

## ÍNDICE

---

<i>Prólogo</i> , del Prof. Dr. MARCELO A. RIGUERT . . . . .	13
<b>I. Crimen organizado trasnacional y cibercrimen</b> . . . .	19
1. De la fenomenología del cibercrimen . . . . .	19
1.1. Introducción . . . . .	19
1.2. Definición y alcance . . . . .	20
1.3. Principales desafíos en torno al cibercrimen	22
2. Evolución del cibercrimen organizado transnacio- nal . . . . .	26
2.1. Del pirata informático solitario a un mercado de servicios de cibercrímenes . . . . .	26
2.2. Crimen organizado y cibercrimen . . . . .	29
3. Derecho internacional y derecho penal sustantivo contra el cibercrimen organizado trasnacional . .	30
3.1. Selección de iniciativas a nivel global sobre ley sustantiva de cibercrimen . . . . .	31
3.1.1. Naciones Unidas . . . . .	31
3.1.2. Unión Internacional de Telecomuni- caciones . . . . .	32

3.1.3. Academia . . . . .	33
3.2. Convención del Consejo de Europa sobre el Ciberdelincuencia . . . . .	34
3.2.1. Resumen histórico, aplicabilidad y alcance . . . . .	34
3.2.2. Delitos contra los sistemas TIC . . . .	37
3.2.3. Delitos relacionados con la informática y el contenido . . . . .	42
3.2.4. Protocolo adicional (actos de natura- leza racista y xenófoba) . . . . .	46
3.3. Otras iniciativas seleccionadas a nivel regio- nal acerca del ciberdelincuencia . . . . .	46
3.3.1. Unión Europea . . . . .	46
3.3.2. Comunidad de Estados Independien- tes . . . . .	49
3.3.3. Organización de Cooperación de Shan- ghai . . . . .	50
3.3.4. Liga de los Estados Árabes . . . . .	50
3.3.5. Comunidad Económica de los Estados de África Occidental . . . . .	51
3.3.6. Unión Africana . . . . .	53
3.3.7. Leyes modelo . . . . .	54
4. Derecho internacional. Investigación y enjuicia- miento coordinado y cooperativo del ciberdelincuencia organizado transnacional . . . . .	54
4.1. Requisitos de los poderes de investigación en derecho internacional sobre ciberdelincuencia . .	55
4.1.1. Medidas coercitivas en general . . . .	55
4.1.2. Identificación de suscriptores, reten- ción de datos de tráfico e identificación de información . . . . .	57

4.2. Cooperación internacional en la investigación y enjuiciamiento del cibercrimen organizado trasnacional . . . . .	59
4.2.1. Modos tradicionales de cooperación en el cibercrimen organizado trasnacional . . . . .	59
4.2.2. Tratamiento de la volatilidad de los datos informáticos . . . . .	60
5. Jurisdicción aplicable en el cibercrimen organizado trasnacional . . . . .	62
5.1. Jurisdicción para aplicar y decidir . . . . .	62
5.2. Jurisdicción para hacer cumplir . . . . .	63
6. Observaciones finales . . . . .	66
<b>II. Cibercrimen y compliance en el cibercrimen . . . . .</b>	<b>69</b>
1. Introducción . . . . .	69
2. Compliance en el cibercrimen en cuatro niveles . . . . .	72
2.1. Primer nivel: corporaciones, agentes y órganos . . . . .	72
2.2. Segundo nivel: empleados, cadena de suministro y personas cercanas a la corporación . . . . .	74
2.3. Tercer nivel: ataques externos contra los sistemas de información . . . . .	76
2.4. Cuarto nivel: delitos por/entre usuarios . . . . .	79
3. Conclusión . . . . .	83
<b>III. Rol del derecho penal en la regulación del cibercrimen y la seguridad informática . . . . .</b>	<b>85</b>
1. Derecho penal y regulación: conceptos básicos, modelos y limitaciones . . . . .	86
1.1. Rol del derecho penal . . . . .	87

1.2. Limitaciones genéricas al derecho penal. . .	89
1.3. ¿Derecho penal como herramienta regulato- ria? . . . . .	93
2. Leyes penales sustantivas sobre cibercrimen en Europa y Alemania: una visión general. . . . .	97
2.1. Tipología de las leyes sobre cibercrimen. . .	97
2.2. Derecho penal de la UE sobre cibercrimen	99
2.3. Leyes penales sustantivas alemanas sobre cibercrimen . . . . .	103
3. Ley de cibercrimen y regulación de la seguridad TI	106
3.1. Represión específica y prevención de ataques a sistemas TI: ataques y atacantes . . . . .	107
3.2. Represión mediada y prevención de ata- ques a sistemas informáticos: requisitos y obligaciones del derecho penal en materia de seguridad TI. . . . .	110
3.3. Represión indirecta y prevención de ataques a sistemas informáticos: responsabilidad penal negligente. . . . .	116
4. Conclusión . . . . .	120
<b>IV. Cibercrimen, derechos humanos y política digital . . .</b>	<b>125</b>
1. Cibercrimen como escudo y espada en relación con los derechos humanos . . . . .	125
1.1. Cibercrimen y herramienta de criminaliza- ción . . . . .	125
1.2. Sobre la influencia política de la “lucha contra el cibercrimen” . . . . .	126
1.3. Cibercrimen como escudo y espada . . . . .	127
1.4. Principales desafíos del cibercrimen. . . . .	131

2. Cibercrimen: visión general desde una perspectiva basada en los derechos humanos . . . . .	132
2.1. Parte General, incluida la jurisdicción . . . .	134
2.2. Delitos contra TIC . . . . .	138
2.3. Delitos relacionados con la informática y el contenido . . . . .	140
3. Investigaciones penales en el ciberespacio: desafíos desde la perspectiva de los derechos humanos. .	141
3.1. Medidas coercitivas . . . . .	142
3.2. Identificación de abonados y retención de datos de telecomunicaciones . . . . .	145
3.3. Cooperación internacional y la jurisdicción para hacer cumplir. . . . .	148
4. Perspectivas . . . . .	152

<b>Anexo: Los delitos informáticos en el Código Penal argentino,</b> por María Belén Linares . . . . .	155
1. Planteamiento sistemático . . . . .	155
2. Seguridad informática . . . . .	157
3. Delitos informáticos regulados en el Código Penal argentino . . . . .	160
3.1. Producción, distribución y tenencia de pornografía infantil (art. 128, C.P.) . . . . .	160
3.2. Ciberacoso sexual de menores (art. 131, C.P) . . . . .	166
3.3. Violación de correspondencia digital (art. 153, C.P) . . . . .	169
3.4. Acceso ilegítimo a datos o a sistema informático (art. 153 bis, C.P) . . . . .	172
3.5. Publicación ilegal o abusiva de comunicación electrónica (art. 155, C.P) . . . . .	174

3.6. Revelación de secretos oficiales (art. 157, C.P) .....	176
3.7. Acceso ilegítimo, difusión o alteración de datos personales (art. 157 bis, C.P) .....	178
3.8. Estafa o fraude informático (art. 173, inc. 16, C.P) .....	181
3.9. Daño en datos y sistemas informáticos (arts. 183 y 184, C.P). ....	183
3.10. Interrupción o entorpecimiento de comunicaciones electrónicas (art. 197, C.P). ....	186
3.11. Alteración de medios probatorios (art. 255, C.P) .....	188
3.12. Otros tipos penales facilitados por las TICs	189
4. Reflexiones finales .....	190
<i>Bibliografía.</i> .....	193