La legislación no se actualiza al ritmo del cibercrimen.
- El país sigue sin contar con una política nacional robusta de ciberseguridad.
- La ausencia de tipos penales modernos ha generado impunidad en casos que involucran ataques a sistemas estatales y particulares

Este libro no solo analiza estos problemas, sino que propone soluciones con un enfoque crítico, realista y

compatible con el marco constitucional, incluyendo análisis comparado, doctrina internacional, problemas prácticos y constitucionales. Con un enfoque general sobre la transformación del terrorismo en la era digital y la importancia de actualizar los sistemas penales en América Latina.

CAPÍTULO I

Fundamentos del Ciberterrorismo

1.1. Introducción conceptual

En América Latina, y especialmente en Ecuador, el ciberterrorismo aún no ha sido conceptualizado ni tipificado adecuadamente, lo que genera grandes desafíos para la política criminal, la investigación penal, la seguridad nacional y la gobernanza digital. Este capítulo desarrolla los fundamentos teóricos, doctrinarios y comparados necesarios para comprender la naturaleza del ciberterrorismo como punto de partida para el análisis posterior del sistema penal de Ecuador y otros países.

1.1.1. Definición:

El ciberterrorismo constituye una de las manifestaciones más complejas, modernas y disruptivas del terrorismo contemporáneo. Se trata de un fenómeno que combina la lógica tradicional del terrorismo, violencia destinada a generar miedo, intimidación y desestabilización estatal,

con las herramientas tecnológicas de la era digital. A diferencia del terrorismo convencional, que depende de recursos físicos, infraestructura y presencia territorial, el ciberterrorismo supone una ruptura estructural: permite operar desde cualquier parte del mundo, con costos muy bajos, de forma anónima y con capacidad de causar daños masivos sin intervención directa sobre el mundo físico (Denning, 2017).

Desde una perspectiva personal y crítica, el ciberterrorismo debe entenderse no solo como la evolución tecnológica del terrorismo, sino como una nueva categoría autónoma de amenaza que reconfigura por completo las relaciones de poder entre el Estado, los grupos radicalizados y la sociedad. A mi criterio, su peligrosidad no radica únicamente en la capacidad técnica de generar ataques informáticos, sino en tres dimensiones adicionales que suelen subestimarse: la invisibilidad operativa, la velocidad del daño y la asimetría estratégica**.**

En primer lugar, su **invisibilidad operativa** desafía los parámetros tradicionales de inteligencia e investigación penal. Los actores pueden estar ubicados fuera de la jurisdicción nacional, operar con identidades sintéticas o utilizar redes anónimas imposibles de rastrear con los mecanismos actuales de cooperación policial. El terrorismo físico deja huellas; el ciberterrorismo, en cambio, deja rastros volátiles, fácilmente alterables y muchas veces no atribuibles.

En segundo lugar, la velocidad del daño supera la capacidad de reacción estatal. Un ataque a infraestructuras críticas, sistemas eléctricos, de agua potable, bancos, aeropuertos o servicios de emergencia, puede paralizar un país entero en cuestión de segundos. No existe una fase de ejecución visible o un escenario físico donde intervenir: el ataque ocurre en tiempo real y la respuesta suele ser tardía.

Finalmente, la **asimetría estratégica** convierte al ciberterrorismo en un fenómeno profundamente democratizado: pequeños grupos, incluso individuos

aislados, pueden generar efectos equiparables a los de una organización terrorista tradicional altamente estructurada. La brecha entre la potencia del atacante y la vulnerabilidad del Estado nunca ha sido tan grande.

Bajo esta lógica, el ciberterrorismo no debe entenderse como una simple modalidad tecnológica delictiva, sino como un nuevo espacio de confrontación, donde el Estado se encuentra en evidente desventaja normativa, técnica y operativa. La ausencia de tipicidad expresa en el Código Orgánico Integral Penal agrava esta situación, pues genera un vacío jurídico que impide una persecución penal efectiva, dejando en evidencia una crisis estructural del sistema penal frente a las amenazas digitales contemporáneas.

La doctrina no ha logrado un consenso absoluto respecto a qué debe considerarse ciberterrorismo. Sin embargo, existen elementos comunes que permiten delimitar el fenómeno. Dorothy Denning (2007), una de las

precursoras en el estudio del tema, sostiene que el ciberterrorismo es “el uso premeditado de la violencia o la amenaza de violencia contra información, sistemas informáticos o redes, con el fin de causar miedo o coaccionar a gobiernos o sociedades”.

Otros autores, como Weimann (2015), agregan que el ciberterrorismo se caracteriza por la posibilidad de generar efectos equivalentes a los del terrorismo físico, pero a través de medios digitales, afectando infraestructura crítica, servicios esenciales y sistemas estatales estratégicos.

La mayoría de definiciones incluyen tres elementos esenciales:

a) **Uso de tecnología o medios digitales.** Ataques a redes, sistemas informáticos, infraestructura de datos, algoritmos, redes financieras, energía, telecomunicaciones y sistemas críticos.
b) **Finalidad terrorista.**
   Intimidar a la población, desestabilizar

instituciones, alterar el orden público, presionar a gobiernos o modificar decisiones políticas.

c) **Potencial de causar daño grave.** No se trata de simples hackeos; implica una amenaza real o potencial a la seguridad nacional, integridad de infraestructura crítica o continuidad del Estado.

Desde la perspectiva jurídico-penal, esta definición implica que el ciberterrorismo debe ser tratado como una forma agravada y autónoma de terrorismo, puesto que su estructura lesiva difiere del terrorismo tradicional.

1.2. Diferencias entre terrorismo tradicional y ciberterrorismo

Aunque comparten la finalidad terrorista de causar grave daño a la población o a la infraestructura de un estado, existen estas grandes diferencias:

1.2.1. Territorialidad

- El terrorismo clásico opera dentro de un territorio físico determinado.
- El ciberterrorismo es transnacional por naturaleza: un ataque desde Asia puede paralizar sistemas eléctricos en Ecuador en cuestión de segundos.

1.2.2. Costos y recursos

- El terrorismo tradicional requiere logística, armas, reclutamiento y movilidad.
- El ciberterrorismo requiere solo un dispositivo electrónico puede ser una computadora, conocimientos técnicos y anonimato en redes.

1.2.3. Identificación de responsables

- En terrorismo físico, existen rastros materiales existen evidencias físicas.
- En ciberterrorismo, la atribución es extremadamente difícil: los ataques pueden ser

simulados, enmascarados o ejecutados desde redes distribuidas.

1.2.4. Potencial destructivo

- Un atentado físico suele tener alcance local.
- Un ciberataque puede derribar sistemas bancarios, energéticos, médicos o militares a escala nacional.

1.2.5. Velocidad de propagación

- El terrorismo convencional tiene impacto inmediato pero limitado.
- El ciberterrorismo se propaga automáticamente y puede expandirse de forma incontrolable.

Estas diferencias justifican la necesidad de un tipo penal autónomo y especializado, como se argumentará en los capítulos posteriores, se debe actualizar la tipicidad de inmediato del tipo penal autónomo e independiente en el COIP.

1.3. Categorías del ciberterrorismo

Diversos organismos y académicos han identificado subtipos del ciberterrorismo. Las categorías más resaltantes son:

1.3.1. Ataques a infraestructura

Incluye ataques a:

- redes eléctricas,
- sistemas hídricos,
- telecomunicaciones, internet
- transporte público,
- hospitales y sistemas de salud,
- banca y pagos electrónicos,
- servicios gubernamentales.

Un ataque exitoso podría generar caos social, pérdidas económicas y afectación directa a derechos fundamentales.

1.3.2. Sabotaje digital

Alteración maliciosa de sistemas estatales o privados con el fin de destruir datos, paralizar servicios o comprometer la funcionalidad institucional.

1.3.3. Terrorismo financiero digital

Manipulación de sistemas bancarios, algoritmos de transacciones o activos digitales con fines de desestabilización económica.

1.3.4. Desinformación masiva y psicoterror digital

Uso de redes sociales, bots y algoritmos para sembrar pánico, alterar el orden público, o manipular procesos sociales y políticos.

1.3.5. Ataques basados en IA

La inteligencia artificial permite crear ataques autónomos capaces de detectar vulnerabilidades, replicarse y evadir mecanismos de seguridad.

1.3.6. Deepfakes con fines terroristas

Videos manipulados que pueden generar caos político, militar o social, simulando discursos o acciones de autoridades.

Estas categorías muestran que el ciberterrorismo es mucho más amplio que un simple “hackeo”.

1.4. Actores del ciberterrorismo

Los actores involucrados pueden ser:

1.4.1. Organizaciones terroristas tradicionales

Que utilizan medios digitales como complemento o sustituto de métodos clásicos.

1.4.2. Grupos extremistas descentralizados

Células digitales que operan sin estructura jerárquica.

1.4.3. Estados y actores paraestatales

En muchos casos, los ciberataques con fines terroristas pueden tener respaldo estatal (state-sponsored attacks).

1.4.4. Grupos criminales organizados

En América Latina, el crimen organizado utiliza técnicas avanzadas de ciberataque para extorsión, control territorial y lavado de activos.

1.4.5. Hacktivistas radicalizados

Grupos que, bajo discursos ideológicos, pueden afectar infraestructuras estratégicas.

En Ecuador, la frontera entre grupos criminales, cárteles transnacionales y cibercriminales es cada vez más difusa, lo que incrementa el riesgo de ciberterrorismo.

1.5. Metodologías y medios tecnológicos del ciberterrorismo

Entre las principales herramientas tecnológicas que utiliza el Ciberterrorismo tenemos:

- Malware avanzado, ransomware, spyware, trojan.
- Ataques DDoS, capaces de tumbar servicios estatales.
- Exploits de vulnerabilidades (día cero).
- IA generativa para automatización de ataques.
- Técnicas de phishing de alta complejidad.
- Inyección de código malicioso en sistemas públicos.
- Compromiso de satélites, drones o redes IoT.
- Intercepción de comunicaciones cifradas.

La sofisticación tecnológica exige un marco penal actualizado.

1.6. Elementos jurídicos del ciberterrorismo

Desde la perspectiva jurídico-penal, el ciberterrorismo posee:

1.6.1. Elemento objetivo

Consiste en el ataque, intrusión, sabotaje o manipulación tecnológica con capacidad de generar daños graves.

1.6.2. Elemento subjetivo

La finalidad terrorista: causar miedo, presión política, desestabilización institucional o coerción al Estado.

1.6.3. Bien jurídico protegido

- Seguridad nacional
- Estabilidad institucional
- Infraestructura pública
- Paz social
- Derechos fundamentales
- Información estatal crítica

En Ecuador, el COIP no reconoce estos elementos dentro de una figura penal específica.

1.7. El ciberterrorismo en el derecho internacional

Diversos organismos han reconocido el ciberterrorismo como amenaza global:

- **ONU**, a través de informes sobre seguridad digital.
- **Convención de Budapest**, principal instrumento contra ciberdelito.
- **OTAN**, que considera el ciberespacio como un campo operativo equivalente a tierra, mar y aire.
- **Unión Europea**, con directivas sobre resiliencia digital.
- **Estados Unidos**, con legislación específica desde la Patriot Act.

La mayoría de sistemas penales modernos tienen tipos penales específicos, lo que marca un contraste notable con Ecuador.

1.8. Impacto del ciberterrorismo en los Estados

El impacto de un ataque ciberterrorista puede ser:

- **Económico**: paralización bancaria, caída de mercados, pérdidas millonarias.
- **Político**: inestabilidad institucional, pérdida de confianza en el gobierno.
- **Social**: caos, pánico, afectación a servicios esenciales.
- **Jurídico**: colapso de sistemas judiciales, pérdida de registros, imposibilidad de certificar información pública.
- **Militar**: vulneración de comunicaciones, armamento digital, inteligencia.

Para un país con instituciones frágiles, el impacto podría ser devastador.

1.9. Tipificar el Ciberterrorismo

Desde el análisis académico y profesional, considero que algunos países incluido el nuestro se encuentra en una situación particularmente vulnerable debido a:

- La ausencia total de un tipo penal de ciberterrorismo.
- La falta de especialización de fiscales y jueces.
- Sistemas estatales expuestos a ataques constantes.
- Infraestructura crítica obsoleta y sin protocolos robustos.
- Desconexión entre el COIP y los fenómenos digitales.
- Impunidad en casos graves por falta de herramientas normativas.
- Incapacidad institucional para atribuir responsabilidad internacional.

Ecuador no puede esperar a que ocurra un ataque catastrófico para reaccionar.
La reforma penal debe ser preventiva, moderna, constitucional y proporcional.

1. El ciberterrorismo es una forma moderna, autónoma y altamente peligrosa de terrorismo.
2. Su naturaleza tecnológica, global y anónima lo convierte en una amenaza distinta a cualquier forma tradicional de violencia.
3. Ecuador carece completamente de una normativa penal adecuada para enfrentarlo.
4. La ausencia de tipicidad genera impunidad, debilidad institucional y riesgo nacional.
5. Es imprescindible que el COIP incorpore un tipo penal específico, adaptado a estándares internacionales.
6. La prevención del ciberterrorismo requiere una política criminal que combina Derecho, tecnología, cooperación internacional y gobernanza digital. La brecha entre el avance tecnológico y la legislación ecuatoriana es crítica.

CAPÍTULO II

Marco Internacional y Derecho Comparado del Ciberterrorismo

2.1. Enfoque comparado

El ciberterrorismo es un fenómeno global que supera las fronteras tradicionales del Estado. Por ello, el análisis jurídico debe considerar instrumentos internacionales, políticas de seguridad, tratados multilaterales y experiencias legislativas de otros países. Este capítulo examina el panorama global y regional, identificando los modelos más relevantes para un eventual proceso de reforma del Código Orgánico Integral Penal (COIP).

La comparación evidencia una realidad inquietante: Ecuador se encuentra entre los países de América Latina sin tipo penal específico de ciberterrorismo, lo que lo coloca en posición de vulnerabilidad frente al crimen organizado transnacional y a actores hostiles con capacidades tecnológicas avanzadas.

2.2. Marco Internacional

2.2.1. Organización de las Naciones Unidas (ONU)

La ONU reconoce al ciberterrorismo como una amenaza real para la seguridad mundial. Aunque no existe todavía una convención específica sobre ciberterrorismo, sí hay resoluciones e informes relevantes:

- **Resolución 55/63 (2000)** y **56/121 (2001)**: llaman a los Estados a reforzar la cooperación contra el uso malintencionado de tecnologías.
- **Informe del Grupo de Expertos Gubernamentales (GGE):** considera los ciberataques contra infraestructura crítica como amenazas equivalentes a ataques armados.
- **Agenda Global de Lucha contra el Terrorismo**: reconoce explícitamente que las organizaciones terroristas utilizan Internet para reclutamiento, financiamiento y ataques técnicos.

Si bien estas disposiciones no son vinculantes, sí configuran obligaciones de soft law que influyen en la política criminal interna de los Estados.

2.2.2. Convención de Budapest (2001) – Consejo de Europa

Es el principal instrumento internacional contra el ciberdelito.
Aunque no menciona expresamente el ciberterrorismo, sí establece bases normativas que sirven de referencia mundial.

Incluye delitos como:

- Acceso ilícito,
- Interceptación ilegal,
- Ataques a la integridad de sistemas,
- Fraude informático,
- Falsificación informática,
- Responsabilidad internacional.

Ecuador no es signatario, lo que lo coloca fuera del estándar internacional en cooperación digital.

2.2.3. OTAN y doctrina de defensa cibernética

La OTAN, desde 2014, considera el ciberespacio como un "ámbito operativo" equivalente a tierra, mar y aire. La doctrina permite incluso activar el Artículo 5, que regula la defensa colectiva, en casos de ciberataques graves.

Este enfoque implica que:

- Un ciberataque puede equivaler a un ataque armado;
- Los Estados deben tener mecanismos internos para tipificar, investigar y sancionar estos hechos;
- Se requiere coordinación entre sistemas de defensa nacional y justicia penal.

La visión de la OTAN es clave para comprender el potencial destructivo del ciberterrorismo.

- **Unión Europea**

  La UE cuenta con varias normas importantes:

- **Directiva NIS (2016 y 2022)**

Establece reglas de seguridad para infraestructura crítica digital.

- **Reglamento de Ciberseguridad (2019)**

  Define estándares para empresas y servicios esenciales.

- **Estrategia Europea contra el Terrorismo (2020)**

  Reconoce expresamente el ciberterrorismo como modalidad terrorista.

La UE **(**Unión Europea) exige a los países tener tipos penales claros y autónomos, generalmente con penas claras y que puedan ser agravadas.

- **Estados Unidos**

Es uno de los sistemas más avanzados en materia de combate al ciberterrorismo.

- **USA Patriot Act (2001)**

Amplió el concepto de terrorismo para incluir daños digitales a sistemas críticos.

- **Computer Fraud and Abuse Act (CFAA)**

  Sanciona ataques informáticos con penas equivalentes a delitos graves contra la seguridad nacional.

- **Cybersecurity and Infrastructure Security Agency (CISA)**

  Coordina la protección de infraestructura crítica.

El modelo estadounidense combina:

- Tipos penales autónomos,
- Unidades especializadas,
- Cooperación internacional inmediata,
- Fuerte inversión en ciberdefensa.

- **China**

China tiene una de las legislaciones más estrictas del mundo:

- Ley de Seguridad Nacional (2015): incluye amenazas digitales como terrorismo.
- Ley de Ciberseguridad (2017): establece responsabilidad penal para ataques contra infraestructura crítica, incluso extraterritorialmente.
- Penas pueden llegar a pena de muerte en casos extremadamente graves.

- **Rusia**

La legislación rusa considera actos informáticos que afecten la infraestructura militar, financiera o estatal como terrorismo digital, con penas severas.

Rusia enfatiza:

- la protección del Estado como bien jurídico máximo,

- la punición extraterritorial,
- la responsabilidad de organizaciones y personas jurídicas.

2.3. Derecho comparado en América Latina

En la región, la mayoría de países ya han incorporado tipos penales específicos o agravados vinculados al ciberterrorismo:

- **Colombia**

Colombia es un referente regional.

- Ley 1273 (2009): delitos informáticos.
- Ley 599 (Código Penal): incluye terrorismo digital de forma agravada.
- Atentar contra infraestructura digital crítica puede ser equiparado al terrorismo tradicional (art. 343).

- **Chile**

Chile se ha actualizado mediante:

- Ley Marco sobre Delitos Informáticos (2022), alineada con Budapest.
- Tipos penales autónomos sobre sabotaje digital y afectación a infraestructura crítica.

➢ **Perú**

Perú ha incorporado:

- Delitos informáticos (Ley 30096).
- Circunstancia agravante cuando el ataque afecta servicios esenciales del Estado.

➢ **México**

México tipifica:

- Acceso ilícito;
- Sabotaje informático;
- Ataques a infraestructura nacional;
- Terrorismo con uso de medios digitales (art. 139 y 140 cp).

