

1ª EDICIÓN

LUCAS MOYANO

Ciberdelitos

CÓMO INVESTIGAR EN ENTORNOS DIGITALES

DEBIDO PROCESO: GARANTÍAS CONSTITUCIONALES. TIPOS PENALES: «MASI», «GROOMING», VIOLACIÓN DE CORRESPONDENCIA ELECTRÓNICA, ACCESO ILEGÍTIMO, PUBLICACIÓN ABUSIVA, ESTAFAS Y DEFRAUDACIONES DIGITALES: «CARDING», «PHISHING», «SEXTORSIÓN». ACCIONES NO TIPIFICADAS: «DOXING», SUPLANTACIÓN DE IDENTIDAD, DIFUSIÓN NO CONSENTIDA DE IMÁGENES ÍNTIMAS, VENTA DE DATOS PERSONALES, HOSTIGAMIENTO DIGITAL. PASO A PASO DE LA INVESTIGACIÓN: PREPARACIÓN, TEORÍA DEL CASO Y GUÍA DE DENUNCIA. MEDIDAS CAUTELARES Y MEDIOS DE PRUEBA: OBTENCIÓN Y PRESERVACIÓN DE EVIDENCIA DIGITAL. CADENA DE CUSTODIA Y DESBLOQUEO COMPULSIVO DE TELÉFONOS. AGENTE REVELADOR DIGITAL Y ALLANAMIENTO REMOTO. CRIPTOACTIVOS. «VAIC». EXTRACCIÓN DE EVIDENCIA DIGITAL EN DISPOSITIVOS MÓVILES Y REDES SOCIALES. REQUERIMIENTOS A PLATAFORMAS Y PROVEEDORES DE SERVICIOS DE INTERNET

EN ANEXO: MODELOS DE ESCRITOS - JURISPRUDENCIA

PRÓLOGO DE **HERNÁN BLANCO** - PRESENTACIÓN DE **MARCOS SALT**



INCLUYE CONTENIDO
AUDIOVISUAL

h
hammurabi
JOSE LUIS DEPALMA EDITOR

ÍNDICE GENERAL

DEDICATORIA	7
PALABRAS PREVIAS	21
PRÓLOGO	25
PRESENTACIÓN	29
ABREVIATURAS	33

PRIMERA PARTE DELITOS INFORMÁTICOS Y DEBIDO PROCESO

Capítulo I

INTRODUCCIÓN

§ 1. Delitos informáticos	41
a) La complejidad de estos tipos de delitos: retos y desafíos que se presentan	41
b) Dificultades de la investigación	42
1. El anonimato	42
2. Comisión de delitos a distancia	43
c) Particularidades de la investigación digital	43
§ 2. Nociones informáticas. ¿Cómo funciona Internet?	47
§ 3. Garantías constitucionales en entornos penales digitales. Debido proceso penal	50
a) Introducción	50
b) Garantías de carácter general	52
c) Garantías de carácter específico	55
d) La influencia de la tecnología en el sistema penal argentino	56
e) Vulneraciones. Jurisprudencia relevante y nuevos desafíos	57
f) Desafíos de la investigación digital	59

g) Algunos casos de la jurisprudencia internacional	59
h) Recomendaciones	63
i) Palabras finales	64
§ 4. Investigación con perspectiva de género	66

Capítulo II

MARCO LEGAL. ANÁLISIS DE LOS TIPOS PENALES

§ 5. Definiciones	67
§ 6. Tipos penales	68
a) Material de difusión sexual infantil. Difusión, distribución, tenencia y suministro (art. 128, CP)	68
1. Introducción	68
2. Bien jurídico protegido	69
3. Sujetos	70
4. Acciones típicas	72
I. Párrafo primero («... producir, financiar, ofrecer, comerciar, publicar, facilitar, divulgar o distribuir...»)	72
I.1 Tipo objetivo	72
I.2 La representación	73
I.3 ¿Cómo determinar cuándo una imagen o video resultan lascivos?	73
I.4 Clasificación de las imágenes	73
I.5 Tipicidad subjetiva	74
I.6 Consumación y tentativa	74
II. Párrafo segundo («... a sabiendas tuviere en su poder representaciones...»)	74
II.1 Acción típica	74
II.2 Sujetos	74
II.3 Aspecto subjetivo	75
II.4 Consumación. Tentativa	75
III. Párrafo tercero («... el que tuviere en su poder representaciones de las descritas en el primer párrafo con fines inequívocos de distribución o comercialización...»)	75
III.1 Acción típica	75
III.2 Sujetos	75
III.3 Tipicidad subjetiva	75
III.4 Consumación. Tentativa	76
IV. Párrafo cuarto («... facilitar el acceso a espectáculos pornográficos o suministrar material pornográfico a menores de catorce años...»)	76
IV.1 Acción típica	76
IV.2 Sujetos	76
IV.3 Tipicidad subjetiva	76
IV.4 Consumación. Tentativa	76
b) Los tipos penales de violación de secreto y privacidad (arts. 153, 153 «bis», 155, 157 y 157 «bis», CP)	76
1. Bien jurídico protegido	76

