

Índice

Dedicatoria	III
Agradecimiento	V
Prólogo	XV
Introducción	XXI
Glosario	XXV
Términos	XXVII

Capítulo Primero

ANTECEDENTES

1.1. Evolución normativa de la ciberdelincuencia en el ordenamiento jurídico ecuatoriano	3
---	---

Capítulo Segundo

ACTUALIZACIÓN LEGISLATIVA DEL CÓDIGO ORGÁNICO INTEGRAL PENAL EN MATERIA DE CIBERDELINCUENCIA Y VIOLENCIA SEXUAL DIGITAL

2.1. Reforma adjetiva y sustantiva realizada a través de la Ley Orgánica Reformatoria al Código Orgánico Integral Penal para prevenir y combatir la violencia sexual digital y fortalecer la lucha contra delitos informáticos	25
2.1.2. Pornografía con utilización de niñas, niños y adolescentes	26
2.1.3. Hostigamiento	27
2.1.4. Contravenciones de acoso escolar y académico	28
2.1.5. Violencia psicológica contra la mujer o miembros del núcleo familiar	30

2.1.6.	Acoso Sexual	31
2.1.7.	Corrupción de niñas, niños y adolescentes	34
2.1.8.	Abuso Sexual	35
2.1.9.	Extorsión Sexual	40
2.1.10.	Revelación de secreto o información personal de terceros	42
2.1.11.	Interceptación ilegal de datos	45
2.1.12.	Ataque a la integridad de sistemas informáticos	49
2.1.13.	Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	51
2.1.14.	Falsificación Informática	54
2.1.15.	Agravantes punitivas	56

Capítulo Tercero

BIEN JURÍDICO

3.1.	Bien jurídico y mandato constitucional en el ecosistema digital	63
3.2.	La funcionalidad informática como objeto de tutela en este tipo de infracciones penales	82

Capítulo Cuarto

**DELITOS CONTRA LA SEGURIDAD DE LOS ACTIVOS DE LOS
SISTEMAS DE INFORMACIÓN Y COMUNICACIÓN – CÓDIGO
ORGÁNICO INTEGRAL PENAL**

4.1.	Clasificación de los delitos contra la seguridad de los activos de los sistemas de información y comunicación	93
4.2.	Revelación ilegal de base de datos	94
4.2.1.	Elementos del tipo	95
4.2.1.1.	Sujeto activo	95
4.2.1.2.	Sujeto pasivo	96

4.2.1.3.	Bien jurídico contenido en el tipo	96
4.2.1.4.	Conducta típica	97
4.2.2.	<i>Iter criminis</i>	99
4.2.3.	Elemento subjetivo	99
4.2.4.	Objeto Material	101
4.2.5.	Ejemplo aplicado	104
4.2.6.	Convergencias y delimitación dogmática: revelación ilegal de base de datos, violación a la intimidad y revelación de secretos o información personal de terceros	106
4.2.7.	Tutela reforzada del bien jurídico: hábeas data en casos de revelación y difusión de información personal	116
4.3.	Interceptación ilegal de datos	120
4.3.1.	Elementos del tipo	121
4.3.1.1.	Sujeto activo	121
4.3.1.2.	Sujeto Pasivo	122
4.3.1.3.	Bien jurídico	124
4.3.1.4.	Conducta típica	127
4.3.2.	<i>Iter criminis</i>	141
4.3.3.	Elemento subjetivo	144
4.3.4.	Objeto Material	147
4.3.5.	Ejemplo aplicado	149
4.3.5.	Ejemplo aplicado	150
4.3.6.	Ejemplo aplicado	151
4.3.7.	Ejemplo aplicado	152
4.3.8.	Respecto al hacking ético en el delito de interceptación ilegal de datos	153
4.3.9.	Análisis entre el “acceso no consentido a sistemas informáticos, telemático o de telecomunicaciones” (artículo 234) e “interceptación ilegal de datos” (artículo	

	230.2): análisis dogmático comparado, criterios de interpretación y ejemplos	155
4.4.	Transferencia electrónica de activo patrimonial	159
4.4.1.	Elementos del tipo	159
4.4.1.1.	Sujeto Activo	159
4.4.1.2.	Sujeto Pasivo	160
4.4.1.3.	Bien jurídico	162
4.4.1.4.	Conducta típica	163
4.4.2.	<i>Iter criminis</i>	168
4.4.3.	Elemento subjetivo	170
4.4.4.	Objeto Material	171
4.4.5.	Ejemplo aplicado – Artículo 231	173
4.4.6.	Ejemplo aplicado – Artículo 231	173
4.4.7.	Delimitación dogmática entre la transferencia electrónica de activo patrimonial y la apropiación fraudulenta por medios electrónicos	175
4.4.8.	Ejemplo aplicado – Artículo 190	181
4.4.9.	Ejemplo aplicado – Apropiación Fraudulenta por medios electrónicos vs Transferencia electrónica de activo patrimonial	183
4.5.	Ataque a la integridad de sistemas informáticos	186
4.5.1.	Elementos del tipo	187
4.5.1.1.	Sujeto activo	187
4.5.1.2.	Sujeto Pasivo	187
4.5.1.3.	Bien jurídico	188
4.5.1.4.	Conducta típica	190
4.5.2.	<i>Iter criminis</i>	193
4.5.3.	Elemento subjetivo	196
4.5.4.	Objeto Material	198