- **Brasil**

El Marco Civil de Internet y la Ley de Seguridad Nacional establecen responsabilidades penales para:

- Actos de desestabilización estatal mediante sistemas digitales,
- Manipulación de información con fines de caos social.

- **Argentina**

Argentina cuenta con:

- Ley de Protección de Infraestructura Crítica (proyecto avanzado);
- Reforma al Código Penal (Delitos Informáticos);
- Jurisprudencia donde ataques DDoS se consideran atentados graves.

2.3.1. Ecuador: rezago regional

Ecuador es uno de los pocos países que **no** cuenta con:

- Tipo penal de ciberterrorismo,
- Agravante por afectación digital a infraestructura crítica,
- Normativa integral sobre delitos informáticos modernos,
- Adhesión a la Convención de Budapest.

El COIP contempla delitos informáticos básicos, pero insuficientes para:

- Ataques a gran escala,
- Atentados contra seguridad nacional,
- Acciones coordinadas por crimen organizado,
- Amenazas híbridas (digitales + físicas).

El vacío legislativo es evidente y peligroso.

2.4. Modelos internacionales de tipificación del ciberterrorismo

De la revisión comparada surgen tres grandes modelos:

2.4.1. Modelo amplificado

Adoptado por EE.UU. y varios países europeos.

Consiste en ampliar el concepto de terrorismo tradicional para incluir ataques digitales contra infraestructura crítica.

2.4.2. Modelo autónomo

Usado por Chile, Colombia, México.

Crea un delito independiente de ciberterrorismo, con elementos específicos:

- Ataque digital,
- Finalidad terrorista,
- Afectación grave a bienes esenciales del Estado.

2.4.3. Modelo mixto

Implementado por Perú y Brasil.

Incluye:

- Delitos informáticos agravados,

- Y un tipo penal especial para casos de grave desestabilización estatal.

2.5. Prácticas internacionales

Los sistemas más exitosos incorporan:

- Definición clara de infraestructura crítica,
- Penas diferenciadas según gravedad,
- Unidades especiales de ciberdefensa,
- Cooperación internacional inmediata,
- Responsabilidad penal de personas jurídicas,
- Protocolos de atribución digital,
- Medidas de aseguramiento de evidencia electrónica,
- Investigación asistida con inteligencia artificial,
- Formación especializada para operadores de justicia.

Estos elementos serán esenciales para la propuesta que se presentará en capítulos posteriores.

2.6. Aprendizajes para Ecuador:

Desde mi perspectiva académica y profesional, considero que se debe adoptar un modelo mixto con predominio autónomo, es decir:

1. Crear un tipo penal específico de ciberterrorismo.
2. Reformar los delitos informáticos ya existentes.
3. Incorporar agravantes por afectación a infraestructura crítica.
4. Crear protocolos nacionales de ciberseguridad.
5. Establecer unidades especializadas en Fiscalía, Policía y Fuerzas Armadas, peritos.
6. Alinear el COIP con estándares internacionales como Budapest.
7. Fortalecer la cooperación regional para enfrentar ataques transnacionales.
8. Integrar inteligencia artificial en la investigación penal.
9. Incorporar responsabilidad penal de personas jurídicas involucradas en ataques complejos.

La modernización jurídica no es opcional: es una obligación constitucional y de seguridad nacional.

1. El derecho comparado muestra que la mayoría de países ha avanzado en la tipificación del ciberterrorismo.
2. Ecuador se encuentra rezagado y en situación de riesgo.
3. Existen al menos tres modelos de regulación aplicables al país.
4. La experiencia internacional demuestra que el ciberterrorismo requiere un tratamiento penal diferenciado.
5. La propuesta ecuatoriana debe integrar estándares globales, pero respetar la Constitución y la proporcionalidad penal.
6. Ecuador tiene la oportunidad de construir una normativa moderna basada en las mejores prácticas globales.

CAPÍTULO III

El Sistema Penal Ecuatoriano ante las Nuevas Amenazas Digitales

El avance acelerado de las tecnologías de la información y la comunicación ha generado desafíos inéditos para los sistemas penales de todo el mundo. Ecuador no ha sido la excepción. Sin embargo, mientras otros países han construido un marco jurídico-penal capaz de responder con mayor coherencia a los riesgos derivados del ciberterrorismo y delitos complejos en entornos digitales, el Ecuador continúa operando con un Código Orgánico Integral Penal (COIP) que presenta serias limitaciones normativas, técnicas e institucionales. Estas debilidades han configurado un escenario de vulnerabilidad estructural frente a amenazas digitales que evolucionan con rapidez y sofisticación.

En este capítulo se examina críticamente la evolución normativa del COIP, su insuficiencia para tipificar conductas de elevado riesgo digital, los problemas probatorios que genera la evidencia electrónica y la falta

de especialización de los operadores de justicia. Finalmente, se evalúa el rol de las instituciones encargadas de la investigación penal frente a eventos que demandan alta capacidad tecnológica, coordinación interagencial y metodologías avanzadas de ciberseguridad.

3.1. Evolución del COIP desde 2014

El Código Orgánico Integral Penal entró en vigencia en agosto de 2014 con el objetivo de unificar y modernizar la legislación penal ecuatoriana. Aunque representó un avance significativo al integrar en un solo cuerpo normativo disposiciones dispersas en diferentes leyes penales, su diseño estuvo más enfocado en combatir la criminalidad tradicional que en anticiparse a los escenarios delictivos emergentes derivados del ciberespacio. En la versión original del COIP, la referencia a delitos informáticos era mínima y no incluía categorías fundamentales como acceso ilícito agravado, interferencia de sistemas críticos estatales, terrorismo digital o ataques a infraestructura estratégica.

A lo largo de la última década, diversas reformas parciales han modificado de manera fragmentada algunos artículos relacionados con fraude informático, violación de claves, falsificación de identidad digital y vulneración de sistemas. Sin embargo, estos cambios responden más a necesidades coyunturales que a una política penal integral para enfrentar riesgos digitales de alta complejidad. Ninguna de las reformas ha construido un capítulo autónomo sobre *ciberdelincuencia*, ni se ha incorporado la figura del *ciberterrorismo* como tipo penal diferenciado.

La evolución del COIP evidencia un problema de origen: el Estado ha legislado bajo un enfoque reactivo, no preventivo, lo cual ha provocado que las reformas penales queden siempre rezagadas frente al ritmo de evolución tecnológica. El resultado es un marco incompleto, poco claro y con vacíos normativos que generan inseguridad jurídica, sobre todo cuando se pretende perseguir conductas altamente sofisticadas ejecutadas a través de medios digitales.

3.2. Delitos informáticos existentes y sus limitaciones

El COIP contempla algunos delitos informáticos, como la trasferencia electrónica de activo patrimonial (art. 231) ataque a la integridad de sistemas informáticos (art. art. 232) delitos contra la información pública reservada (art. 233) acceso no consentido a un sistema informático, telemático o de telecomunicaciones (art. 234) falsificación informática (134.1) y fraude electrónico (art. 190 - 195). No obstante, estos tipos penales presentan tres limitaciones fundamentales:

a) Tipicidad restrictiva y falta de adecuación tecnológica

Los artículos del COIP no recogen la complejidad actual de los ataques informáticos. No existe regulación sobre phishing masivo, ransomware, botnets, ataques DDoS, ingeniería social avanzada, suplantación de identidad mediante IA, deepfakes o manipulación algorítmica, ciberterrorismo. La estructura típica del COIP exige demostrar acciones manuales directas del sujeto activo, lo

cual resulta obsoleto en un contexto digital basado en automatización, scripts y ataques distribuidos.

b) Ausencia de agravantes en casos de afectación a infraestructura crítica

Tampoco se prevén agravantes para ataques contra sistemas del Estado, redes financieras, telecomunicaciones, hospitales, transporte o energía eléctrica. Esto impide diferenciar daños comunes de conductas que pueden comprometer la seguridad nacional. En materia de terrorismo digital, la ausencia de agravantes o tipos autónomos es especialmente grave.

c) Falta de articulación con normativa internacional

El Ecuador no ha armonizado su normativa penal con estándares internacionales como el Convenio de Budapest (2001), considerado la base jurídica global en la lucha contra el ciberdelito. La falta de alineación dificulta la cooperación internacional, elemento fundamental dado que la mayoría de ataques se ejecutan desde fuera del territorio ecuatoriano.

Desde mi perspectiva personal, esta insuficiencia legislativa genera una situación paradójica: el Estado reconoce que el ciberterrorismo representa una amenaza estratégica, pero carece de herramientas jurídicas mínimas para perseguirlo. El resultado es un sistema penal desfasado y desarmado frente a actores que operan con superioridad tecnológica.

3.3. Problemas probatorios, cadena de custodia digital y evidencia volátil

Uno de los desafíos más críticos del sistema penal frente al ciberterrorismo es la gestión de la evidencia digital. A diferencia de la evidencia física, que es tangible y relativamente estable, la evidencia electrónica es frágil, fácilmente manipulable y altamente dependiente de procedimientos técnicos especializados.

a) Volatilidad de la evidencia digital

Los registros informáticos pueden desaparecer con un simple reinicio del sistema o mediante herramientas que borran metadatos; la evidencia RAM se pierde en

segundos; los registros de tráfico en servidores extranjeros pueden eliminarse automáticamente por políticas internas de almacenamiento. Esto exige reacciones inmediatas, pero en Ecuador los procesos suelen tardar horas o días, lo que compromete irreversiblemente la integridad de la evidencia.

b) Falta de protocolos nacionales unificados

Aunque la cadena de custodia está regulada en el COIP y el COGEP, no existe un protocolo unificado para manejo de evidencia digital que contemple estandarización, peritaje forense, preservación de logs, duplicación forense (imaging), hash de seguridad o custodia de dispositivos. Cada fiscalía aplica criterios distintos, generando inconsistencias procesales y pérdida de evidencia.

c) Insuficiencia de laboratorios forenses

La Policía Nacional cuenta con unidades de ciberdelincuencia, pero sus laboratorios carecen de software actualizado, herramientas de análisis forense avanzadas, servidores propios y equipamiento

especializado para rastreo de redes oscuras. La falta de inversión provoca demoras que afectan la validez de los elementos probatorios.

d) Testigos técnicos no especializados

Los peritos deben explicar procedimientos altamente complejos ante jueces y fiscales que, en muchos casos, carecen de conocimientos básicos en informática. Esto debilita la valoración de la prueba digital y facilita que la defensa cuestione la confiabilidad de la evidencia.

El diagnóstico personal es claro: el sistema penal ecuatoriano no está preparado técnica ni operativamente para manejar evidencia digital en casos de alta complejidad, lo cual abre la puerta a impunidad estructural y genera desconfianza en la capacidad del Estado para enfrentar amenazas digitales sofisticadas.

3.4. La falta de especialización de operadores de justicia

La especialización es un requisito esencial en delitos informáticos y ciberterrorismo. Sin embargo, se evidencia una brecha profunda en jueces, fiscales y defensores públicos:

- Muchos operadores no distinguen entre malware, spyware, phishing o ransomware.
- No existe formación obligatoria ni certificación continua en derecho digital, ciberseguridad o cadena de custodia informática.
- La interpretación de los delitos informáticos sigue criterios analógicos, desconociendo la lógica del entorno tecnológico.
- Las audiencias sobre evidencia digital se reducen a formalismos, sin análisis técnico riguroso.

Como aporte personal, considero que esta falta de especialización es una de las principales causas de impunidad en delitos complejos. La administración de justicia continúa operando con una visión tradicionalista,

a pesar de que los delitos cometidos en el ciberespacio exigen un entendimiento profundo de tecnología, redes, programación, criptografía, inteligencia digital y análisis forense.

Esta brecha cognitiva entre el sistema penal y el avance tecnológico genera decisiones judiciales erráticas, interpretaciones contradictorias y nulidades procesales que favorecen a los agresores digitales.

3.5. Instituciones débiles: Policía Nacional, Fiscalía y peritos

Finalmente, el sistema penal enfrenta un problema estructural: la debilidad institucional. Las entidades encargadas de la investigación penal presentan fallas en tres niveles:

a) Insuficiencia tecnológica

La Policía Nacional y la Fiscalía General del Estado carecen de herramientas para identificar direcciones IP, rastrear usuarios en la deep web, descifrar

comunicaciones encriptadas o intervenir redes botnet. Sin esta capacidad técnica, resulta casi imposible investigar ataques complejos.

b) Falta de personal especializado

Los equipos de investigación informática son reducidos y no logran cubrir la demanda creciente de delitos digitales. Un país que enfrenta ciberataques constantes no puede sostener unidades con pocos peritos y sin formación avanzada continua.

c) Problemas estructurales de coordinación interinstitucional

No existen protocolos efectivos de coordinación entre la Policía, Fiscalía, Ministerio de Telecomunicaciones, ARCOTEL y empresas privadas proveedoras de internet. La falta de articulación provoca que las solicitudes de información tarden días o semanas, tiempo más que suficiente para que los atacantes eliminen rastros digitales.

Realizando un análisis, la debilidad institucional es quizás la variable más determinante del fracaso del sistema penal para enfrentar amenazas digitales. No se trata únicamente de carencias tecnológicas, sino de un problema sistémico que incluye burocracia, falta de inversión, ausencia de política pública y escasa cultura de ciberseguridad en el Estado.

CAPÍTULO IV

Vacíos de Tipicidad y Crisis Penal

En el sistema penal enfrentamos una crisis estructural que se evidencia con especial claridad al analizar la ausencia de tipicidad específica para fenómenos complejos como el ciberterrorismo. Aunque el COIP incorpora algunos delitos informáticos y mantiene una tipificación general del terrorismo, la normativa no responde a las nuevas modalidades de agresión digital que pueden afectar gravemente a la seguridad nacional, la estabilidad democrática y el funcionamiento de servicios e infraestructuras críticas.

El resultado es un marco legal que opera como un "sistema penal desactualizado", incapaz de procesar, perseguir y sancionar adecuadamente estos ataques, lo cual genera impunidad y vulnerabilidad estatal.

4.1. Análisis Jurídico de la Ausencia de Tipo Penal Específico de Ciberterrorismo

El Código Orgánico Integral Penal no contiene un tipo penal que sancione de manera autónoma el ciberterrorismo. El artículo 366 tipifica el terrorismo bajo un enfoque clásico: violencia física, destrucción, explosiones, incendios, armas, y actos dirigidos a generar terror colectivo. Esta descripción no contempla ataques que se cometen exclusivamente en entornos digitales, con tecnología como lo digo de punta como:

- interferencia remota en infraestructuras críticas,
- destrucción masiva de bases de datos estatales,
- toma hostil de plataformas de seguridad pública,
- manipulación algorítmica con fines desestabilizadores,
- paralización de servicios esenciales mediante ataques DDoS,
- secuestro digital de sistemas hospitalarios o policiales.

Desde un análisis jurídico estricto, existen tres razones fundamentales por las cuales el tipo penal de terrorismo del COIP no puede extenderse de manera analógica a delitos informáticos complejos:

a) Principio de legalidad y prohibición de analogía penal

En el artículo 76.3 de la Constitución de la Republica del Ecuador y en el artículo 5 del Código Orgánico Integral Penal tenemos los principios procesales, y en materia penal está prohibido la analogía en perjuicio del procesado. Pretender "estirar" la definición de terrorismo para incluir ataques digitales violaría el núcleo del principio de legalidad.

b) Falta de adecuación típica objetiva

El terrorismo clásico exige elementos materiales (armas, explosiones, violencia física). El ciberterrorismo prescinde de ellos; su naturaleza es inmaterial y digital. No existe adecuación típica posible sin transformar la propia estructura del tipo penal.

c) Falta de elementos subjetivos específicos

El ciberterrorismo implica intenciones y efectos distintos, como afectar infraestructura crítica digital, alterar bases de datos estatales o producir colapsos tecnológicos. Estos fines no están recogidos en el tipo penal.

Desde mi perspectiva, considero que Ecuador enfrenta un "vacío normativo" que deja sin protección penal áreas sensibles del Estado. El legislador no ha asimilado la naturaleza autónoma del ciberterrorismo, tratándolo como una variante menor del terrorismo clásico, cuando en realidad se trata de una amenaza diferente en esencia, efectos y modo de ejecución.

4.2. Sabotaje, ataques informáticos y terrorismo clásico delitos similares pero insuficientes:

Ante la ausencia de un tipo penal de ciberterrorismo, fiscales y jueces han intentado subsumir estos hechos en otros delitos, como:

- Sabotaje (art. 345 COIP)

- Interferencia en sistemas informáticos (arts. 232, 233, 234 COIP)
- Terrorismo clásico (art. 366 COIP)

Sin embargo, estos tipos son jurídicamente insuficientes.

a) Sabotaje (art. 345)

Exige daño material directo a bienes o servicios. En ataques digitales, no siempre existe daño físico o destrucción tangible, por lo que el tipo se queda corto para abarcar la dimensión digital.

b) Delitos informáticos (arts. 232–234)

Fueron diseñados para perseguir conductas individuales, de menor escala, relacionadas con intrusiones, manipulación o daño de datos. No contemplan ataques estructurados con finalidad de producir terror, desestabilización política o colapso de servicios esenciales.

c) Terrorismo clásico (art. 366)

Exige actos violentos físicos. La ejecución digital, aunque provoque caos masivo, no encaja en los elementos constitutivos.

Desde una perspectiva analítica personal, se produce un fenómeno preocupante: la legislación ecuatoriana minimiza la gravedad del ciberterrorismo al tratarlo como una simple infracción informática, lo que genera una respuesta penal desproporcionadamente débil frente a la magnitud del daño potencial.

4.3. Casos reales en Ecuador

Aunque el país no ha sufrido ataques cibernéticos comparables a los de Estonia en 2007 o Ucrania en 2015, sí ha enfrentado eventos graves que evidencian vulnerabilidad estatal y carencia de herramientas jurídico-penales.

a) Ataques a páginas gubernamentales

Diversos sitios oficiales incluyendo ministerios, municipios y plataformas públicas han sido atacados mediante defacement, phishing o DDoS. En la mayoría de los casos, las investigaciones se archivaron por falta de evidencias digitales o porque no encajaban plenamente en el tipo penal de sabotaje.

b) Filtración de datos del Estado

En 2019 se produjo la filtración masiva de datos de millones de ecuatorianos a través de un servidor vulnerable. Este hecho, que comprometió información sensible de la ciudadanía, no pudo ser procesado como un ataque a seguridad nacional por falta de tipo penal adecuado.

c) Ataques a infraestructura crítica o bancaria

Instituciones financieras, sistemas municipales de pago, portales de servicios básicos y entidades públicas han sufrido ataques de ransomware y bloqueos de acceso. Pese a su gravedad, muchos casos se investigaron bajo figuras

mínimas como "acceso no autorizado" o "daño informático simple".

En todos los ejemplos, la constante es la misma: no existe un marco penal sólido que permita perseguir estas conductas como ataques contra la seguridad del Estado.