2. Acción penal	77
3. Violación de correspondencia electrónica (art. 153, CP)	77
I. Apertura o acceso a la correspondencia electrónica	77
I.1 Tipo subjetivo	78
I.2 Sujeto	78
I.3 Consumación y tentativa	78
II. Apoderamiento de una comunicación electrónica	78
II.1 Tipo objetivo	78
II.2 Tipo subjetivo	78
II.3 Sujetos	79
II.4 Consumación y tentativa	79
III. Supresión y desvío de comunicaciones electrónicas	79
III.1 Acción típica	79
III.2 Tipo subjetivo	79
III.3 Sujetos	79
III.4 Consumación y tentativa	80
IV. Interceptación y captación indebida de comunicaciones electrónicas	80
IV.1 Acción típica	80
IV.2 Tipo subjetivo	80
IV.3 Sujetos	80
IV.4 Consumación y tentativa	80
V. Comunicación o publicación ilegítima de correspondencia electrónica	81
V.1 Acción típica	81
V.2 Tipo subjetivo	81
V.3 Sujetos	81
V.4 Consumación y tentativa	81
VI. Agravamiento de la acción cuando fuera cometida por funcionario público	81
4. Acceso ilegítimo a sistema informático (art. 153 «bis», CP)	82
I. Bien jurídico protegido	82
II. Acción penal	82
III. Acción típica	82
IV. Tipo subjetivo	83
V. Sujetos	83
VI. Consumación y tentativa	83
VII. Agravante por perjuicio a un sistema o dato informático, de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros	83
5. Publicación abusiva de correspondencia (art. 155, CP)	83
I. Bien jurídico protegido	84
II. Acción penal	84
III. Acción típica	84
III.1 Tipo objetivo	84
III.2 Tipo subjetivo	85
IV. Sujetos	85
V. Consumación y tentativa	85

6. Revelación de secretos (art. 157, CP)	85
I. Bien jurídico protegido	85
II. Acción penal	85
III. Acción típica	85
III.1 Tipo objetivo	85
III.2 Tipo subjetivo	86
IV. Sujetos	86
V. Consumación y tentativa	86
7. Acceso ilegítimo a un banco de datos, revelación ilegítima de información y alteración de datos (art. 157 «bis», CP)	86
I. Bien jurídico protegido	86
II. Acción penal	86
III. Acción típica	86
III.1 Tipo objetivo	86
III.2 Tipo subjetivo	87
IV. Sujetos	87
V. Consumación y tentativa	88
VI. Agravante por la calidad de funcionario público	88
c) Defraudación informática (art. 173, inc. 16, CP)	88
1. Bien jurídico protegido	88
2. Acción penal	88
3. Acción típica	88
I. Tipo objetivo	88
II. Tipo subjetivo	89
4. Sujeto	90
5. Consumación y tentativa	90
d) Daño informático (art. 183, CP)	90
1. Bien jurídico protegido	90
2. Acción penal	90
3. Acción típica	90
I. Tipo objetivo	90
I.1 Alteración, destrucción o inutilización de datos, documentos, programas o sistemas informáticos. Sabotaje informático	91
I.2 Venta, distribución, circulación o introducción de cualquier programa destinado a causar daños en un sistema informático	91
II. Tipo subjetivo	91
4. Subsidiariedad	91
5. Sujetos	92
6. Consumación y tentativa	92
e) Daño informático agravado (art. 184, CP)	92
1. Bien jurídico protegido	92
2. Acción penal	92
3. Acción típica	93
I. Tipo objetivo	93
II. Tipo subjetivo	93