4.5.5.	Inciso segundo del artículo 232 del Código Orgánico Integral Penal	205
4.5.5.1.	En cuanto a los elementos objetivos de este inciso	207
4.5.5.2.	Tipicidad subjetiva	209
4.5.5.3.	<i>Iter criminis</i>	209
4.5.6.	Inciso tercero del artículo 232 del Código Orgánico Integral Penal	211
4.5.7.	Reforma de este delito según la Ley Orgánica para el fortalecimiento de Ciberseguridad	212
4.5.8.	Ejemplo aplicado	228
4.6.	Delitos contra la información pública reservada legalmente	229
4.6.1.	Elementos del tipo	231
4.6.1.1.	Sujeto activo	231
4.6.1.2.	Sujeto pasivo	234
4.6.1.3.	Bien jurídico	236
4.6.1.4.	Conducta Típica	246
4.6.2.	<i>Iter criminis</i>	248
4.6.3.	Elemento subjetivo	250
4.6.4.	Objeto Material	253
4.6.5.	Ejemplo aplicado – Artículo 233	254
4.6.6.	Ejemplo aplicado – Artículo 233	255
4.6.7.	Ejemplo aplicado – Artículo 233	256
4.6.8.	Ejemplo aplicado – Artículo 233	257
4.7.	Acceso no consentido a sistemas informático, telemático y o de telecomunicaciones	261
4.7.1.	Elementos del tipo	262
4.7.1.1.	Sujeto activo	262
4.7.1.2.	Sujeto Pasivo	263
4.7.1.3.	Bien Jurídico	264
4.7.1.4.	Conducta Típica	267
4.7.2.	<i>Iter criminis</i>	271

4.7.3.	Elemento Subjetivo	274
4.7.4.	Hacking ético en el delito de acceso no consentido a sistemas informáticos, telemático o de telecomunicaciones	277
4.7.5.	Objeto Material	283
4.7.6.	Ejemplo aplicado	287
4.7.7.	Ejemplo aplicado	288
4.7.8.	Ejemplo aplicado - Circunstancia Fáctica Compleja	289
4.8.	Falsificación informática	291
4.8.1.	Elementos del tipo	292
4.8.1.1.	Sujeto activo	292
4.8.1.2.	Sujeto Pasivo	293
4.8.1.3.	Bien jurídico	294
4.8.1.4.	Conducta Típica	297
4.8.2.	Análisis de este tipo penal en relación con el Convenio de Budapest	300
4.8.3.	Iter criminis	306
4.8.4.	Elemento Subjetivo	312
4.8.5.	Objeto Material	315
4.8.6.	Ejemplo aplicado - Artículo 234.1	317
4.8.7.	Ejemplo aplicado - Artículo 234.1	318

Capítulo Quinto

INVESTIGACIÓN PENAL, EVIDENCIA DIGITAL Y COOPERACIÓN INTERNACIONAL EN MATERIA DE CIBERDELINCUENCIA

5.1.	Creación de la Unidad Especializada de Ciberdelito de la Fiscalía General del Estado	323
5.2.	Contenido Digital	326
5.3.	El tratamiento procesal del contenido digital y su articulación con el Convenio de Budapest sobre Ciberdelincuencia	338

5.4.	Cooperación Internacional	344
------	---------------------------------	-----

Capítulo Sexto

**ANÁLISIS ESTADÍSTICO Y TENDENCIAS
DE LA CIBERDELINCUENCIA**

6.1.	Comportamiento, evolución y patrones de la criminalidad informática	357
6.2.	Evolución y dinámica del registro delictivo	361
6.2.1.	Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	361
6.2.2.	Ataque a la integridad de sistemas informáticos	362
6.2.3.	Transferencia Electrónica de Activo Patrimonial	362
6.2.4.	Interceptación Ilegal de Datos	363
6.2.5.	Falsificación Informática	363
6.2.6.	Revelación Ilegal de Base de Datos	364
6.2.7.	Delito contra la información pública reservada legalmente	364
6.3.	Trayectoria procesal de los casos: del registro a la decisión	365
	Bibliografía	369