4.4. Consecuencias jurídicas: impunidad, archivo de causas, reclasificación inadecuada

La falta de tipicidad genera consecuencias directas y profundas:

a) Impunidad estructural

Al no existir un tipo penal aplicable, las investigaciones se archivan o quedan inconclusas. Esto envía un mensaje peligroso: el ciberespacio es un terreno sin sanción efectiva.

b) Reclasificación inadecuada

Fiscales intentan “encajar” los hechos en tipos menores, lo que reduce la gravedad jurídica y debilita la sanción.

Un ataque que paraliza servicios públicos puede terminar procesado como “violación de claves”.

c) Dificultad en la cooperación internacional

Sin tipificación clara, Ecuador no puede solicitar asistencia penal efectiva ni adherirse plenamente a tratados como el Convenio de Budapest.

d) Vulneración al principio de proporcionalidad

Cuando los ataques son graves, pero se sancionan con penas bajas, se rompe el equilibrio entre daño causado y respuesta penal.

Desde mi criterio personal, este escenario ha convertido al Ecuador en un destino atractivo para ataques digitales, pues los agresores perciben debilidad normativa, técnica e institucional. La ausencia de un tipo penal de ciberterrorismo es, en sí misma, un factor criminógeno.

4.5. Riesgos para la seguridad nacional y la democracia

La falta de regulación penal eficaz no es un problema meramente jurídico: compromete la estabilidad del Estado. Los riesgos pueden clasificarse en cinco categorías:

a) Riesgo para infraestructuras críticas

Ataques a sistemas eléctricos, con esto se paralizan hospitales, bancos, agua potable o aeropuertos pueden paralizar un país en minutos.

b) Riesgo para la estabilidad política

La manipulación digital, la filtración masiva de datos o el bloqueo de plataformas estatales pueden utilizarse para desestabilizar gobiernos.

c) Riesgo para la seguridad nacional

El ciberterrorismo es hoy un instrumento geopolítico. Sin legislación clara, Ecuador se expone a agresiones externas sin capacidad de respuesta jurídica.

d) Debilitamiento de la confianza ciudadana

Cuando el Estado no puede proteger datos y sistemas, la percepción de inseguridad digital se incrementa.

e) Amenaza a la democracia

Fake news, ataques informáticos a sistemas electorales o manipulación algorítmica pueden erosionar procesos democráticos.

Mi reflexión es contundente: Ecuador se encuentra en una etapa crítica en la que debe decidir si adapta su sistema penal a las amenazas digitales contemporáneas o permanece vulnerable a actores capaces de comprometer la soberanía estatal sin necesidad de ingresar físicamente al territorio nacional.

CAPÍTULO V

Gobernanza Digital y Responsabilidad del Estado

La acelerada digitalización de los servicios públicos, la creciente dependencia tecnológica de la administración estatal y la expansión de riesgos derivados de la ciberdelincuencia han colocado a la *gobernanza digital* y a la *responsabilidad del Estado* en el centro del debate jurídico contemporáneo. La transformación digital no solo implica la adopción de infraestructuras tecnológicas avanzadas, sino también la construcción de políticas públicas eficientes, mecanismos de seguridad integral y sistemas de transparencia que garanticen la protección de derechos fundamentales en el entorno digital. Las brechas normativas, técnicas y operativas han generado un escenario de vulnerabilidad que se ha manifestado en ataques sistemáticos contra instituciones públicas, servicios críticos y bases de datos gubernamentales. Esto evidencia la necesidad de un rediseño de la arquitectura estatal en materia de ciberseguridad.

5.1. Falta de estrategia nacional de ciberseguridad

Ecuador carece de una estrategia nacional integral, unificada y vinculante en materia de ciberseguridad. Aunque existen iniciativas parciales, decretos y proyectos dispersos entre diferentes instituciones, no existe un documento rector que articule políticas, responsabilidades, protocolos de respuesta, estándares mínimos y mecanismos de coordinación interestatal.

Este vacío estratégico provoca:

- **Fragmentación institucional**, donde cada entidad opera bajo criterios propios sin interoperabilidad.
- **Reacción tardía ante ataques**, al no contar con un Centro Nacional de Ciberseguridad con mando y control unificado.
- **Falta de estándares técnicos**, lo que debilita la protección de infraestructuras críticas como energía, telecomunicaciones, banca pública o seguridad interna.

- **Desactualización tecnológica**, debido a que no se planifica la renovación ni la protección del hardware y software estatal.

Desde la perspectiva jurídica, esta ausencia constituye una forma de omisión estatal, que se traduce en responsabilidad administrativa, patrimonial e incluso internacional, cuando la falta de protección compromete datos personales o derechos fundamentales.

Considero que Ecuador debe adoptar una estrategia nacional de ciberseguridad con rango legal, no solo administrativo. Un *Marco de Ciberseguridad del Estado* debería incluir:

- Protocolos obligatorios de gestión de incidentes.
- Auditorías permanentes de seguridad digital.
- Un sistema nacional de alertas tempranas.
- Capacitación técnica y jurídica para funcionarios públicos.
- Coordinación con el sector público como privado y universidades.

Solo una buena política nacional permitirá consolidar una verdadera soberanía digital.

5.2. Debilidades en la protección de datos y sistemas del Estado

Los sistemas informáticos del Estado presentan debilidades estructurales que ponen en riesgo la integridad, disponibilidad y confidencialidad de la información pública y privada. Entre las problemáticas más visibles se encuentran:

- **Bases de datos sin cifrado**, situación especialmente grave en sectores como salud, educación o justicia.
- **Falta de control de accesos**, lo que permite a funcionarios no autorizados ingresar a información sensible.
- **Inexistencia de políticas de respaldo y recuperación**, lo que ha producido pérdidas irreparables de información estatal.
- **Infraestructura obsoleta**, con servidores vulnerables a ataques comunes.

- **Procesos lentos de actualización de software**, lo que deja expuestos sistemas críticos por meses o años.

Aunque Ecuador cuenta con la **Ley Orgánica de Protección de Datos Personales**, su implementación estatal aún es insuficiente. Los incidentes masivos de filtración de datos (por ejemplo, registros de instituciones educativas, policiales o de salud) revelan la incapacidad actual para garantizar la seguridad informática en el sector público.

La debilidad de los sistemas estatales no es solo tecnológica, sino cultural. El Estado debe promover una cultura de ciberseguridad obligatoria en todas las instituciones, donde el funcionario comprenda que la información es un activo jurídico esencial y que su protección tiene la misma importancia que la seguridad física. Propongo implementar:

- "*Oficiales de protección de datos*" en cada entidad pública.

- Certificaciones obligatorias en seguridad digital para funcionarios que manejan información sensible.
- Sistemas de autenticación multifactor para toda la administración pública.

La seguridad del Estado depende, en gran medida, de la conducta humana y no solo de la tecnología.

5.3. Rol del Ministerio del Interior, CNT, ECU911, Fuerzas Armadas y Secretaría de Inteligencia

La gobernanza digital requiere una arquitectura institucional coordinada. En Ecuador, varias entidades participan en funciones de ciberseguridad, pero sin un marco operativo común. Su rol debería ser el siguiente:

- **Ministerio del Interior**

  - Liderar la política de seguridad interna digital.
  - Coordinar a la Policía Nacional en la persecución del delito informático.

- Gestionar el intercambio de información sobre amenazas entre instituciones.

➢ **Corporación Nacional de Telecomunicaciones (CNT)**

- Proteger la infraestructura de telecomunicaciones estatal y mixta.
- Garantizar protocolos de continuidad operativa en caso de ciberataques.
- Cooperar con la Agencia de Regulación y Control de Telecomunicaciones (ARCOTEL).

➢ **ECU911**

- Administrar sistemas de respuesta ante emergencias digitales.
- Integrar los incidentes cibernéticos dentro del Sistema Nacional de Prevención de Riesgos.
- Supervisar eventos que amenacen infraestructuras críticas (energía, agua, transporte, salud etc.).

- **Fuerzas Armadas**

    - Defender infraestructuras críticas que tengan dimensión estratégica nacional.
    - Implementar capacidades militares de ciberdefensa.
    - Coordinar con aliados regionales en amenazas de alto nivel.

- **Secretaría de Inteligencia (o Centro de Inteligencia Estratégica)**

    - Monitorear amenazas de alto riesgo, incluidos actores estatales y no estatales.
    - Producir inteligencia para decisiones de seguridad digital.
    - Establecer cooperación internacional para análisis de ciber amenazas.

Hoy estas instituciones trabajan de manera aislada, lo que reduce la capacidad nacional de respuesta. Es indispensable crear un *Sistema Nacional de Ciberseguridad y Ciberdefensa*, con un mando unificado

y un registro obligatorio de incidentes. La coordinación debe ser permanente, no reactiva. Sin integración interoperable no es posible garantizar seguridad en el entorno digital.

5.4. Relaciones entre ciberterrorismo y crimen organizado transnacional

El ciberterrorismo y el crimen organizado transnacional han encontrado en el ecosistema digital una plataforma para expandir sus operaciones. Estas amenazas convergen en actividades como:

- Ataques contra infraestructura crítica (energía, banca, servicios públicos).
- Secuestro de información mediante *ransomware*.
- Interferencia en comunicaciones estatales.
- Lavado de activos mediante criptomonedas.
- Extorsiones digitales y reclutamiento en línea.

La penetración de organizaciones criminales y la debilidad institucional han permitido que estas estructuras utilicen herramientas tecnológicas para coordinar ataques,

evadir controles, espiar comunicaciones o alterar sistemas públicos.

El ciberterrorismo, aunque menos visible, tiene la capacidad de paralizar instituciones enteras, creando caos social y vulnerabilidad estatal. La línea entre terrorismo tradicional y digital se vuelve difusa cuando los ataques buscan afectar la estabilidad democrática o causar pánico generalizado.

La lucha contra el ciberterrorismo debe abordarse desde una perspectiva regional. Ecuador no puede combatir solo a redes criminales que actúan simultáneamente en Colombia, Perú, Centroamérica y Europa. Propongo la creación de un **Mecanismo Andino de Ciberseguridad y Ciberdefensa**, que permita:

- Intercambio de inteligencia en tiempo real.
- Operaciones coordinadas contra redes digitales criminales.
- Protocolos transfronterizos contra ataques de alta complejidad.

El crimen organizado es global. La respuesta del Estado también debe serlo.

CAPÍTULO VI

Propuesta de Reforma al COIP

La transformación tecnológica global, el incremento de ataques cibernéticos y la creciente participación de organizaciones criminales en el ámbito digital han generado un nuevo escenario de riesgo para el Estado. El Código Orgánico Integral Penal (COIP), pese a incluir delitos informáticos y ciertas figuras relacionadas con la afectación a sistemas, no incorpora un tratamiento penal especializado para amenazas de alta complejidad, como el ciberterrorismo, la manipulación de algoritmos con fines ilícitos o el uso malicioso de inteligencia artificial (IA).

La presente propuesta ofrece una reforma estructural, sistemática y técnicamente actualizada para fortalecer la respuesta penal del Ecuador frente a riesgos que comprometen la seguridad nacional y la estabilidad institucional.

6.1. Redacción de un tipo penal autónomo de ciberterrorismo

El COIP carece de un tipo penal específico que sancione conductas terroristas ejecutadas mediante medios digitales, aun cuando los efectos de estos ataques pueden ser equivalentes o superiores a los del terrorismo tradicional. Un tipo penal autónomo permitiría:

- Tipificar conductas complejas y multiformes.
- Superar la dispersión normativa actual.
- Dotar a operadores de justicia de un marco claro y eficaz.

Propuesta de tipo penal (redacción sugerida)

Artículo X – Ciberterrorismo.

> *La persona que, mediante el uso de sistemas informáticos, redes de comunicación, inteligencia artificial o cualquier tecnología digital, ejecute, facilite o coordine actos destinados a provocar terror, intimidación colectiva, desestabilización*

institucional o afectación grave a infraestructuras críticas del Estado, será sancionada con pena privativa de libertad de veinte a treinta años.

La misma pena se aplicará cuando la conducta tenga por finalidad coaccionar a autoridades públicas, alterar el orden constitucional, interrumpir servicios esenciales o causar daños masivos a la población mediante ataques digitales.

Considero indispensable que el tipo penal defina con precisión los elementos objetivos y subjetivos:

- Uso de medios digitales,
- Finalidad terrorista o desestabilizadora,
- Afectación masiva.

Esto permitirá evitar interpretaciones abusivas o expansivas que vulneren libertades fundamentales.

6.2. Tipos penales complementarios

El ciberterrorismo debe complementarse con una serie de delitos conexos que respondan a daños intermedios, técnicas de ataque específicas y nuevas amenazas derivadas del uso de Inteligencia Artificial.

a) Sabotaje digital agravado

Artículo Y – Sabotaje digital agravado.

> *La persona que destruya, inutilice, altere o interfiera sistemas informáticos, redes, servidores o datos con la finalidad de afectar funciones estatales, servicios esenciales o actividades estratégicas será sancionada con pena privativa de libertad de diez a quince años.*
>
> *La pena será de quince a veinte años si la conducta se realiza contra sistemas de salud, seguridad pública, hidroelectricidad, transporte, banca pública o defensa nacional.*

b) Ataques a infraestructura crítica

Artículo Z – Ataque a infraestructura crítica digital.

Quien acceda, invada, manipule o interrumpa sistemas catalogados como infraestructura crítica del Estado será sancionado con pena privativa de libertad de doce a veinte años.

Se consideran infraestructuras críticas: energía, agua potable, telecomunicaciones, transporte, finanzas, defensa, seguridad interna, justicia y salud.

c) Manipulación de algoritmos que comprometan la seguridad nacional

Artículo A1 – Manipulación algorítmica con riesgo a la seguridad nacional.

La persona que manipule, altere, programe o desvíe algoritmos destinados al funcionamiento de servicios públicos, seguridad interna, defensa, procesos electorales o vigilancia estatal, con el fin

de obtener beneficios indebidos o causar daño a la estabilidad institucional, será sancionada con pena privativa de libertad de ocho a doce años.

d) Uso de inteligencia artificial para actos terroristas

Artículo A2 – Uso de inteligencia artificial con fines terroristas.

Quien diseñe, entrene, implemente o utilice sistemas de Inteligencia Artificial, modelos generativos, agentes autónomos o redes neuronales para la ejecución de actos terroristas o para facilitar la planificación, reclutamiento, financiamiento o anonimización de dichas actividades, será sancionado con pena privativa de libertad de quince a veinticinco años.

Sugiero que estos tipos penales incluyan definiciones normativas claras sobre lo que constituye:

- Infraestructura crítica,
- Algoritmos relevantes para seguridad nacional,

- IA utilizada para fines terroristas,
- Niveles de daño o riesgo.

La seguridad jurídica exige que la redacción sea técnica, pero comprensible para jueces y fiscales.

6.3. Reglas especiales de investigación

Los delitos informáticos de alta complejidad requieren técnicas de investigación distintas a las tradicionales. El COIP debe incorporar reglas específicas para garantizar eficacia sin vulnerar derechos fundamentales.

a) Agentes encubiertos digitales

Se propone incluir la figura del **agente encubierto digital**, quien:

- Operará bajo autorización judicial;
- Podrá infiltrarse en redes cerradas, foros clandestinos o canales cifrados;
- Podrá simular identidades digitales para detectar planificación de ataques;

- Estará sujeto a límites estrictos para evitar provocación delictiva.

b) Retención y preservación de metadatos

Se requiere obligar a proveedores de servicios digitales a:

- conservar metadatos (direcciones IP, registros de conexión, localización digital) por un plazo mínimo de 12 meses;
- implementar sistemas de resguardo técnico auditables;
- entregar información bajo orden judicial motivada.

c) Cooperación internacional inmediata

El COIP debe establecer procedimientos rápidos para:

- Intercambio de información con agencias extranjeras;
- Acceso a servidores ubicados fuera del país;
- Solicitudes de preservación de evidencia digital;

- Reconocimiento de estándares internacionales de cadena de custodia.

Propongo que se cree un **Centro Nacional de Respuesta Penal Digital**, integrado por Fiscalía, Policía, CNT y Fuerzas Armadas, con competencia exclusiva para investigar delitos de alta tecnología y coordinar cooperación internacional.

6.4. Incorporación de estándares del Convenio de Budapest (sin adhesión formal)

Aunque Ecuador no es parte del **Convenio de Budapest sobre Ciberdelincuencia**, puede adoptar sus estándares como buenas prácticas. Estos lineamientos internacionales fortalecen:

- La tipificación penal moderna,
- La preservación de datos,
- La cooperación transfronteriza,
- La cadena de custodia digital.

Entre los elementos aplicables destacan:

- Obligación de preservación rápida de datos.
- Facultades de registro de sistemas informáticos.
- Acceso transfronterizo a datos con consentimiento o urgencia.
- Definiciones armonizadas de ciberdelitos.

Sugiero incorporar estos estándares a través de una **Ley Orgánica de Ciberseguridad y Delitos Tecnológicos**, que complemente al COIP y permita una futura adhesión internacional. El país necesita una normativa moderna y compatible con sistemas globales de investigación.

CAPÍTULO VII
Análisis Crítico: Derecho Penal del Enemigo y Garantismo Digital

La incorporación de nuevos tipos penales relacionados con el ciberterrorismo y los ataques digitales plantea un debate complejo en el campo del derecho penal: **¿hasta qué punto debe fortalecerse la respuesta estatal sin comprometer garantías fundamentales?** El reto está en comprender que el ciberespacio es un entorno donde el Estado se encuentra particularmente vulnerable, lo que ha llevado a algunos autores a justificar modelos de hipercriminalización. Sin embargo, el derecho penal no puede renunciar ni a su matriz constitucional ni a los límites propios del Estado democrático de derecho.

7.1. ¿Debe endurecerse el derecho penal?

El surgimiento del ciberterrorismo y la sofisticación de los ataques digitales han generado un argumento recurrente: el derecho penal debe endurecerse para responder a estas amenazas. La posición se sustenta en tres premisas:

1. **Los ataques digitales pueden causar daños equiparables a actos terroristas físicos**: paralización de hospitales, interrupción de energía, manipulación de datos del Estado o afectación a infraestructuras críticas.
2. **La persecución penal es extremadamente difícil**, debido al anonimato y transnacionalidad de los agresores.
3. **La ineficiencia estatal obliga a un aumento del poder punitivo** para compensar debilidades operativas.

La teoría del derecho penal del enemigo (Jakobs) suele invocarse en estos casos: el Estado debe anticiparse y actuar con severidad frente a quienes representan una amenaza existencial. Bajo este enfoque, el ciberterrorista sería un actor que no respeta las reglas del contrato social, y por tanto no debe ser tratado como un ciudadano con plenos derechos.

Aunque es necesario fortalecer la tipificación y las facultades de investigación, considero que recurrir al

derecho penal del enemigo sería un error grave. Las experiencias comparadas muestran que este modelo termina expandiendo el poder punitivo más allá de los supuestos originales, afectando a la ciudadanía en general y debilitando el control de constitucionalidad.