4. Sujetos	93
5. Consumación y tentativa	93
f) Bloqueo de comunicaciones informáticas (art. 197, CP)	93
1. Bien jurídico protegido	93
2. Acción penal	93
3. Acción típica	94
I. Tipo objetivo	94
II. Tipo subjetivo	94
4. Sujetos	94
5. Consumación y tentativa	94
g) Bloqueo de comunicaciones informáticas (art. 255, CP)	95
1. Bien jurídico protegido	95
2. Acción penal	95
3. Acción típica	95
I. Tipo objetivo	95
II. Tipo subjetivo	95
4. Sujetos	96
5. Consumación y tentativa	96
6. Agravante por la calidad de depositario	96
7. Comisión por imprudencia o negligencia del depositario	96
h) Ciberacoso sexual de menores (art. 131, CP)	96
1. Bien jurídico protegido	96
2. Acción penal	97
3. Acción típica	97
4. Tipo subjetivo: ultraintencionalidad	97
5. Sujetos	98
6. Consumación y tentativa	98
§ 7. Normativa de delitos informáticos	100
a) Normativa internacional sobre delitos informáticos. Convención sobre Cibercriminalidad	100
b) Segundo Protocolo Adicional del Convenio sobre Ciberdelincuencia del Consejo de Europa, conocido como Convenio Budapest	101
1. Cooperación directa con proveedores y entidades del sector privado	102
I. Solicitud de información sobre registro de nombres de dominio (art. 6º)	102
II. Solicitud de información sobre abonados (art. 7º)	103
2. Procedimientos para mejorar la cooperación internacional entre autoridades para la divulgación de datos informáticos almacenados	104
I. Obtención rápida de datos almacenados en otro Estado (art. 8º)	104
II. Divulgación acelerada de datos informáticos de emergencia (art. 9º)	105
III. Asistencia mutua en situaciones de emergencia (art. 10)	105
3. Procedimientos relativos a la cooperación internacional en ausencia de acuerdos internacionales aplicables	106
I. Videoconferencia (art. 11)	106
II. Equipos Conjuntos de Investigación e Investigaciones Conjuntas (art. 12)	106
c) Normativa nacional sobre delitos informáticos	106

Capítulo III

ACCIONES NO TIPIFICADAS

§ 8. El hostigamiento digital	109
§ 9. «Doxing»	111
§ 10. Publicación no consentida de imágenes íntimas	111
§ 11. «Sextorsión»	114
§ 12. Suicidio feminicida por inducción o ayuda	115
§ 13. Suplantación de identidad	115
§ 14. «Phishing»	117
§ 15. Venta de datos personales	118
§ 16. Secuestro de datos informáticos	118
§ 17. Hurto informático	119
§ 18. Incitación al odio	120

SEGUNDA PARTE

PRÁCTICA FORENSE

Capítulo IV

¿CÓMO PREPARAR LA INVESTIGACIÓN?

§ 19. La investigación penal preparatoria y la teoría del caso	125
a) Principio de libertad probatoria	126
b) Principio de objetividad	128
c) Acceso a la justicia de las víctimas	128
d) Principio de continuidad	129
— Teoría del caso	131
§ 20. Toma de denuncias	133
a) Características de la Evidencia Digital	133
b) Principios de Manejo de la Evidencia digital	133
c) Elementos a tener en cuenta al momento de tomar denuncias por el delito de «grooming»	135
d) Guía de evidencia para incorporar a la denuncia	136
1. Identificar el dispositivo de la víctima	137
2. Capturas de pantalla de las conversaciones mantenidas por WhatsApp	138
3. Redes sociales	141
4. Utilización de Google Maps	143
5. Investigación utilizando Google Maps	147
6. ¿Cómo encontrar un dispositivo perdido o sustraído?	148
§ 21. Medidas urgentes	152
a) Preservación de la evidencia digital	152
b) Preservación de perfiles	153
1. Google	153
2. Meta	154
c) Paso a paso cómo preservar un perfil de Facebook o Instagram	155

Capítulo V

¿CÓMO INVESTIGAR EN EL CIBERESPACIO?