7.2. Riesgos de desnaturalizar garantías constitucionales

El principal riesgo de ampliar el derecho penal frente al ciberterrorismo es desnaturalizar garantías constitucionales, especialmente en un país con debilidades institucionales. Los puntos críticos son:

- **Debilitamiento del principio de legalidad:** tipos penales demasiado amplios o vagos pueden permitir interpretaciones arbitrarias.
- **Restricciones excesivas a la privacidad digital:** retención indiscriminada de datos, vigilancia masiva o registros sin control judicial.
- **Afectación a la libertad de expresión:** discursos radicales o disensos políticos podrían ser catalogados como “ciberamenazas”.

- **Uso político del derecho penal:** gobiernos pueden manipular leyes antiterroristas para perseguir a opositores.

La experiencia latinoamericana muestra que leyes antiterroristas mal diseñadas terminan criminalizando protestas, activismo digital o investigaciones periodísticas.

El verdadero reto no es solo evitar la desnaturalización de garantías, sino diseñar herramientas legales que operen con precisión quirúrgica: fuertes contra los agresores, pero intocables frente a la ciudadanía. La tecnología permite control social total; por ello, cualquier expansión del poder investigativo debe tener límites claros, supervisión judicial continua y mecanismos de rendición de cuentas.

7.3. Ponderación entre derechos, seguridad y libertad digital

El análisis constitucional exige una ponderación entre:

- Seguridad nacional,
- Libertad digital,
- Privacidad,
- Derechos de acceso a la información,
- Garantías del debido proceso.

La Corte Interamericana de Derechos Humanos (CIDH) ha señalado que las limitaciones a los derechos deben cumplir:

1. Finalidad legítima,
2. Necesidad,
3. Proporcionalidad estricta.

La ponderación en materia digital es particularmente compleja porque:

- El volumen de datos es gigantesco.
- Los riesgos son globales y permanentes.
- La evidencia digital es volátil.
- Los ataques pueden producir daños irreversibles.

La ponderación debe partir de un principio: la seguridad digital no es opuesta a la libertad digital, sino condición de posibilidad de la misma.

Sin protección de infraestructuras críticas, datos personales y sistemas estatales, no es posible ejercer plenamente los derechos en el ciberespacio. El equilibrio no se logra reduciendo libertades, sino creando un entorno digital seguro y transparente.

7.4. Propuesta de equilibrio

Frente a las tensiones anteriores, es necesario establecer un modelo de equilibrio entre eficacia penal y garantismo digital. Se propone:

1. **Tipificación precisa y técnica**

Redactar tipos penales estrictos, sin cláusulas abiertas, evitando conceptos como “amenaza digital genérica”.

2. **Control judicial reforzado**

Toda medida intrusiva debe requerir autorización judicial motivada, con supervisión estricta y límites temporales.

3. **Transparencia estatal**

Las instituciones deben publicar informes anuales de: ataques digitales, investigaciones, técnicas especiales empleadas, resultados y eficacia.

4. **Especialización de operadores**

Un derecho penal más fuerte solo es legítimo si fiscales, jueces y peritos tienen alto nivel técnico. La ignorancia genera abusos y errores.

5. **Protección de la libertad digital**

Toda reforma debe incorporar principios de: neutralidad tecnológica, minimización de datos, seguridad por diseño, auditoría ciudadana de sistemas de vigilancia.

6. **Fomento de la cooperación internacional**

La seguridad digital exige coordinación transfronteriza, pero bajo criterios de protección de derechos humanos.

Creo que el equilibrio ideal no se basa en la expansión ilimitada del poder punitivo ni en un garantismo rígido que ignore amenazas reales. El punto medio es un

garantismo estratégico, que defiende derechos, pero reconoce la sofisticación del cibercrimen. La clave es la proporcionalidad: sanciones severas y técnicas invasivas solo cuando exista riesgo real y verificable para la seguridad nacional o para derechos fundamentales de gran escala.

CAPÍTULO VIII

Conclusiones Generales

El análisis del ciberterrorismo y su impacto en el sistema penal permite afirmar que el país enfrenta una amenaza para la cual aún no se encuentra preparado, ni en términos normativos, ni operativos, ni institucionales. El crecimiento acelerado de ataques digitales, la vulnerabilidad de las infraestructuras, la falta de especialización técnica y el vacío legislativo en el Código Orgánico Integral Penal han generado un escenario de riesgo permanente para la seguridad nacional, la estabilidad democrática y la confianza ciudadana en los servicios públicos. El análisis demuestra que el ciberterrorismo constituye una amenaza real, creciente y estructural para la seguridad y estabilidad institucional del Ecuador. Su naturaleza transnacional, anónima, modular y altamente técnica supera con amplitud la capacidad actual del Estado para prevenir, investigar y sancionar ataques que comprometen derechos fundamentales, infraestructuras críticas y funciones esenciales.

Este capítulo presenta una síntesis doctrinaria, jurídica y política, así como un modelo de política criminal moderna para Ecuador y recomendaciones dirigidas a operadores de justicia y legisladores.

El presente libro ha buscado aportar una visión integral, técnica y crítica sobre estos desafíos, proponiendo mecanismos de fortalecimiento jurídico y político-criminal orientados a la protección del Estado y de los derechos fundamentales en el entorno digital.

8.1. Síntesis doctrinaria y jurídica

Desde un punto de vista doctrinario, el ciberterrorismo debe entenderse como una categoría autónoma dentro del derecho penal contemporáneo, con elementos estructurales propios:

1. **Medios digitales como herramienta de ataque:** la violencia se ejecuta mediante sistemas informáticos, algoritmos, malware, IA o redes distribuidas.

2. **Finalidad terrorista:** provocar miedo colectivo, interrumpir funciones estatales o desestabilizar instituciones democráticas.
3. **Daño masivo e inmaterial:** afectación inmediata a servicios esenciales sin necesidad de presencia física.

La dogmática penal demuestra que los tipos penales tradicionales, sabotaje, terrorismo clásico, ataque a sistemas informáticos, no logran abarcar las dimensiones complejas del fenómeno. Falta un tipo específico que articule finalidad terrorista + medios digitales + afectación crítica.

Desde la perspectiva constitucional, quedó claro que fortalecer el poder punitivo sin límites puede vulnerar principios como:

- Legalidad,
- proporcionalidad,
- necesidad,
- presunción de inocencia,
- protección de datos personales.

El equilibrio debe darse entre seguridad y libertad digital, evitando caer en modelos de derecho penal del enemigo, que erosionan garantías básicas.

A mi criterio, Ecuador se encuentra ante un punto de inflexión: puede seguir con un derecho penal reactivo y fragmentado, o construir una doctrina penal moderna, técnica y garantista que responda al siglo XXI sin sacrificar los cimientos del Estado constitucional.

8.1.1. El ciberterrorismo como categoría autónoma

No puede ser reducido a una simple variante del terrorismo tradicional ni a un delito informático agravado. Su esencia radica en su capacidad de generar daño masivo a través de medios digitales, con anonimato, transaccionalidad y costos operativos mínimos. Doctrinariamente, representa la convergencia entre la violencia política y el poder tecnológico.

8.1.2. Insuficiencia del marco penal actual

El COIP, desde su entrada en vigencia en 2014, no ha evolucionado al ritmo del entorno digital. Sus delitos informáticos son genéricos, técnicamente limitados y no abarcan fenómenos como:

- ataques algorítmicos,
- uso de IA para fines terroristas,
- sabotaje digital de infraestructura crítica,
- manipulación masiva de datos estatales.

Esta omisión genera vacíos de tipicidad que impiden una persecución eficaz.

8.1.3. El rol del garantismo digital

La respuesta penal frente al ciberterrorismo debe ser firme, pero no ilimitada. Un Estado que combate amenazas digitales sacrificando derechos digitales termina debilitando su legitimidad y fortaleciendo el autoritarismo. El garantismo aplicado al entorno digital implica:

- proporcionalidad estricta,
- precisión normativa,
- control judicial reforzado,
- transparencia institucional,
- auditoría tecnológica.

8.1.4. Responsabilidad del Estado en la gobernanza digital

El Estado no ha desarrollado una estrategia nacional de ciberseguridad sólida, ni ha modernizado sus sistemas ni capacitado adecuadamente a sus operadores. La vulnerabilidad no solo proviene del atacante, sino también de la fragilidad institucional.

8.1.5. Necesidad de una política criminal preventiva y especializada

El delito digital requiere anticipación, análisis de riesgos, cooperación internacional, infraestructura tecnológica y operadores de justicia altamente capacitados.

8.2. Modelo de política criminal moderna para Ecuador

Una política criminal adecuada debe ser **integral**, **interinstitucional** y **técnica**, no meramente reactiva. Se propone un modelo estructurado en cinco ejes:

- **Prevención estratégica: Estado fuerte y resiliente**
  - Creación de una Estrategia Nacional de Ciberseguridad con rango legal.
  - Fortalecimiento de la infraestructura crítica y adopción de estándares internacionales.
  - Auditorías permanentes de vulnerabilidades en entidades públicas.
- **Reformas normativas inteligentes**
  - Incorporación de un tipo penal autónomo de ciberterrorismo.

- Tipos complementarios: sabotaje digital agravado, manipulación algorítmica, uso de IA con fines terroristas.
- Reglas especiales y controladas de investigación digital: agentes encubiertos, retención de metadatos, cooperación internacional.

➢ **Especialización de operadores**

- Creación de una Fiscalía Nacional de Cibercrimen y Terrorismo Digital.
- Unidades de la Policía Nacional exclusivamente dedicadas a delitos de alta tecnología.
- Peritos certificados y laboratorios con acreditación internacional.

➢ **Coordinación interinstitucional**

- Participación integrada del:
- Ministerio del Interior,

- Fuerzas Armadas,
- CNT,
- ECU911,
- Secretaría de Inteligencia.

Debe existir un Centro Nacional de Respuesta Penal Digital, encargado de la coordinación técnica y operativa.

- **Garantismo digital como principio rector**
  - Mecanismos de supervisión judicial estricta.
  - Minimización de datos y protección de privacidad.
  - Auditorías públicas para evitar abusos.

Considero que la política criminal moderna debe asumir que la defensa del ciberespacio no es solo cuestión de seguridad, sino de preservación democrática. La tecnología puede fortalecer o destruir libertades; el derecho debe decidir hacia dónde se inclina la balanza.

Se propone un modelo de política criminal digital basado en cinco pilares estratégicos:

- **Normativa penal moderna y específica**

Incluye:

- Tipo penal autónomo de ciberterrorismo,
- Delitos complementarios de sabotaje digital agravado, manipulación algorítmica e IA con fines terroristas,
- Reglas especiales de investigación digital,
- Estándares del Convenio de Budapest.

8.3. Necesidad jurídica y constitucional de un tipo penal autónomo

El ordenamiento penal ecuatoriano carece actualmente de una disposición que sancione específicamente el ciberterrorismo como manifestación autónoma del terrorismo moderno. El artículo 366 del COIP tipifica el terrorismo en sus modalidades tradicionales (uso de explosivos, armas, violencia física, intimidación), pero no

contempla la modalidad digital, que constituye hoy una de las amenazas más graves para la seguridad nacional.

Desde una perspectiva constitucional, la protección del Estado frente a amenazas que comprometen la integridad institucional, la gobernabilidad democrática y los servicios esenciales forma parte del derecho a la seguridad integral previsto en los artículos 3, 66 numeral 3, 158, 389 y 393 de la Constitución de la República. El Estado tiene el deber jurídico de prevenir, investigar y sancionar conductas terroristas, incluso en sus manifestaciones tecnológicas contemporáneas.

La ausencia de regulación específica genera impunidad, pues los operadores de justicia se ven obligados a encajar conductas digitalmente complejas dentro de tipos penales insuficientes (sabotaje, ataque a sistemas informáticos, terrorismo clásico), produciendo interpretaciones forzadas, reclasificaciones y archivos de causa.

8.3.1. Naturaleza particular del ciberterrorismo

La doctrina reconoce al ciberterrorismo como una forma autónoma del terrorismo, con características propias que justifican su tipificación independiente. Según Denning (2017), el ciberterrorismo consiste en *ataques premeditados, políticamente motivados y dirigidos contra sistemas computacionales, redes de información, infraestructuras críticas o servicios digitales esenciales*, con el fin de causar miedo, desestabilizar instituciones o coaccionar al Estado.

A diferencia del terrorismo físico, el ciberterrorismo presenta:

- Capacidad transnacional inmediata y anonimato elevado.
- Bajo costo operativo y uso de infraestructura tecnológica legítima.
- Capacidad de paralizar servicios esenciales (energía, salud, banca, transporte, comunicaciones).

- Difusión masiva y automática del daño, sin presencia física del agresor.
- Alta volatilidad y complejidad probatoria, que dificulta persecución penal.

Estas características evidencian que el ciberterrorismo no es una variante técnica del terrorismo, sino una nueva categoría criminológica que requiere un tratamiento penal autónomo.

8.3.2. Derecho comparado y estándares internacionales

Numerosos países han tipificado el ciberterrorismo como figura independiente, entre ellos:

- **España:** LO 10/2021 incorpora delitos graves contra infraestructura crítica.
- **Colombia:** Ley 1273 sanciona atentados digitales agravados cuando comprometen seguridad nacional.
- **Chile:** Ley 21.459 introduce sabotaje informático agravado y protección de infraestructura crítica.

- **Estados Unidos:** El *Patriot Act* define ciberterrorismo como ataque digital que busca coacción política.
- **Unión Europea:** Directiva 2013/40/UE incluye ataques agravados contra servicios esenciales.

La Budapest Convention, aunque Ecuador no es parte establece principios para sancionar ataques a sistemas informáticos cuando comprometen infraestructura crítica, lo cual respalda la creación de tipos penales especializados.

El derecho comparado muestra un consenso internacional: los ataques digitales dirigidos a afectar funciones esenciales del Estado requieren una respuesta penal diferenciada.

8.3.3. Justificación técnica desde la política criminal

Los delitos informáticos tipificados actualmente en el COIP (arts. 229–233) fueron diseñados para infracciones de menor escala: acceso ilícito, violación de claves,

sabotaje informático, interceptación de datos. No fueron estructurados para afrontar atentados que:

- buscan fines terroristas o políticos;
- comprometen infraestructura crítica nacional;
- causan colapso de servicios públicos esenciales;
- tienen impacto en la estabilidad democrática;
- se vinculan con crimen organizado transnacional;
- emplean inteligencia artificial o herramientas avanzadas de automatización.

El sistema penal enfrenta una crisis estructural debido a esta falta de adecuación normativa: no puede responder eficazmente a ciberataques de alta complejidad.

8.3.4. Principio de legalidad y prohibición de analogía penal

El artículo 76 numeral 3 de la Constitución y el artículo 5 del COIP sancionan la aplicación analógica del derecho penal. Por ello, no es jurídicamente válido extender el tipo de terrorismo tradicional al ámbito digital mediante

interpretación extensiva, pues esto vulneraría el principio de tipicidad.

La ausencia de una figura penal autónoma genera:

- vacuidad normativa,
- imposibilidad de atribución penal,
- criterios discrecionales de fiscales y jueces,
- archivos por atipicidad,
- debilitamiento de la política criminal del Estado.

Por esta razón, la autonomía del tipo penal no solo es conveniente, sino constitucionalmente necesaria.

8.4. Propuesta de texto normativo para el COIP

A continuación, se presenta un posible artículo que puede incorporarse después del artículo 366:

Artículo XXX. Ciberterrorismo

> *La persona que, mediante el uso de tecnologías de la información, redes digitales, sistemas informáticos, inteligencia artificial, o cualquier*

medio electrónico, realice acciones destinadas a afectar, interrumpir, inutilizar o controlar infraestructuras críticas, servicios públicos esenciales, sistemas de seguridad del Estado, instituciones gubernamentales o plataformas estratégicas, con el fin de causar terror, intimidar a la población, desestabilizar el orden constitucional o coaccionar a las autoridades públicas, será sancionada con pena privativa de libertad de veinte a treinta años.

Constituyen circunstancias agravantes:

1. *Si el ataque compromete sistemas de salud, agua potable, energía eléctrica, transporte, banca, defensa, seguridad interna o emergencias.*
2. *Si se genera difusión masiva automatizada mediante inteligencia artificial o redes de bots.*
3. *Si el autor pertenece a una organización terrorista nacional o transnacional.*

4. *Si se ocasiona muerte, lesiones graves o pérdidas económicas superiores a los límites previstos legalmente.*

8.5. Inclusión en el COIP: impacto y beneficios

La incorporación de un tipo penal autónomo permitirá:

- Adaptar el sistema penal ecuatoriano a la era digital.
- Fortalecer la política criminal contra amenazas tecnológicas avanzadas.
- Proteger la infraestructura crítica nacional.
- Reducir la impunidad en ataques sofisticados.
- Armonizar el COIP con estándares internacionales.
- Mejorar la cooperación con agencias extranjeras de ciberseguridad.
- Garantizar una persecución penal efectiva y constitucionalmente legítima.

8.5.1. Profesionalización especializada

Crear unidades élite en:

- Fiscalía,
- Policía Nacional (ciberdelitos),
- CNT,
- ECU911,
- Fuerzas Armadas.

Estas unidades deben operar con conocimientos avanzados en forensia digital, ciberinteligencia, análisis de malware, blockchain, algoritmos y redes.

8.5.2. Infraestructura de ciberseguridad estatal

Se requiere:

- centros de respuesta ante incidentes,
- sistemas cifrados,
- protección de bases de datos públicas,
- auditorías técnicas periódicas,
- protocolos de continuidad operativa para infraestructura crítica.

8.5.3. Política criminal preventiva

Debe incluir:

- alertas tempranas,
- análisis de amenazas,
- cooperación con sector privado,
- educación digital para funcionarios públicos y población en general.

8.5.4. Gobernanza interinstitucional

El Estado debe crear un Consejo Nacional de Ciberseguridad y Política Penal Digital, encargado de articular decisiones entre todas las instituciones involucradas. Un país fragmentado no puede defenderse de un enemigo digital altamente coordinado.

8.6. Recomendaciones para jueces, fiscales, policías y legisladores

Para jueces

Exigir argumentación técnica en medidas intrusivas.

Garantizar la cadena de custodia digital con criterios científicos.

Aplicar el principio de proporcionalidad en investigaciones sobre datos sensibles.

Aceptar pericias tecnológicas complejas solo de expertos certificados.

Para fiscales

Impulsar líneas de investigación digital desde el inicio del proceso.

Solicitar retención urgente de metadatos.

Coordinar con unidades transnacionales (INTERPOL, Europol, 24/7 Cybercrime Network).

Capacitarse de manera continua en análisis de evidencia digital.

Para la Policía Nacional

Implementar protocolos digitales de primera respuesta.

Preservar evidencia volátil mediante herramientas forenses.

Crear unidades especializadas en OSINT, caza de amenazas, análisis de malware y rastreo de criptomonedas.

Coordinar con proveedores tecnológicos y sector privado.

Para legisladores

Aprobar reformas penales altamente técnicas y precisas.

Evitar leyes expansivas que vulneren derechos fundamentales.

Financiar la infraestructura tecnológica estatal y los laboratorios forenses.

Establecer mecanismos de control legislativo sobre las prácticas de vigilancia digital.

Creo firmemente que cualquier reforma será inútil si no se acompaña de educación continua, inversión en tecnología y especialización real. No basta con cambiar el COIP: se necesita transformar la cultura jurídica y operativa del país frente a las amenazas digitales.

El Ecuador enfrenta un reto histórico: adaptar su derecho penal y su sistema de seguridad al siglo XXI. El ciberterrorismo no es un fenómeno hipotético, sino una amenaza latente que ha demostrado su capacidad de afectar la estabilidad institucional. La respuesta estatal debe ser firme, técnica y garantista.

Este libro ha propuesto una hoja de ruta para fortalecer la legislación penal, modernizar la política criminal, profesionalizar operadores y construir una defensa efectiva del espacio digital, sin renunciar a los principios constitucionales que sostienen la democracia.

CAPÍTULO IX

Delitos Complementarios al Tipo Penal De Ciberterrorismo

Fundamentación doctrinaria, jurídica, criminológica y técnico-digital para su incorporación al COIP

9.1. Necesidad de delitos complementarios: razones estructurales

El ciberterrorismo es una amenaza compleja, multidimensional y altamente sofisticada. Sin embargo, no todas las conductas preparatorias o auxiliares al ciberterrorismo alcanzan el umbral típico del "ataque terrorista digital", lo que genera un grave vacío en la política criminal del Ecuador.

Actualmente, el COIP contempla:

- **sabotaje informático básico** (art. 232),
- **interferencia en sistemas y datos** (arts. 229–233),
- **terrorismo** (art. 366).

Estos tipos penales fueron diseñados antes de la revolución de la IA, del auge de infraestructuras críticas altamente digitalizadas y del incremento de ataques estatales o paraestatales.

Por lo tanto:

- El COIP no permite sancionar la fase preparatoria avanzada del ciberterrorismo, tales como:

- manipulación de algoritmos de inteligencia artificial para generar caos;
- modificación de sistemas automatizados que controlan energía, agua, transporte, hospitales;
- inyección de malware persistente destinado a activarse posteriormente;
- creación de deepfakes terroristas para desestabilizar al Estado;
- programación de bots armados digitalmente para colapsar redes institucionales.

En Derecho Penal contemporáneo, los delitos preparatorios cualificados son indispensables para delitos

de altísima lesividad (terrorismo, crimen organizado, lavado, corrupción, trata). Lo mismo ocurre en el plano digital.

9.2. Delito complementario: Sabotaje Digital Agravado

Fundamentación jurídica

El sabotaje digital afecta bienes jurídicos como:

- Funcionamiento del Estado,
- Seguridad pública,
- Continuidad de servicios esenciales,
- Confianza digital institucional,
- Estabilidad económica,
- Integridad de infraestructuras críticas.

La doctrina penal moderna (Boehm, 2020; Schjolberg, 2021) clasifica al sabotaje informático como un delito de peligro abstracto y concreto, dependiendo del nivel de afectación.

El sabotaje informático del COIP es insuficiente, porque:

- No distingue entre sabotaje simple y sabotaje crítico (por ejemplo, contra hospitales o energía eléctrica).
- No reconoce la finalidad terrorista como agravante.
- No sanciona ataques a sistemas estatales estratégicos.
- No considera formas modernas de sabotaje: ransomware, wipers, ataques DDoS masivos, inyección de código malicioso persistente, etc.

Fundamentación técnico-digital

Los ataques actuales incluyen técnicas avanzadas como:

- *Distributed Denial of Service (DDoS)* contra plataformas gubernamentales.
- *Ransomware* que paraliza hospitales y municipalidades.
- Inserción de *logic bombs* programadas para activarse en momentos de crisis política.

- Destrucción de sistemas SCADA y PLC utilizados en energía, agua, transporte o telecomunicaciones.

Estas acciones **no siempre constituyen ciberterrorismo**, pero son **delitos puente o de facilitación**.

Propuesta de texto legal

Artículo XXX – Sabotaje digital agravado

> *La persona que destruya, inutilice, altere, modifique o interrumpa sistemas informáticos, redes digitales, bases de datos o infraestructuras tecnológicas del sector público o privado, afectando la prestación de servicios esenciales o estratégicos, será sancionada con pena privativa de libertad de diez a quince años.*

Agravantes específicas:

1. *Si la conducta recae sobre infraestructura crítica nacional.*

2. *Si la acción se realiza con fines terroristas, desestabilización institucional o coacción a autoridades.*
3. *Si se utiliza malware avanzado, ransomware, IA o técnicas de anonimización sofisticada.*
4. *Si se generan pérdidas económicas o institucionales de alta magnitud.*

9.3. Delito complementario 2: Ataques a Infraestructura Crítica

Fundamentación jurídica

La infraestructura crítica es indispensable para la supervivencia del Estado. Según estándares internacionales (ENISA, NIST, Unión Europea), incluye:

- Energía eléctrica,
- Hidrocarburos,
- Agua potable,
- Telecomunicaciones,
- Salud y hospitales,
- Banca y sistema financiero,
- Transporte,

- Seguridad interna,
- Comunicaciones gubernamentales.

Un ataque a estas infraestructuras puede paralizar la vida del país, por ejemplo:

- un apagón nacional,
- Colapso de centrales hidroeléctricas,
- Corte de suministro de agua,
- Caída de la banca,
- Paralización del ecu-911,
- Ataque a bases de datos policiales o militares,
- Sabotaje a radares o sistemas de defensa.

Pese a esta gravedad, el COIP no contiene un tipo penal autónomo que proteja la infraestructura crítica por vía digital.

Fundamentación político-criminal

Los Estados modernos equiparan el ataque a infraestructura crítica con actos terroristas. Ecuador es especialmente vulnerable porque:

- Posee un sistema eléctrico altamente centralizado,
- Su infraestructura gubernamental digital es débil,
- Existen antecedentes de hackeos estatales y filtración de datos masiva,
- El país es blanco del crimen organizado transnacional,
- El uso de IA por bandas criminales ya es una amenaza real.

Propuesta de texto legal

Artículo XXX – Ataques a infraestructura crítica

> *La persona que, mediante medios digitales o electrónicos, afecte, interrumpa, modifique, controle o inutilice infraestructura crítica nacional o servicios esenciales del Estado o del*

sector privado, será sancionada con pena privativa de libertad de quince a veinte años.

Infraestructura crítica incluye, entre otras: energía, agua, petróleo, bancos, telecomunicaciones, salud, transporte, seguridad, servicios de emergencia, defensa.

9.4. Delito complementario 3: Manipulación Algorítmica o IA con Fines Terroristas

Este es el tipo penal más innovador y responde a una realidad creciente: la inteligencia artificial se ha convertido en arma criminal.

9.4.1. Fundamentación científica y técnica

La IA permite:

- Generar *deepfakes* que simulan discursos oficiales, desinforman o provocan pánico;
- Manipular algoritmos de tráfico de ciudades;
- Alterar sistemas de hospitales o distribución de oxígeno;

- Controlar drones, robots o sistemas automatizados;
- Automatizar ataques masivos con bots;
- Alterar modelos predictivos gubernamentales;
- Manipular sistemas de votación o recuento electoral.

Estas conductas pueden ser preparatorias del ciberterrorismo, pero no están tipificadas.

9.4.2. Fundamentación jurídica

El Derecho Penal debe anticiparse al riesgo extraordinario que representa la IA utilizada como arma (Wittes, 2022). Los sistemas automatizados pueden causar:

- Daños masivos,
- Desinformación generalizada,
- Pánico social,
- Alteración del orden democrático,
- Ataques simultáneos sin intervención humana directa.

La manipulación algorítmica constituye un peligro concreto para la seguridad nacional.

9.4.3. Propuesta de texto legal

Artículo XXX – Manipulación algorítmica o uso de IA con fines terroristas

> *La persona que diseñe, entrene, modifique, utilice o manipule sistemas algorítmicos, inteligencia artificial, redes neuronales, automatismos digitales o programas autónomos con el fin de generar terror, coaccionar a autoridades, desestabilizar el orden constitucional o facilitar actos de ciberterrorismo, será sancionada con pena privativa de libertad de doce a dieciocho años.*

Se consideran especialmente graves:

1. *La creación de deepfakes estatales o militares destinados a generar pánico o caos social.*
2. *La manipulación de algoritmos de infraestructura crítica o servicios esenciales.*

3. *El uso de IA para dirigir ataques automatizados o autónomos.*
4. *El uso de IA para interferir en elecciones, seguridad, defensa o comunicaciones del Estado.*

9.5. Integración sistemática en el COIP

Los delitos complementarios deben integrarse en un nuevo **Título o Capítulo**:

"De los delitos contra la seguridad digital del Estado y la infraestructura crítica"

Incluiría:

1. Ciberterrorismo
2. Sabotaje digital agravado
3. Ataques a infraestructura crítica
4. Manipulación algorítmica o IA con fines terroristas
5. Delitos preparatorios (alistamiento digital, provisión de herramientas de hacking, etc.)

9.6. Beneficios jurídico-penales de incorporar estos tipos

✔ Garantiza el principio de legalidad (art. 76.3 Const.)

✔ Reduce la impunidad en ataques tecnológicos complejos

✔ Protege la infraestructura crítica del Estado

✔ Da herramientas reales a fiscales, jueces y peritos

✔ Moderniza el COIP y lo adapta al siglo XXI

✔ Facilita cooperación internacional en cibercrimen

✔ Disuade ataques transnacionales

✔ Protege la democracia frente a manipulación algorítmica.

CAPÍTULO X

Reglas Especiales de Investigación Digital: Fundamentación Doctrinaria y Jurídica

La criminalidad digital especialmente aquella vinculada a ciberterrorismo, sabotaje a infraestructuras críticas, manipulación algorítmica o uso de IA para fines ilícitos, presenta características que desbordan por completo las herramientas tradicionales de investigación penal. Esta realidad justifica la incorporación de reglas especiales de investigación que, aunque excepcionales, se ajusten a los estándares internacionales de derechos humanos.

A continuación, se desarrolla la fundamentación profunda para cada una.

10.1. Necesidad Constitucional y Legal de Reglas Especiales de Investigación Digital

10.1.1. Principio de eficacia del ius puniendi

El Estado está constitucionalmente obligado a proteger bienes jurídicos, como la seguridad nacional, continuidad

de servicios esenciales, infraestructura crítica, integridad del sistema financiero y orden democrático.

Los ciberdelitos avanzados se caracterizan por:

- Anonimato del atacante.
- Velocidad y volatilidad de la evidencia digital.
- Transnacionalidad inmediata.
- Uso de cifrado y redes privadas virtuales.
- Ataques automatizados o autónomos mediante IA.

Los medios tradicionales de investigación resultan insuficientes ante criminales que operan en:

- redes cifradas (TOR, I2P),
- plataformas descentralizadas (P2P, blockchain),
- infraestructura cloud en múltiples jurisdicciones,
- inteligencia artificial generativa y scripts autónomos.

Por tanto, la proporcionalidad inversa exige que, a mayor sofisticación tecnológica, el Estado cuente con herramientas capaces de responder en el mismo nivel.

10.2. Fundamentación para cada regla especial

10.2.1 Agentes encubiertos digitales

Fundamento técnico

Los grupos ciberterroristas, hacktivistas o sindicatos criminales usan plataformas cerradas:

- Canales cifrados en Telegram, Signal u otros,
- Foros clandestinos en Dark Web,
- Mercados ilícitos digitales,
- Servidores privados con acceso solo por invitación,
- Redes P2P con autenticación por reputación.

La única forma de acceder a esos espacios es infiltrarse digitalmente, ya que no existen equivalentes "presenciales" para operaciones clásicas de encubierto.

Fundamento doctrinario

- La infiltración digital es equivalente funcional a la infiltración física.

- Está amparada en la doctrina del agente encubierto aceptada en casi todas las legislaciones de la región.

Responde al principio de necesidad investigativa ante criminalidad altamente clandestina.

Fundamento constitucional

La jurisprudencia comparada admite operaciones encubiertas si cumplen:

1. Control judicial previo.
2. Proporcionalidad.
3. No inducción al delito (entrapment).

Justificación para el COIP

El COIP ya regula agentes encubiertos para droga, crimen organizado y corrupción. El ciberterrorismo tiene complejidad igual o mayor, por lo que su exclusión carece de lógica sistemática.

Se propone:

> *"El agente encubierto digital podrá interactuar mediante identidad simulada en entornos virtuales, infiltrarse en sistemas, foros, redes o plataformas donde existan indicios fundados de planeación o ejecución de delitos informáticos o de ciberterrorismo, con autorización judicial previa."*

10.2.2 Retención y preservación de metadatos

Fundamento técnico

Los metadatos son muchas veces la única evidencia cierta de un ataque:

- Direcciones IP,
- Timestamps de transmisión,
- Registros de acceso a servidores,
- Logs de auditoría,
- Hash de archivos.

El problema: los metadatos se sobrescriben entre 24 horas y 7 días, dependiendo de la política del proveedor.

Fundamento doctrinario

- Para Silva Sánchez, los delitos informáticos requieren "prueba de rastro", no de contenido.
- Para Bock y Brenner, la retención de metadatos es esencial para reconstrucción del *modus operandi*.

Fundamento constitucional

La Corte IDH ha establecido que:

- La injerencia en comunicaciones requiere proporcionalidad.
- Sin embargo, los metadatos no tienen la misma intensidad intrusiva que el contenido.

Esto permite una regulación especial con menor umbral de restricción.

Justificación para el COIP

Ecuador carece completamente de una obligación legal de preservar evidencia digital.

Esto provoca que:

- los proveedores borren registros necesarios,
- la Fiscalía dependa de voluntariedad empresarial,
- casos complejos se archiven por imposibilidad técnica.

Por ello se propone:

"Los proveedores de servicios digitales deberán conservar metadatos esenciales por 12 meses en casos investigados por delitos informáticos graves, ciberterrorismo y ataques a infraestructura crítica, previa orden motivada de autoridad judicial."

10.2.3 Cooperación internacional inmediata

Fundamento técnico

El 90% de la evidencia digital en Ecuador está alojada en:

- Google Cloud,
- Meta,
- Amazon Web Services,
- proveedores extranjeros,
- registros DNS ubicados fuera del país.

Los protocolos actuales (cartas rogatorias, asistencia penal internacional) tardan entre 6 y 12 meses, tiempo en el cual la evidencia:

- ha expirado,
- ha sido borrada,
- o ya no es útil.

Fundamento doctrinario e internacional

- La Convención de Budapest (Estándares globales) exige
  respuesta inmediata a requerimientos de preservación digital.
- Naciones Unidas en su *Cybercrime Assessment* recomienda cooperación en tiempo real.

- La Corte Europea ha admitido medidas transfronterizas rápidas cuando la evidencia es volátil.

Fundamento constitucional

La cooperación internacional forma parte del **deber del Estado de proteger derechos** mediante políticas públicas eficaces.

Justificación para el COIP

Ecuador, aunque no sea parte aún de Budapest, puede incorporar sus estándares internamente como:

"Cooperación internacional inmediata mediante canales directos entre Policía, Fiscalía y proveedores extranjeros, válida como evidencia, siempre con control judicial posterior."

Esta fórmula permite actuar rápido sin vulnerar garantías.

10.2.4 Otras reglas especiales que pueden incluirse

A. Allanamientos digitales remotos (live forensics).

Permiten capturar evidencia en tiempo real sin necesidad de presencia física.

B. Interceptación de tráfico cifrado mediante captura de endpoints.

No rompe cifrado; actúa en origen o destino.

C. Monitorización de botnets y servidores comando-control.

Aceptada internacionalmente para neutralizar ataques masivos.

10.3. Principios garantistas para limitar estas medidas

Para evitar abusos, todas las reglas deben sustentarse en:

1. Autorización judicial previa, fundada y motivada.
2. Control de proporcionalidad, aplicable especialmente en casos de peligro para infraestructura crítica.

3. Registro de auditoría, para prevenir manipulaciones.
4. Validez limitada a delitos graves definidos en la reforma.
5. Protecciones reforzadas para derechos de privacidad.

Las reglas especiales de investigación digital no son un privilegio del Estado, sino una consecuencia lógica de:

- la naturaleza volátil, criptográfica y transnacional de la evidencia,
- la sofisticación de los actores criminales,
- la necesidad de garantizar seguridad nacional y continuidad institucional,
- y el compromiso constitucional del Ecuador de proteger bienes jurídicos superiores.

Incorporarlas en el COIP significa modernizar el sistema penal, alinearlo con estándares internacionales y asegurar que la lucha contra el ciberterrorismo sea eficaz, proporcional y ajustada a derechos humanos.

CAPÍTULO XI

Estándares del Convenio de Budapest Sobre Cibercrimen

Fundamentación para su incorporación en el sistema penal ecuatoriano

El Convenio sobre Ciberdelincuencia del Consejo de Europa (2001), conocido como Convenio de Budapest, constituye el instrumento jurídico internacional más avanzado y adoptado a nivel mundial para la lucha contra los delitos informáticos y la regulación de la evidencia digital. A pesar de no ser parte del convenio, Ecuador puede adoptar sus estándares internamente para modernizar el COIP, el Código Orgánico de la Función Judicial y los protocolos de investigación digital.

A continuación, se desarrollan los principios, obligaciones y estándares técnicos y jurídicos, con una justificación para la realidad ecuatoriana.

11.1. Estándares sustantivos (tipos penales mínimos)

El Convenio fija cuatro grupos esenciales de delitos, considerados el "mínimo universal" que toda legislación debe tipificar.

Acceso ilícito (hacking)

- Acceso no autorizado a sistemas informáticos.
- Base para combatir intrusiones, espionaje digital, ransomware y ataques a infraestructura crítica.

Relevancia para Ecuador: El COIP regula algunos supuestos, pero su redacción es dispersa y no define claramente accesos con fines terroristas, espionaje o manipulación algorítmica. Se requiere tipo penal autónomo y detallado.

Interceptación ilegal

- Captura no autorizada de datos en tránsito o almacenados.
- Incluye sniffing, ataques MITM, y técnicas de escucha digital.

Relevancia local: El COIP no regula adecuadamente la interceptación de datos no contenidos en comunicaciones tradicionales.

Interferencia en datos e interferencia en sistemas

- Borrado, deterioro, modificación o supresión de datos.
- Sabotaje digital, ataques DDoS, alteración de algoritmos o data poisoning.

Relevancia local: Los tipos del COIP son insuficientes, no contemplan agravantes para infraestructura crítica ni para fines terroristas.