§ 22. ¿Cómo investigar un delito informático?	159
a) Introducción	159
b) Línea de investigación	161
§ 23. Investigación de estafas	165
a) Presentación del caso	165
b) Nuevos esquemas delictivos. Transformación del dinero a criptoactivos	168
c) Formas de actuación. Información a recabar al momento de la denuncia	169
1. Oficiar al banco emisor	170
2. Oficiar al banco destinatario	172
3. Oficiar a COELSA	176
4. Oficiar al Banco Central de la República Argentina	176
5. Aspectos a tener en cuenta en investigación de estafas donde se utilice a modalidad «mulas bancarias» y compra de criptomonedas	178
— Rastreo criptográfico	179
§ 24. Investigación de delito de difusión de material de abuso sexual infantil	181
a) Inicio de la investigación	181
b) Línea de investigación	183
§ 25. Investigación de «grooming»	186
a) Inicio	186
b) Línea de investigación	186
§ 26. OSINT: Ingeniería social. Investigaciones en fuentes abiertas	189
a) OSINT: Ingeniería social	189
b) Comandos de búsqueda avanzada	190
c) Metodología de OSINT	196
§ 27. Extorsión: pautas a tener en cuenta para su investigación	202
§ 28. «Carding», la organización criminal. Caso práctico. Elementos a tener en cuenta	205
— Caso práctico	207
§ 29. Pasos para diligenciar oficios judiciales para Facebook e Instagram	210

Capítulo VI

MEDIOS DE PRUEBA

§ 30. Herramientas de investigación para delitos complejos. Agente encubierto y agente revelador para las investigaciones en entornos digitales. Intervención policial en investigaciones digitales en otros supuestos	213
a) Agente encubierto y agente revelador digital	215
b) Agente revelador en Telegram	216
— Jurisprudencia	217
c) Intervención policial en investigaciones digitales en otros supuestos	218
d) ¿Qué herramientas se pueden utilizar para la creación de un Avatar para obtener información el Agente Encubierto Digital?	220

§ 31. Medidas de allanamiento, registro, requisa, secuestro y análisis de dispositivos mediante triage. Secuestro de criptoactivos. Secuestro de datos en extraña jurisdicción. Allanamiento remoto. doctrina «plain view»	220
a) Registro domiciliario (allanamiento)	220
1. Forma del procedimiento	221
2. Allanamiento de morada	222
3. Allanamiento de otros locales	222
b) Requisa personal	222
— Requisitos	222
c) Secuestro	223
1. Secuestro de criptoactivos	224
2. Secuestro de datos en extraña jurisdicción	226
— La Ley Cloud Act de EE.UU. y su importancia en las investigaciones	230
d) Solicitud de triage al momento de realizarse el allanamiento	231
— Modelo de solicitud de triage	234
e) Allanamiento remoto	235
1. Allanamiento remoto mediante «software» judicial	236
2. Utilización del allanamiento remoto en la jurisprudencia	237
3. Regulación procesal en España	239
4. Regulación en nuestro sistema procesal	240
5. La libertad probatoria y el allanamiento remoto	242
6. Importancia de la cadena de custodia	243
7. Conclusión	243
f) Registro y secuestro de datos en un sistema informático. ¿Es aplicable la doctrina del hallazgo a simple vista o «plain view»?	244
1. Hallazgo casual o «plain view doctrine» en el ámbito físico	245
2. Hallazgo casual en el entorno digital	245
3. ¿Cómo debemos proceder en el caso de encontrarnos con el descubrimiento casual de indicios de otro delito distinto al investigado?	247
§ 32. Desbloqueo compulsivo de dispositivos telefónicos y de las aplicaciones contenidas	247
a) Desbloqueo compulsivo de dispositivo celular	247
b) Desbloqueo de aplicaciones contenidas en los dispositivos telefónicos	251
c) Modelo de solicitud de desbloqueo de dispositivo telefónico	252
§ 33. La Geovalla como herramienta de investigación	253
§ 34. Vínculos por análisis informáticos de las comunicaciones (VAIC)	256
§ 35. Trazabilidad de criptoactivos	273
a) Criptoactivos y cibercrimen	273
b) Anonimato, ofuscamiento y servicio de mixado	281
c) Usando herramientas en investigaciones	282
— Maltego	283
§ 36. Cómo obtener evidencia digital de dispositivos móviles y de redes sociales	284
a) Evidencia digital en dispositivos móviles	285
1. Formas de incorporación de evidencia digital de dispositivos móviles	286
I. Dispositivo aportado por la víctima	286
II. Dispositivo móvil de un imputado	287