Uso indebido de dispositivos

- Creación, difusión o tenencia de programas maliciosos (malware).
- Herramientas de hacking, keyloggers, botnets, ransomware kits.

Justificación para Ecuador: Es necesario penalizar la preparación y facilitación del delito, no solo la ejecución.

11.2. Estándares probatorios y procesales

Budapest es fundamental por su capítulo sobre obtención de evidencia digital, con estándares específicos que ningún otro instrumento internacional desarrolla con tanta claridad.

Preservación rápida de datos (art. 16)

- Permite que el Estado ordene a un proveedor la preservación inmediata de metadatos.
- Plazo: urgente, antes de que se borren automáticamente.

Fundamento para Ecuador: La evidencia digital usualmente desaparece en horas.
Sin esta medida, es imposible obtener IP, logs o registros de acceso.

Conservación y revelación de tráfico (art. 17 y 18)

- Preservación extendida por orden judicial.
- Posibilidad de obtener información del abonado.

Ventaja: No implica interceptar contenido; por tanto, es menos invasiva.

Facultades de registro y allanamiento digital (art. 19)

- Autoriza el allanamiento remoto, búsqueda de dispositivos, acceso a cuentas cloud, servidores externos o sistemas cifrados.

Necesidad para Ecuador: El COIP no regula allanamientos digitales ni órdenes de acceso a datos cloud, causando vacíos investigativos.

Recolección en tiempo real de tráfico y contenido (arts. 20 y 21)

- Permite capturar datos mientras se generan.
- Aplicable para ataques en curso (ransomware, DDoS, intrusiones persistentes).

Relevancia: La evidencia digital es dinámica; sin captación en tiempo real, la investigación pierde eficacia.

11.3. Estándares de cooperación internacional

La verdadera fortaleza del Convenio de Budapest es su sistema de cooperación global rápida, imprescindible para Ecuador debido a que:

- Más del 90% de la evidencia está en servidores extranjeros.
- Las cartas rogatorias demoran entre 6 y 12 meses.
- Los ciberdelincuentes actúan desde múltiples países.

Cooperación inmediata (24/7 Network)

- Cada país debe tener un punto de contacto disponible 24/7 para requerimientos urgentes.
- Facilita preservar logs, metadatos, direcciones IP y registros críticos.

Propuesta para Ecuador: Crear una unidad 24/7 en Policía o Fiscalía para coordinar preservación digital internacional.

Asistencia directa con proveedores

- Permite solicitudes de conservación sin necesidad de tratados previos.
- Empresas como Google, Meta, Telegram aceptan requerimientos basados en Budapest.

Impacto: Mejora la rapidez y la eficiencia en investigaciones complejas.

Extraterritorialidad racional

- Autoriza medidas cuando el delito afecta a nacionales o infraestructura crítica del país, incluso si el atacante está afuera.

11.4. Principios transversales del convenio

Proporcionalidad y estándares de derechos humanos

- Cualquier interferencia en datos o comunicaciones requiere control judicial.

- Protección de privacidad y garantías de debido proceso.

Relevancia: Permite evitar un modelo de Derecho Penal del Enemigo, aun en delitos graves.

Tecnología-neutral

La redacción del Convenio evita referencias a tecnologías específicas, lo cual:

- lo mantiene vigente pese a tecnologías emergentes,
- lo hace fácilmente adaptable a IA, algoritmos, big data, blockchain, etc.

Enfoque dual: prevención y represión

Incluye buenas prácticas, medidas administrativas y cooperación público–privada.

11.5. Aplicación para la reforma del COIP

Basado en Budapest, Ecuador debería incorporar:

a. Nuevos tipos penales

- Acceso ilícito agravado.
- Interferencia de datos con fines terroristas.
- Sabotaje digital a infraestructura crítica.
- Manipulación algorítmica e IA maliciosa.
- Producción y distribución de malware.

b. Reglas procesales especiales

- Allanamiento digital remoto.
- Preservación urgente de metadatos.
- Recolección en tiempo real.
- Agentes encubiertos digitales.
- Órdenes para acceder a cuentas cloud y dispositivos cifrados.

c. Cooperación internacional inmediata

- Unidad 24/7.
- Mecanismos de preservación rápida.
- Protocolos directos con proveedores globales.

CAPÍTULO XII

Los Ciberdelitos y el Marco Jurídico Internacional: Análisis del Convenio de Budapest (2001)

12.1. Introducción al fenómeno de los ciberdelitos

Los ciberdelitos constituyen una de las transformaciones más significativas del derecho penal contemporáneo. A diferencia de los delitos tradicionales, los ilícitos cometidos mediante tecnologías digitales se caracterizan por su transnacionalidad, anonimato, baja huella física, alta volatilidad de evidencia y capacidad disruptiva sin precedentes. El ciberespacio, inicialmente concebido como un entorno descentralizado, libre y global, se ha convertido en un escenario propicio para el surgimiento de conductas criminales altamente sofisticadas que desafían los marcos jurídicos clásicos.

Los ciberdelitos incluyen desde el acceso no autorizado a sistemas informáticos, fraude digital, phishing, ransomware y robo de información, hasta formas altamente complejas como el ciberterrorismo, el espionaje digital, la manipulación algorítmica, ataques a

infraestructura crítica y delitos cometidos mediante inteligencia artificial. Este crecimiento acelerado ha puesto en evidencia que la legislación penal de muchos países entre ellos Ecuador, carece de herramientas suficientes para enfrentar estas amenazas.

La magnitud del problema llevó a la comunidad internacional a buscar un marco normativo común, culminando en el **Convenio sobre Ciberdelincuencia del Consejo de Europa (2001)**, conocido como **Convenio de Budapest**, el instrumento jurídico internacional más importante en esta materia.

12.2. Conceptualización y tipología de los ciberdelitos

Los ciberdelitos suelen clasificarse en dos grandes categorías:

A. Delitos dirigidos contra sistemas o datos informáticos

- Acceso no autorizado (hacking).
- Interceptación ilícita de datos.

- Interferencia ilícita en datos (borrado, alteración, deterioro).
- Interferencia en sistemas (ataques DDoS, sabotaje).
- Uso indebido de dispositivos (malware, herramientas de hacking).

B. Delitos cometidos mediante sistemas informáticos

- Fraudes digitales y phishing.
- Robo de identidad.
- Pornografía infantil y explotación sexual.
- Amenazas, extorsión y ransomware.
- Estafas bancarias y financieras.
- Ciberterrorismo y manipulación algorítmica.
- Uso de Inteligencia Artificial (IA) para la comisión de delitos.

Ambas categorías presentan desafíos comunes: volatilidad de evidencia, anonimato del atacante, dificultad de jurisdicción, necesidad de cooperación internacional y falta de capacidad técnica de los Estados.

12.3. El Convenio de Budapest (2001): origen y alcance

El Convenio de Budapest es el primer tratado internacional vinculante sobre ciberdelincuencia. Adoptado por el Consejo de Europa en 2001, se ha convertido en el estándar global debido a su enfoque integral, tecnología neutral y reglas procesales específicas para la obtención de evidencia digital.

Aunque Ecuador aún no es parte del Convenio, sus estándares pueden y deben adoptarse internamente para fortalecer el sistema penal y modernizar el COIP. Al ser un instrumento ampliamente aceptado, incluso proveedores de servicios globales (Google, Meta, Microsoft, Telegram) cooperan con solicitudes basadas en sus principios.

El Convenio tiene cuatro grandes ejes:

1. Delitos informáticos (tipos penales mínimos).
2. Medidas procesales específicas para evidencia digital.
3. Cooperación internacional inmediata 24/7.

4. Garantías y estándares de derechos humanos.

12.4. Tipos penales sustantivos en el Convenio de Budapest

El Convenio exige que los Estados tipifiquen, como mínimo, los siguientes delitos:

12.4.1. Acceso ilícito (Artículo 2)

Ingreso no autorizado a sistemas informáticos. Fundamental para atacar hacking, intrusiones, ransomware y espionaje.

12.4.2. Interceptación ilícita (Artículo 3)

Captación no autorizada de datos en tránsito o almacenados.

12.4.3. Interferencia en datos (Artículo 4)

Borrado, deterioro, alteración o supresión de datos.

12.4.4. Interferencia en sistemas (Artículo 5)

Ataques que impidan el funcionamiento normal de un sistema.

12.4.5. Uso indebido de dispositivos (Artículo 6)

Creación, distribución o utilización de malware o herramientas de hacking.

12.4.6. Falsificación informática (Artículo 7)

Alteración de datos con efectos jurídicos.

12.4.7. Fraude informático (Artículo 8)

Acciones dirigidas a obtener beneficio económico mediante manipulación informática.

12.4.8. Delitos relacionados con contenidos ilegales (Artículos 9 y 10)

Pornografía infantil, violaciones a derechos de autor y propiedad intelectual.

Estos estándares constituyen el fundamento técnico para una reforma profunda del COIP, especialmente en materia de ciberterrorismo, ya que muchos de sus elementos hoy no están previstos en la legislación.

12.5. Medidas procesales del Convenio de Budapest

Estas medidas son el corazón del tratado y representan una revolución en el derecho procesal penal digital.

12.5.1. Preservación rápida de datos (Artículo 16)

Permite ordenar a un proveedor que preserve datos antes de que se borren automáticamente.

12.5.2. Conservación y revelación de tráfico (Artículos 17 y 18)

Autoriza la retención y entrega de información de abonado y metadatos.

12.5.3. Allanamiento digital (Artículo 19)

Registro de sistemas informáticos, dispositivos, servidores o cuentas cloud.

12.5.4. Recolección en tiempo real (Artículos 20 y 21)

Captura de datos mientras se generan.

12.5.5. Interceptación legal de datos digitales

Faculta la vigilancia digital con autorización judicial.

Estos mecanismos son indispensables para investigar ataques complejos como DDoS, ransomware, espionaje o ciberterrorismo.

12.6. Cooperación internacional inmediata

El Convenio incorpora un sistema de cooperación basado en:

a. **Red de puntos de contacto 24/7**

Para preservar datos urgentes en otros países.

b. Asistencia directa con proveedores tecnológicos

Permite solicitar información sin tratados específicos.

c. Extraterritorialidad razonable

Aplicable cuando los delitos afectan infraestructura crítica nacional.

Para Ecuador, donde entre el 80% y 95% de la evidencia digital reside fuera del país, esta cooperación es esencial.

12.7. Estándares de derechos humanos y garantías procesales

El Convenio preserva:

- Proporcionalidad.
- Control judicial.
- Protección de la privacidad.
- Legalidad estricta.
- Debida diligencia tecnológica.

Esto evita que las facultades especiales deriven en abusos o desnaturalización de derechos fundamentales, especialmente frente al riesgo de instalar un derecho penal del enemigo digital.

12.8. Importancia del Convenio de Budapest para Ecuador

Ecuador enfrenta una vulnerabilidad estructural debido a:

- Ausencia de tipo penal de ciberterrorismo.
- Tipos informáticos insuficientes en el COIP.
- Falta de capacidad técnica de Fiscalía y Policía.
- Carencia de cadena de custodia digital adecuada.
- Debilidad en cooperación internacional.
- Ausencia de estrategia nacional de ciberseguridad.

El Convenio ofrece un marco listo para adoptarse, que no solo fortalece la respuesta penal, sino también la prevención, la coordinación institucional y la seguridad nacional.

12.9. Propuesta de incorporación parcial del Convenio al COIP

Se sugiere que Ecuador adopte:

1. **Tipos penales mínimos**

Acceso ilícito, interferencia en sistemas, uso indebido de dispositivos, fraude informático, sabotaje digital y ciberterrorismo autónomo.

2. **Reglas procesales especiales**

Preservación urgente, órdenes de acceso digital, captura en tiempo real y agentes encubiertos digitales.

3. **Protocolo de cooperación internacional 24/7**

Con puntos de contacto en Fiscalía, Policía y Cancillería.

4. **Actualización de la cadena de custodia digital**

Incluyendo evidencia volátil, logs, metadatos y trazabilidad técnica.

5. Marco para inteligencia digital

Con enfoque garantista y tecnológico.

Los ciberdelitos representan uno de los mayores desafíos para el derecho penal del siglo XXI. El Convenio de Budapest, aunque no vinculante para Ecuador, constituye una guía normativa, procesal y político-criminal sólida, indispensable para reformar el COIP y enfrentar amenazas digitales como el ciberterrorismo. Su adopción total o parcial permitiría al Estado cerrar vacíos normativos, modernizar su sistema penal y proteger efectivamente la seguridad nacional, los derechos fundamentales y la infraestructura crítica del país.

El Convenio de Budapest es hoy el estándar internacional dominante porque combina:

- Tipos penales modernos,
- Procedimientos de obtención de evidencia digital,
- Cooperación internacional rápida,
- Garantías de derechos humanos,

- Adaptabilidad a nuevas tecnologías como ia y blockchain.

Su incorporación como marco de referencia en la reforma del COIP fortalecerá la capacidad del Estado para enfrentar:

- Ciberterrorismo,
- Sabotaje a infraestructura crítica,
- Manipulación algorítmica,
- Ataques a servicios esenciales,
- Delitos transnacionales complejos.

12.10. Recomendaciones para jueces, fiscales, policías y legisladores

a) Para los legisladores

- Aprobar reformas penales específicas en materia digital.
- Establecer definiciones técnicas claras y evitar ambigüedades.
- Incorporar obligaciones de preservación de datos y cooperación internacional.

- Aprobar una Ley Orgánica de Ciberseguridad complementaria al COIP.
- Asignar presupuesto estable a unidades técnicas.

b) Para los fiscales

- Especializarse en análisis de evidencia digital y cadena de custodia.
- Solicitar medidas intrusivas solo con proporcionalidad y motivación suficiente.
- Utilizar peritajes interdisciplinarios (informáticos, electrónicos, algorítmicos).
- Priorizar la cooperación internacional y preservación temprana de datos.

c) Para la Policía Nacional

- Fortalecer la Dirección Nacional de Delitos Informáticos.
- Mejorar capacidades operativas: análisis de malware, OSINT, SIGINT, ciberinteligencia.
- Realizar entrenamientos constantes y actualizados.

- Implementar protocolos unificados de primeros auxilios digitales.

d) Para los jueces

- Comprender la naturaleza técnica del ciberterrorismo.
- Aplicar criterios garantistas en la autorización de medidas especiales.
- Exigir precisión en la cadena de custodia digital.
- Evitar criminalizar conductas sin lesividad real o sin pruebas técnicas contundentes.

e) Para el Estado en general

- Garantizar la protección de datos personales.
- Asegurar transparencia tecnológica.
- Dotar de recursos suficientes a todas las instituciones involucradas.
- Implementar auditorías externas de seguridad digital.

CAPÍTULO XIII

Inteligencia Artificial y Ciberdelincuencia Avanzada

13.1. Introducción: la inteligencia artificial como nuevo escenario delictivo

La Inteligencia Artificial (IA) se ha consolidado como una de las tecnologías más transformadoras del siglo XXI. Su capacidad para aprender, predecir patrones, automatizar procesos y generar contenidos la convierte en una herramienta con enorme potencial positivo, pero también abre la puerta a riesgos inéditos. La IA ya no solo es un instrumento neutral: se ha convertido en actor autonomizado dentro del ecosistema delictivo digital.

El surgimiento de técnicas avanzadas como el machine learning, el deep learning y los modelos generativos, así como su integración con big data, blockchain, robótica, sistemas autónomos y ciberarmas, ha creado lo que la doctrina denomina ciberdelincuencia aumentada por IA (AI-Augmented Crime).

Este nuevo escenario plantea desafíos profundos para el Derecho Penal ecuatoriano, especialmente considerando que el COIP no regula las conductas realizadas mediante IA ni los delitos que se potencian gracias a ella, y mucho menos aquellos que pueden derivar en acciones de alto impacto como el ciberterrorismo algorítmico.

13.2. La IA como herramienta criminal

La participación de la IA en conductas delictivas puede clasificarse en tres niveles:

13.2.1. IA como herramienta instrumental (asistencia al delincuente)

La IA se utiliza como un instrumento para facilitar actividades criminales:

- Generación automatizada de malware avanzado.
- Algoritmos para descifrar contraseñas o romper cifrados.
- Optimización de ataques DDoS.
- Bots autónomos para phishing o ingeniería social.

- Deepfakes para fraudes bancarios o extorsiones.

La IA actúa amplificando capacidades humanas, reduciendo costos y aumentando eficiencia.

13.2.2. IA como agente semi-autónomo

El sistema opera con grado de autonomía:

- Bots que seleccionan víctimas según patrones.
- Malware que se adapta al entorno para evitar detección.
- Sistemas que aprenden del comportamiento de antivirus.

Aquí surge la pregunta: **¿Quién responde penalmente cuando el sistema toma decisiones no programadas explícitamente?**

13.2.3. IA como creadora de riesgo sistémico

La IA no solo comete delitos, sino que crea vulnerabilidades estructurales:

- Modelos generativos que replican identidades.
- Sistemas de decisión que manipulan mercados, elecciones o infraestructuras.
- Algoritmos que pueden emplearse para ciberterrorismo sin intervención humana directa.

Esto coloca al Derecho Penal en una crisis conceptual frente a la responsabilidad por algoritmos.

13.3. Deepfakes, identidad digital y nueva formas de fraude

Los deepfakes permiten crear videos o audios hiperrealistas, capaces de imitar rostros, voces y gestos. Sus riesgos penales incluyen:

- Suplantación de identidad.
- Fraude financiero.
- Extorsión sexual.
- Manipulación política.
- Propaganda terrorista.

La ausencia de regulación específica dificulta sancionar la creación y difusión maliciosa de estos contenidos.

13.4. IA en ransomware y ataques avanzados

El ransomware ha evolucionado hacia modelos con IA embarcada:

- Análisis automático de redes para identificar activos críticos.
- Velocidad de cifrado optimizada.
- Selección de víctimas según capacidad de pago.
- Negociación automatizada con las víctimas ("auto-ransom bots").

La IA reduce drásticamente el margen de respuesta institucional.

13.5. IA como arma de ciberterrorismo

Esta es la dimensión de mayor riesgo.

13.5.1. Algoritmos utilizados para planificar ataques

La IA puede identificar vulnerabilidades en:

- Centrales eléctricas.
- Sistemas bancarios.
- Redes de agua potable.
- Infraestructura militar.

13.5.2. Automatización del ataque

La IA puede ejecutar ataques sincronizados con:

- Drones.
- Robots autónomos.
- Sistemas de sabotaje industrial.

13.5.3. Propaganda algorítmica

El terrorismo moderno utiliza IA para:

- Viralizar mensajes radicales.
- Crear discursos personalizados.
- Manipular emociones en redes sociales.

- Simular líderes o voceros ficticios.

La capacidad de la IA para influir en masas la convierte en un arma no convencional.

13.6. Responsabilidad penal en delitos con IA

El uso de IA plantea preguntas fundamentales:

¿Quién es el autor?

- ¿El programador?
- ¿El usuario que emplea la IA?
- ¿El propietario del sistema?
- ¿El entrenador del modelo?

El COIPno regula estos escenarios.

Responsabilidad por riesgo tecnológico

La doctrina propone categorías como:

- Autoría mediata mediante IA.
- Creación de riesgo jurídicamente desaprobado.
- Responsabilidad por defectos de diseño.

- Culpabilidad por falta de diligencia técnica.

¿Puede la IA ser sujeto de imputación?

No, en el sistema penal ecuatoriano, ni en ninguno, pero afecta la forma de imputar a los humanos detrás del algoritmo.

13.7. Necesidad de tipos penales especiales en el COIP

La IA exige incorporar nuevos tipos penales o agravar los existentes. Se proponen los siguientes:

13.7.1. Manipulación algorítmica con fines delictivos

Delito autónomo para castigar la alteración de sistemas de decisión automatizada que afecten bienes jurídicos esenciales.

13.7.2. Uso de IA para ataques informáticos agravados

Agravar:

- Sabotaje digital.
- Interferencia en sistemas.

- Ataques a infraestructura crítica.
- Cuando se utilice IA para automatizar o maximizar daños.

13.7.3. IA con fines terroristas

Una de las figuras más urgentes:

- Uso de IA para seleccionar objetivos.
- Creación de deepfakes terroristas.
- Manipulación algorítmica de opinión pública con fines violentos.
- Despliegue de bots terroristas autónomos.

13.7.4. Deepfake ofensivo agravado

Cuando afecte:

- Instituciones del Estado.
- Procesos electorales.
- Administración de justicia.
- Seguridad nacional.

13.8. Medidas procesales para investigar delitos cometidos con IA

13.8.1. Peritaje especializado en IA

Es indispensable crear:

- Laboratorios de análisis algorítmico.
- Equipos interdisciplinarios (juristas, ingenieros, analistas de datos, criptógrafos).

13.8.2. Auditoría algorítmica forense

Permite reconstruir decisiones tomadas por el sistema.

13.8.3. Preservación de modelos y bases de datos

Incluye:

- Logs de entrenamiento.
- Conjuntos de datos utilizados.
- Parámetros del modelo.

13.8.4. Orden de acceso a sistemas autónomos

Similares al allanamiento digital del Convenio de Budapest, pero enfocados en IA.

13.8.5. Agentes encubiertos digitales con IA

Para infiltrarse en redes criminales automatizadas.

13.9. Perspectiva de derechos fundamentales

Los delitos cometidos mediante IA pueden vulnerar masivamente:

- Privacidad.
- Identidad.
- Veracidad de la información.
- Seguridad digital.
- Derechos políticos.
- Debido proceso.

La regulación debe equilibrar seguridad y libertad, evitando un derecho penal del enemigo algorítmico.

13.10. Recomendaciones para Ecuador

1. Tipificar la manipulación algorítmica y el uso de IA con fines delictivos.
2. Crear laboratorio nacional de IA forense en Fiscalía.
3. Reformar el COIP para incorporar delitos agravados por uso de IA.
4. Regular deepfakes, identidad digital y fraude algorítmico.
5. Adoptar estándares del Convenio de Budapest para evidencia digital.
6. Impulsar cooperación internacional inmediata 24/7.
7. Capacitar a operadores de justicia en análisis de IA.
8. Implementar auditoría algorítmica obligatoria en infraestructuras críticas.

La Inteligencia Artificial no solo transforma la economía y la sociedad: transforma el delito. La ciberdelincuencia avanzada basada en IA representa un desafío sin

precedentes para el sistema penal, que carece de normas, capacidades técnicas y estrategias adecuadas. Frente a ello, es imprescindible una reforma integral del COIP, inspirada en marcos internacionales como el Convenio de Budapest, pero orientada a enfrentar riesgos emergentes propios del siglo XXI.

La IA amplifica, automatiza y perfecciona el delito. Por ello, la respuesta jurídica debe ser igualmente sofisticada, tecnológicamente informada y garantista.

CAPÍTULO XIV

Derecho Penal del Enemigo Digital y la Desnaturalización de los Derechos Fundamentales

14.1. Introducción: la expansión del punitivismo digital

La acelerada digitalización del mundo contemporáneo ha generado nuevas formas de criminalidad, altamente tecnificadas y transnacionales, que desafían la estructura tradicional del derecho penal. Frente a amenazas como el ciberterrorismo, la manipulación algorítmica, los ataques a infraestructuras críticas o el uso de inteligencia artificial para cometer delitos complejos, los Estados han reaccionado con una tendencia global: ampliar el poder punitivo, flexibilizar garantías y adoptar modelos de intervención que se aproximan al denominado *Derecho Penal del Enemigo*.

Esta transformación plantea un desafío ontológico: ¿puede el derecho penal modernizado ahora digitalizado seguir siendo un sistema garantista sin sacrificar la seguridad nacional? O, por el contrario, ¿se está

configurando un nuevo paradigma de persecución penal basado en la identificación de "enemigos digitales", susceptibles de ser tratados con reglas excepcionales?

Este capítulo busca analizar críticamente esta tensión, especialmente donde la falta de tipicidad penal, la debilidad institucional y la presión social por respuestas inmediatas favorecen la expansión de modelos punitivos incompatibles con la Constitución de la República del Ecuador de 2008.

14.2. El concepto de "enemigo" en el espacio digital

Jakobs (1985) formuló la teoría del *Derecho Penal del Enemigo* para describir un sistema penal dirigido no a ciudadanos sino a sujetos que, mediante su peligrosidad y acciones, renuncian al pacto social. El Estado, frente a ellos, aplica un derecho penal excepcional que flexibiliza garantías y prioriza la seguridad por sobre la libertad.

En el ámbito digital, esta noción se ha visto reforzada por el devenir de la modernidad del ciber:

- Los cibercriminales pueden actuar desde cualquier jurisdicción.
- Los daños pueden ser masivos, inmediatos y globales.
- La atribución penal es extremadamente compleja.
- La afectación a servicios esenciales puede paralizar un país entero.

De esta forma, se configura una categoría emergente: **el enemigo digital**, caracterizado por su invisibilidad, capacidad técnica, anonimato y potencial devastador. No obstante, la importación acrítica de esta categoría supone riesgos severos para el Estado constitucional.

Concepto "enemigo digital"

Desde mi perspectiva, propongo entender al **enemigo digital** como:

Aquel sujeto individual o colectivo que, mediante el uso intensivo, oculto y tecnológicamente avanzado de herramientas digitales, ejecuta acciones destinadas a vulnerar la estabilidad institucional, afectar

infraestructuras críticas o generar un estado de inseguridad prolongada en la sociedad, aprovechándose de la asimetría técnica frente al Estado y operando desde un espacio transnacional, anónimo y difícilmente atribuible. No se define por su identidad, sino por la naturaleza estratégica, continuada y de alto impacto de sus ataques, los cuales buscan fracturar el orden constitucional utilizando el ciberespacio como campo de confrontación.

Este concepto incorpora varios elementos:

1. **No es una categoría ontológica de persona, sino de conducta**

A diferencia del enfoque clásico de Jakobs, el enemigo digital no es alguien que pierde su calidad de ciudadano, sino un sujeto que desarrolla acciones digitalmente estructuradas y de riesgo extremo.

2. **Opera desde la asimetría tecnológica**

El enemigo digital explota:

- Anonimato,
- Criptografía,
- Redes ocultas,
- Bots,
- IA,
- Infraestructura distribuida,
- Jurisdicciones con baja cooperación.

Su ventaja frente al Estado es técnica, no ideológica.

3. **Persigue fines de desestabilización sistemática**

Su objetivo no es cometer un delito aislado, sino:

- Paralizar servicios esenciales,
- Afectar la seguridad nacional,
- Comprometer procesos democráticos,
- Manipular información estratégica.

4. **Su peligrosidad deriva de la intangibilidad**

El enemigo digital no necesita presencia física, armas ni territorio; su poder surge de la penetración en sistemas, lo

cual le otorga un alcance global y un perfil difícil de combatir.

5. No debe justificar un derecho penal de excepción

Aunque el término describe una amenaza severa, no puede ser fundamento para suprimir garantías. El Estado debe responder con un derecho penal técnico, no con un derecho penal del enemigo en sentido político.

14.3. Tecnologías como catalizadoras de un derecho penal excepcional

Las nuevas tecnologías, lejos de requerir únicamente adaptación normativa, han impulsado transformaciones profundas se debe reconceptualizar algunos tipos penales por cuanto los conceptos antiguos quedan insuficientes frente al desarrollo tecnológico:

14.3.1. Vigilancia masiva y metadatos

Para combatir ciberamenazas, los Estados han ampliado herramientas como:

- Retención obligatoria de datos.
- Acceso ampliado a metadatos.
- Algoritmos predictivos.
- Monitoreo de redes sociales.

Estas medidas, aunque útiles, generan una zona gris donde la seguridad digital se impone sobre la privacidad, contradiciendo estándares como la Opinión Consultiva OC-24/17 de la Corte IDH.

14.3.2. Persecución extraterritorial

El enemigo digital no reconoce fronteras. Ante ello, se han propuesto mecanismos de jurisdicción universal limitada, cooperación inmediata o intervención estatal más allá del territorio, lo cual tensiona la soberanía y el principio de legalidad.

14.3.3. Algoritmos de vigilancia predictiva

Su uso puede derivar en una lógica de *Derecho Penal de Autor*: las personas son tratadas en función de su

probabilidad estadística de delinquir, no por hechos concretos.

14.4. La tendencia al debilitamiento de derechos fundamentales

Cuando el Estado adopta una visión del enemigo digital, se produce un proceso de desnaturalización de derechos constitucionales:

14.4.1. Presunción de inocencia

La vigilancia preventiva, el perfilamiento y la retención de datos sin sospecha concreta reducen la presunción de inocencia a una formalidad.

14.4.2. Legalidad y tipicidad

La presión social por respuestas inmediatas genera tipos penales abiertos o vagos, como:

- "Ataques informáticos que comprometan la seguridad nacional".
- "Conductas de riesgo elevado en el ciberespacio".

Estos tipos, si no se redactan con precisión, amplían peligrosamente el poder punitivo.

14.4.3. Intimidad y protección de datos

La lucha contra amenazas digitales ha llevado a justificar intrusiones desproporcionadas, como:

- Acceso a dispositivos sin orden judicial,
- Interceptaciones basadas en sospechas mínimas,
- Confiscación digital sin criterios claros.

14.4.4. Debido proceso

El uso de evidencia digital opaca algoritmos, análisis automatizados, perfiles, que dificulta auditabilidad, contradicción y defensa efectiva.

14.4.5. Libertad de expresión

La moderación automatizada o estatal puede etiquetar actividades legítimas como riesgosas, afectando el debate democrático.

14.5. ¿Ciberterroristas como enemigos? Crítica desde el garantismo

Si bien los ciberterroristas representan una amenaza real y de alto impacto, clasificarlos como "enemigos" en el sentido de Jakobs es problemático:

1. **Su peligrosidad no elimina su calidad de persona.**
   El derecho penal constitucional debe juzgar hechos, no identidades.
2. **El enemigo digital no es una categoría objetiva.**
   Puede derivar en criminalizar disidencia, hacktivismo o conductas ambiguas.
3. **La excepcionalidad se normaliza.**
   Lo que inicia como excepción para casos extremos termina aplicándose a delitos comunes.
4. **El garantismo no es un obstáculo, sino un filtro.**
   El Estado puede protegerse sin sacrificar derechos.

En síntesis, la respuesta adecuada no es un derecho penal del enemigo, sino un derecho penal moderno, técnico y

garantista, capaz de investigar cibercrímenes sin vulnerar el sistema constitucional.

14.6. Propuestas de equilibrio: seguridad digital con garantías

Este capítulo propone un modelo de seguridad jurídica respetuoso de la Constitución:

14.6.1. Tipos penales tecnológicos claros y específicos

La reforma del COIP debe evitar tipos amplios y optar por descripciones técnicas y verificables.

14.6.2. Controles estrictos a las facultades excepcionales

Cualquier acceso digital, retención de datos o interceptación debe:

- Tener sustento judicial,
- Ser proporcional,
- Limitarse en tiempo,
- Ser auditado técnicamente.

14.6.3. Transparencia algorítmica

Los sistemas automatizados utilizados por Policía, Fiscalía o Inteligencia deben ser auditables y verificables para garantizar defensa efectiva.

14.6.4. Capacitación especializada

El garantismo digital exige operadores de justicia capaces de:

- Interpretar pruebas digitales,
- Entender metadatos,
- Auditar tecnologías,
- Evitar abusos estatales.

El concepto personal de *enemigo digital* se ubica en un punto doctrinario equilibrado:

- **Reconoce la gravedad de las amenazas digitales** (afinidad con Silva Sánchez y Jakobs).
- **Rechaza la deshumanización y la suspensión de garantías** (coherente con Ferrajoli y Zaffaroni).

- **Propone un derecho penal técnico, preciso y constitucional** (en línea con Mir Puig).

En definitiva, esta definición integra lo mejor de cada corriente, sin caer en los extremos punitivistas ni en el garantismo paralizante, lo cual lo convierte en un concepto doctrinario aplicable y útil para la discusión penal contemporánea.

14.6.5. Instituciones fuertes y controladas

Un Estado con debilidad institucional corre el riesgo de convertir el discurso del enemigo digital en justificación de abusos.

El desarrollo del derecho penal frente a las amenazas digitales no debe replicar modelos de enemigo ni justificar la erosión de derechos fundamentales. La lucha contra el ciberterrorismo y el crimen informático requiere un derecho penal técnico, preciso y garantista, alineado con estándares democráticos y con la Constitución de la República.

Aceptar sin crítica un derecho penal del enemigo digital significaría asumir que ciertos individuos dejan de ser titulares de derechos, lo cual sería incompatible con un Estado constitucional de derechos y justicia.

La seguridad del Estado no debe alcanzarse sacrificando la esencia del derecho penal: la protección de la dignidad humana.

El Ecuador se encuentra en un punto de inflexión. La amenaza del ciberterrorismo no es una especulación, sino una realidad que avanza más rápido que el marco jurídico y que la capacidad institucional del Estado. Sin una reforma penal profunda, una política criminal moderna y una estrategia nacional de ciberseguridad, el país corre el riesgo de enfrentar ataques que puedan paralizar servicios esenciales, comprometer la democracia y generar daños irreparables.

Sin embargo, responder a esta amenaza no implica renunciar a los principios constitucionales. La clave está en construir un modelo de seguridad digital democrática,

donde la protección del Estado y la tutela de los derechos convivan en equilibrio.

Un Ecuador preparado para el siglo XXI es aquel que entiende que la seguridad digital es parte esencial del desarrollo, de la estabilidad política y de la vigencia plena del Estado de derecho.

CAPÍTULO XV
Metaverso, Ciberespacio Expandido y Nuevos Desafíos para el Derecho Penal

15.1. Introducción: del ciberespacio al metaverso

El metaverso constituye la evolución más avanzada del ciberespacio, entendido como una realidad digital inmersiva, persistente, tridimensional y compartida, en la cual los usuarios interactúan mediante avatares, dispositivos de realidad virtual o aumentada, inteligencia artificial y sistemas algorítmicos autónomos. No es simplemente un entorno virtual recreativo, sino un ecosistema social, económico, laboral y cultural.

Desde la óptica penal, el metaverso no es un espacio ajeno al derecho: se convierte en un nuevo escenario criminológico, donde las conductas pueden adquirir un impacto real, incluso si se ejecutan en un entorno digital. La interacción entre anonimato, descentralización, criptomonedas, IA y simulación 3D genera formas inéditas de riesgo penal.

Cuya regulación en materia de ciberdelitos es limitada en nuestro país, el metaverso abre un desafío urgente: actualizar el COIP para prever conductas que, aunque ocurran en entornos virtuales, producen efectos en la vida física o en la seguridad estatal.

15.2. Naturaleza jurídica del metaverso como "espacio penalmente relevante"

La doctrina internacional comienza a reconocer que el metaverso constituye:

- Un espacio de interacción humana,
- Un ente con valor jurídico,
- Una fuente de obligaciones y responsabilidades,
- Un ámbito donde pueden cometerse delitos reales.

Interrogantes que nacen desde la perspectiva penal tendríamos tres dimensiones en el metaverso.

¿Dónde ocurre la conducta punible? (territorialidad)

El metaverso diluye las fronteras físicas. Un usuario en Ecuador puede cometer un delito contra una persona en

Europa dentro de un servidor ubicado en Estados Unidos. Ello plantea retos en:

- Competencia penal,
- Cooperación internacional,
- Ejecución de evidencia digital.

¿Qué bienes jurídicos se afectan? En el metaverso pueden lesionarse:

- Libertad sexual (acoso virtual, agresiones simuladas, captación de menores),
- Patrimonio (fraude nft, robo de criptomonedas),
- Identidad (suplantación de avatar),
- Seguridad nacional (espionaje en espacios corporativos simulados),
- Integridad psicológica (acoso persistente y sensorial).

¿Quién es el sujeto activo? Pueden intervenir:

- Personas,
- Avatares controlados por ia,

- Bots autónomos,
- Colectivos criminales coordinados en tiempo real.

15.3. Ciberdelitos y nuevas tipologías criminales en entornos inmersivos.

En el metaverso emergen formas expandidas de ciberdelincuencia:

1. **Agresiones sexuales virtuales inmersivas**

Cuando mediante realidad virtual un usuario toca, hostiga o abusa de otro avatar con haptics (trajes sensoriales), se genera una afectación psicológica real. Algunos países ya lo clasifican como *sexual harassment in immersive environments*.

2. **Fraudes y estafas con activos inmersivos. Incluyen:**

- Venta de terrenos virtuales falsos,
- Manipulación de nfts,
- Estafas mediante tokens,
- Casinos vr ilegales,

- Préstamos en plataformas defi dentro del metaverso.

3. Manipulación algorítmica de avatares

Deepfakes 3D, clonación de voz, identidad sintética y suplantación completa del avatar para fines ilícitos.

4. Espionaje digital inmersivo

Infiltración en:

- Reuniones corporativas en VR,
- Simuladores militares,
- Laboratorios académicos virtuales,
- Espacios gubernamentales simulados.

Esto constituye un riesgo directo para la seguridad nacional.

5. **Coordinación de ciberdelitos desde el metaverso**

Grupos criminales pueden reunirse en entornos privados en VR, encriptados, invisibles para la vigilancia policial tradicional.

6. **Delitos contra menores en entornos inmersivos. Incluye:**

- Grooming,
- Captación,
- Manipulación emocional con avatares infantiles generados por ia,
- Exposición a contenidos violentos o sexuales.

15.4. Metaverso y ciberterrorismo

El metaverso puede ser utilizado como plataforma para:

- Entrenar ataques a infraestructuras críticas,
- Simular atentados físicos y ciberataques,
- Reclutar y adoctrinar,
- Difundir propaganda radicalizada,

- Utilizar entornos VR como refugio oculto.

Existen reportes internacionales sobre el uso del metaverso por grupos extremistas para simular ataques reales antes de ejecutarlos físicamente.

Para nosotros, que carecemos de un tipo penal específico de ciberterrorismo, este espacio multiplica la vulnerabilidad estatal.

15.5. Brecha normativa en Ecuador frente al metaverso.

El COIP no contempla:

- Delitos inmersivos,
- Agresiones en entornos digitales corporeizados,
- Suplantación algorítmica de identidad,
- Manipulación de avatares autónomos,
- Simulaciones dañinas,
- Propiedad virtual,
- Reconocimiento jurídico de bienes intangibles inmersivos.

Esto genera:

- Impunidad,
- Reclasificación inadecuada,
- Inseguridad jurídica,
- Imposibilidad de protección de usuarios.

15.6. Criterios de política criminal para regular el metaverso.

Se propone que el Estado adopte un modelo que integre:

- Reconocimiento del metaverso como espacio penalmente relevante.

Se requiere incorporar en el COIP una cláusula que establezca que las conductas realizadas en entornos inmersivos que produzcan efectos jurídicamente relevantes serán penalizables.

- Regulación de agresiones y delitos contra la integridad psicológica en VR.
- Tipificación de la suplantación algorítmica de identidad.

- Creación de un régimen jurídico de bienes virtuales.
- Incorporación de delitos de manipulación de avatares y deepfakes 3D.
- Controles algorítmicos y auditorías obligatorias para empresas del metaverso.
- Actualización probatoria sobre evidencia inmersiva:
  - Capturas VR,
  - Logs tridimensionales,
  - Registros sensoriales,
  - Metadatos de interacción.

15.7. Riesgos de desnaturalización de derechos fundamentales en el metaverso

Los riesgos principales son:

- Vigilancia masiva dentro de ambientes VR,
- Rastreo biométrico involuntario (movimientos oculares, patrones motores),

- Perfilización algorítmica extrema,
- Privatización de espacios públicos digitales,
- Pérdida de anonimato.

El Estado debe evitar que el combate a la ciberdelincuencia en VR resulte en:

- Abuso policial digital,
- Monitoreo permanente,
- Restricciones desproporcionadas,
- "estado de excepción digital".

El metaverso amplía el campo criminológico y exige una reconceptualización completa del Derecho Penal. Representa un desafío urgente que implica:

- Actualizar el COIP,
- Fortalecer investigación forense digital,
- Cooperar internacionalmente,
- Regulares empresas tecnológicas,
- Garantizar derechos fundamentales.

Se trata de un territorio nuevo donde confluyen riesgo, anonimato, IA y economía digital, demandando un sistema penal más sofisticado, técnico y moderno.

ANEXOS

- Glosario de ciberdelitos.
- Flujograma de investigación digital penal.

GLOSARIO DE CIBERDELITOS

Acceso ilícito

Ingreso no autorizado a un sistema informático, red, servidor o base de datos, vulnerando mecanismos de seguridad o superando barreras lógicas de acceso. Constituye la puerta de entrada típica para otros ataques más complejos.

Actos preparatorios digitales

Conductas previas a la ejecución de un ciberdelito, tales como escaneo de puertos, recolección de credenciales, análisis de vulnerabilidades o instalación de backdoors. En delitos de terrorismo o ataques a infraestructura crítica, suelen estar penalizados de forma autónoma.

Actualización maliciosa (malicious update)

Modificación fraudulenta de software legítimo para introducir código dañino que permita control remoto, extracción de datos o sabotaje.

Algoritmo adversarial

Técnica destinada a manipular o engañar sistemas de inteligencia artificial especialmente modelos de reconocimiento facial o clasificación automática para alterar decisiones automatizadas, evadir controles o generar resultados falsos.

Análisis de vulnerabilidades

Evaluación técnica de puntos débiles en un sistema informático. Aunque es una práctica legítima en ciberseguridad, se convierte en ilícita cuando se realiza sin consentimiento o con fines delictivos.

Ataque de denegación de servicio (DoS / DDoS)

Acción destinada a saturar un servidor o red mediante múltiples solicitudes, impidiendo su funcionamiento

normal. En su versión distribuida (DDoS), usa botnets o múltiples dispositivos infectados.

Ataques a infraestructura crítica

Cualquier interferencia digital que afecte sistemas esenciales para la seguridad nacional, tales como energía, agua potable, hospitales, telecomunicaciones, transporte o servicios financieros.

Botnet

Red de dispositivos infectados y controlados remotamente por un actor malicioso para ejecutar ataques masivos, robo de información o minería no autorizada.

Cibercrimen organizado

Estructuras criminales que operan de forma estable en el entorno digital, especializadas en fraudes, ransomware, extorsión, lavado de activos digital y tráfico ilícito en la dark web.

Ciberespionaje

Acciones encubiertas encaminadas a obtener información secreta, reservada o estratégica mediante técnicas informáticas, con fines políticos, militares o económicos.

Ciberextorsión

Amenaza de realizar un ataque informático, divulgar información comprometida o paralizar un sistema, con el fin de obtener dinero, bienes, criptomonedas u otras ventajas.

Ciberterrorismo

Uso de tecnologías digitales, sistemas informáticos o inteligencia artificial para generar terror, desestabilizar al Estado, atacar infraestructura crítica o coaccionar a autoridades y población civil.

Código malicioso (malware)

Software diseñado para causar daño, infiltrarse, controlar, espiar o alterar sistemas informáticos. Incluye virus, gusanos, troyanos, spyware, ransomware y rootkits.

Colapso algorítmico

Manipulación intencional de modelos o sistemas automatizados con el objetivo de provocar fallas masivas en procesos críticos (ej. sistemas bancarios, transporte, electricidad).

Criptojacking

Uso no autorizado de recursos informáticos de terceros para minar criptomonedas, generalmente mediante malware oculto.

Dark web

Segmento de internet no indexado por buscadores, accesible mediante redes como Tor, donde proliferan mercados ilícitos, servicios criminales y foros de ciberataques.

Deepfake

Contenido audiovisual generado mediante inteligencia artificial para suplantar identidades, manipular hechos o inducir engaño. Su utilización maliciosa abarca estafas, sextorsión, propaganda y daño reputacional.

Desfiguración de sitios web (defacement)

Modificación no autorizada de la apariencia, contenido o estructura de un sitio web, generalmente con fines de protesta, vandalismo digital o propaganda.

Exfiltración de datos

Extracción ilegal de información sensible desde un sistema mediante técnicas de intrusión silenciosas, túneles cifrados o canales encubiertos.

Fraude informático

Obtención ilícita de un beneficio económico mediante manipulación digital, suplantación de identidad, phishing, clonación de tarjetas o alteración de sistemas bancarios.

Hacking ético

Actividad técnica para evaluar la seguridad de sistemas con autorización del propietario. Se diferencia del hacking ilícito por el consentimiento y finalidad de protección.

Ingeniería social

Manipulación psicológica de personas para obtener acceso, información o credenciales. Incluye phishing, vishing, smishing y pretexting.

Interferencia de datos

Alteración, borrado, corrupción o modificación de datos electrónicos sin autorización. Afecta integridad y disponibilidad de la información.

Interferencia del sistema

Perturbación o parálisis de la funcionalidad de un sistema informático mediante ataques directos, malware o sobrecarga del tráfico.

Manipulación algorítmica

Intervención maliciosa en algoritmos de decisión automática para modificar resultados, sesgar procesos o vulnerar la seguridad nacional.

Ransomware

Malware que cifra la información de un sistema y exige un rescate generalmente en criptomonedas para restablecer el acceso.

Retención de metadatos

Obligación legal de conservar información técnica mínima (IP, puertos, horarios, tráfico) para permitir investigaciones penales eficientes.

Sabotaje digital agravado

Conducta que afecta deliberadamente la operación de sistemas estratégicos o servicios esenciales, provocando daño económico, social o funcional a gran escala.

Skimming digital

Captura de datos de tarjetas o credenciales de pago mediante dispositivos o scripts insertados en sistemas de comercio electrónico.

SQL Injection

Ataque que consiste en insertar comandos SQL maliciosos en formularios o entradas web para acceder, modificar o destruir bases de datos.

Suplantación de identidad digital

Uso fraudulento de credenciales o información personal para hacerse pasar por otra persona en entornos digitales, con fines delictivos.

Troyano

Tipo de malware que se presenta como software legítimo, pero permite acceso remoto o control del sistema.

Vulnerabilidad cero-día (zero-day)

Falla de seguridad desconocida por el desarrollador del software. Su explotación suele ser altamente peligrosa y utilizada por grupos criminales o estatales.

FLUJOGRAMA DE INVESTIGACIÓN DIGITAL PENAL

(Etapas, acciones y responsables)

1) Recepción y calificación de la noticia del delito

→ **Responsable:** Fiscalía / Policía especializada

- Recepción de denuncia, reporte institucional o alerta automatizada.
- Verificación preliminar de tipicidad (ciberdelitos del COIP o delitos comunes con componente digital).
- Análisis de urgencia para determinar riesgos actuales (pérdida de evidencia, ataques activos, propagación).

Si existe urgencia → activar procedimiento inmediato de preservación.

2) Orden de inicio de investigación previa

→ **Responsable:** Fiscalía

- Apertura formal de investigación previa.
- Determinación del tipo de delito informático: acceso ilícito, sabotaje, fraude, ciberterrorismo, etc.
- Definición preliminar de hipótesis investigativa digital.

3) Preservación urgente de evidencia digital

→ **Responsable:** Policía especializada, Fiscalía

- Emisión de órdenes de preservación de datos a proveedores de servicios (ISP, plataformas digitales, bancos).
- Congelamiento de datos de tráfico, registros de acceso, contenidos críticos y metadatos.
- Aseguramiento del sistema afectado, evitando apagados no controlados.
- Elaboración de *hashes* de evidencia (MD5/SHA256).

→ **Punto crítico:** evitar la alteración o pérdida de la evidencia volátil.

4) **Aseguramiento y cadena de custodia**

→ **Responsable:** Policía especializada

- Levantamiento físico o lógico de dispositivos: computadores, teléfonos, servidores, discos duros, routers.
- Registro detallado: fecha, hora, ubicación, estado del equipo, firma de responsables.
- Embalaje y transporte siguiendo estándares de cadena de custodia digital.

5) **Imagen forense y duplicación de dispositivos**

→ **Responsable:** Laboratorio forense digital

- Creación de copia bit a bit (*bitstream image*).
- Verificación de integridad mediante *hash* inicial y final.
- Análisis solo sobre la copia, nunca sobre el original.

6) **Análisis forense técnico especializado**

→**Responsable:** Peritos informáticos Incluye:

- Recuperación de archivos borrados.
- Análisis de logs, metadatos, historial de navegación, correos, chats, redes sociales.
- Identificación de malware, troyanos, ransomware, scripts o conexiones remotas.
- Trazabilidad de direcciones IP (correlación con proveedores).
- Análisis de blockchain o transacciones en criptomonedas cuando exista.

→ **Producto:** Informe técnico preliminar.

7) **Investigación en fuentes abiertas (OSINT)**

→ **Responsable:** Unidades de análisis digital

- Búsqueda en redes sociales, foros, dark web, motores especializados.
- Correlación de alias, perfiles, patrones y relaciones digitales.

- Identificación de indicios sobre motivación, grupos asociados o modus operandi.

8) Solicitudes judiciales

→ **Responsable:** Fiscalía / Juez de Garantías

- Autorizaciones para:
    - Intervención de comunicaciones digitales.
    - Retención y acceso a metadatos.
    - Geolocalización en tiempo real.
    - Ingreso remoto a cuentas (con orden judicial).
- Control estricto de proporcionalidad y finalidad.

9) Perfilamiento de sospechosos y atribución

→ **Responsable:** Fiscalía + Policía

- Correlación entre evidencia técnica, actividad digital y sujeto investigado.
- Determinación de autoría: individual, en grupo, organizada, o vinculada a infraestructura extranjera.

- Identificación de patrones de conducta digital (tiempos, dispositivos, direcciones IP, idioma, zona horaria).

10) Entrevistas y declaraciones

→ **Responsable:** Fiscalía

- Toma de versiones de víctimas, testigos, administradores de sistemas.
- Declaración de expertos técnicos.
- Integración de evidencia testimonial con la técnica-digital.

11) Informe pericial forense final

→**Responsable:** Perito acreditado
Debe contener:

- Metodología utilizada.
- Herramientas certificadas (EnCase, FTK, Autopsy, Cellebrite, Magnet AXIOM, etc.).
- Resultados verificables y reproducibles.
- Gráficos, cronología de eventos y *hashes*.

- Conclusiones claras y fundamentadas.

12) Valoración jurídico-técnica

→ **Responsable:** Fiscalía

- Integración de evidencia digital + pericial + testimonial.
- Determinación de existencia de delito y responsabilidad penal.
- Principios: autenticidad, integridad, confiabilidad, pertinencia y licitud.

13) Formulación de cargos

→ **Responsable:** Fiscalía / Juez

- Presentación formal de cargos.
- Solicitud de medidas cautelares digitales (restricción de cuentas, bloqueo de activos, suspensión de acceso remoto).
- Presentación de elementos de convicción digitales.

14) Etapa procesal y juicio

→ **Responsable:** Tribunal

- Presentación y exhibición de evidencia digital.
- Explicación técnica por peritos.
- Contradicción, refutación y contra-pericia.
- Análisis de admisibilidad de evidencia digital.

15) Sentencia

→ **Responsable:** Tribunal

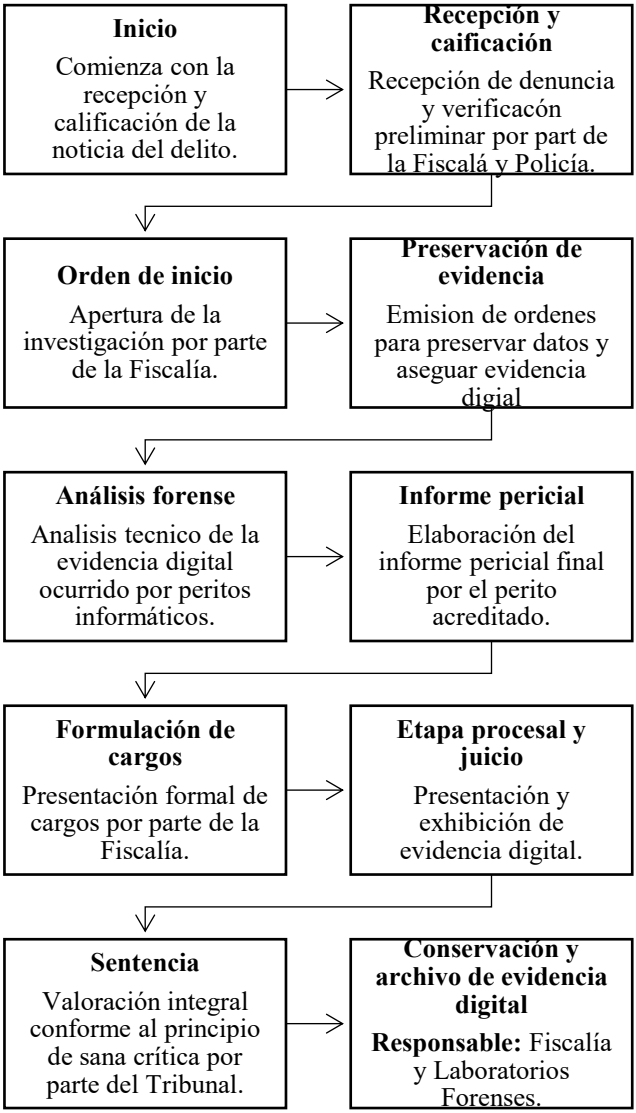
- Valoración integral conforme al principio de sana crítica.
- Reconocimiento formal de validez de evidencias digitales.
- Determinación de culpabilidad o inocencia.

16) Conservación y archivo de evidencia digital

→ **Responsable:** Fiscalía y Laboratorios Forenses

- Mantenimiento de copias forenses.

- Registro de custodia post-sentencia.
- Destrucción controlada en casos permitidos por ley.


Inicio
Comienza con la recepción y calificación de la noticia del delito.
Recepción y caificación
Recepción de denuncia y verificacón preliminar por part de la Fiscalá y Policía.
Orden de inicio
Apertura de la investigación por parte de la Fiscalía.
Preservación de evidencia
Emision de ordenes para preservar datos y aseguar evidencia digial
Análisis forense
Analisis tecnico de la evidencia digital ocurrido por peritos informáticos.
Informe pericial
Elaboración del informe pericial final por el perito acreditado.
Formulación de cargos
Presentación formal de cargos por parte de la Fiscalía.
Etapa procesal y juicio
Presentación y exhibición de evidencia digital.
Sentencia
Valoración integral conforme al principio de sana crítica por parte del Tribunal.
Conservación y archivo de evidencia digital
Responsable: Fiscalía y Laboratorios Forenses.

BIBLIOGRAFÍA

Asamblea Nacional del Ecuador. (2014). *Código Orgánico Integral Penal*. Registro Oficial Suplemento No. 180.

Council of Europe. (2001). *Convention on Cybercrime (Budapest Convention)*. https://www.coe.int/en/web/cybercrime/the-budapest-convention

Cybersecurity and Infrastructure Security Agency. (2023). *Critical infrastructure security*.

Denning, D. E. (2017). Cyber conflict as an emergent social phenomenon. *Social Science Research Council*.

Estados Unidos Mexicanos. Código Penal Federal. (2024).

European Union. (2016). *Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems (NIS*

Directive). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L1148

European Union. (2022). *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS 2)*. https://eur-lex.europa.eu/eli/dir/2022/2555

North Atlantic Treaty Organization. (2016). *Cyber defence*.

República Argentina. Ministerio de Seguridad. (2022). *Infraestructura crítica y ciberseguridad*.

República de Chile. (2022). *Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información*.

República de Colombia. Congreso de la República. (2009). *Ley 1273 de 2009*.

República del Perú. (2013). *Ley N.º 30096 – Ley de delitos informáticos*.

República Federativa del Brasil. (2014). *Marco Civil da Internet (Lei nº 12.965)*.

United Nations General Assembly. (2000). *Resolution 55/63: Combating the criminal misuse of information technologies*. https://digitallibrary.un.org/record/423046

United Nations General Assembly. (2001). *Resolution 56/121: Combating the criminal misuse of information technologies*. https://digitallibrary.un.org/record/450589

United Nations Group of Governmental Experts. (2015). *Developments in the field of information and telecommunications in the context of international security*.

United Nations Office on Drugs and Crime. (2012). *The use of the Internet for terrorist purposes*. https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

United States Congress. (2001). *USA PATRIOT Act*. https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf

United States Department of Justice. (2023). *Computer Fraud and Abuse Act (18 U.S.C. § 1030)*.

Weimann, G. (2015). *Terrorism in cyberspace: The next generation*. Woodrow Wilson Center Press / Columbia University Press.