III. Extracción con UFED o similar	288
IV. Por parte de un tercero voluntario	288
b) Redes sociales	288
c) Resguardo de correos electrónicos	289
§ 37. Requerimiento de datos a las ISP / LACNIC y organismos nacionales e internacionales, estatales como privados	289
a) Prestadoras de servicio de Internet (ISP)	290
b) Organismos estatales	290
c) Requerimientos a LACNIC	290
d) Organismos privados	291
§ 38. Cadena de custodia	291
§ 39. Cómo se extraen los datos de un equipo. Funcionamiento del dispositivo universal de extracción forense (UFED)	296
a) Extracción lógica	297
1. Extracciones lógicas de dispositivos iOS	297
2. Extracciones físicas en equipos Apple	297
3. ¿Cómo sabe el examinador qué método elegir?	298
4. Extracción del sistema de archivos	298
5. Decodificación	298
6. ¿Puede la decodificación perder algunos datos?	299
7. Nivelación de desgaste y recolección de basura	299
b) Extracción física	300
1. Cargadores de arranque	301
2. Otras metodologías de extracción física	301
c) Autenticación y generación de informes	302

Capítulo VII

¿QUÉ MEDIDAS CAUTELARES PODEMOS SOLICITAR EN EL PROCESO PENAL?

§ 40. Introducción	305
§ 41. Medidas cautelares civiles aplicadas al proceso penal	306
§ 42. Inmovilización de fondos en cuenta de destino	308
§ 43. Medida cautelar de no innovar	309
§ 44. Medida cautelar innovativa	310
§ 45. Cautela personal	312
a) Detención	312
b) Prisión preventiva	313

Capítulo VIII

CIERRE DE INSTRUCCIÓN

§ 46. Declaración del imputado	315
§ 47. Inicio de la declaración del imputado	316
a) Interrogatorio de identificación	316

b) Forma de la indagatoria	317
c) Información al imputado	317
d) Acta	317
§ 48. Elevación a juicio	318

CONCLUSIÓN

	319
--	-----

ANEXO I

MODELOS DE ESCRITOS JUDICIALES

1. Modelos de solicitud de bloqueo de cuenta	321
Modelo (A)	321
Modelo (B)	322
2. Modelos de solicitud de medida cautelar	323
3. Modelo de oficio de investigación de estafa	325
4. Modelo de llamado a declaración del imputado	325
5. Modelo de elevación a juicio	326
6. Modelos de oficios de investigación de difusión de material de abuso sexual infantil	329
Modelo (A)	329
Modelo (B)	329
Modelo (C)	330
Modelo (D)	330
7. Modelo de intervención telefónica	331
8. Modelo de solicitud de allanamiento	332
9. Modelo de solicitud de detención	333

ANEXO II

JURISPRUDENCIA

I. Material de abuso sexual infantil (art. 128, CP)	337
1. Bien jurídico tutelado. Terminología. Sexualización de los menores. Contenido de los archivos	337
2. Concepto de explotación sexual infantil	338
3. Tenencia MASI	338
4. Distribución MASI	339
5. Facilitación	339
6. Tenencia con fines de distribución	339
7. Tipo subjetivo	340
8. Red P2P	340
II. «Grooming»	341
1. Configuración	341
2. Indemnidad sexual	342
3. Concurso de delitos	342
4. Inicio del contacto	344

III. Violación de correspondencia electrónica (art. 153, CP)	344
1. Competencia	345
2. Violencia de género. Inspección de celulares	345
IV. Acceso ilegítimo a sistema informático (art. 153 bis, CP)	345
1. Concurso de delitos	346
2. Competencia. Delitos de acción privada	346
3. Competencia. Comunicación electrónica. Correo electrónico. Facebook	347
V. Publicación abusiva de correspondencia (art. 155, CP)	347
VI. Revelación de secretos (arts. 157 y 157 bis, CP)	348
1. Atipicidad	348
2. Ejercicio de la acción penal. Delito de acción privada	349
3. Configuración	349
4. Competencia. Conflictos o cuestiones de competencia	350
5. Acción penal	350
VII. Estafa (art. 172, CP)	350
— Ardid	350
VIII. Defraudación informática (art. 173, inc. 16, CP)	351
1. Tipo subjetivo	352
2. Absolución	352
3. Técnicas de manipulación informática	353
4. «Hackers»	353
5. Concurso de delitos. Criptofraude	354
6. Competencia	354
IX. Daño (arts. 183 y 184, CP)	355
1. Tipo. Requisitos	356
2. Competencia	356
3. Nulidad	356
4. Configuración	356
5. Daño agravado	357
6. Concurso de delitos	357
X. Bloqueo de comunicaciones (art. 197, CP)	357
— Concurso de delitos	357
XI. Alteración de prueba, registros y documentos (art. 255, CP)	358
XII. Investigación	358
1. «Plain View»	358
2. Investigación digital	359
3. Autorización agente encubierto digital. Requisitos. Forma de implementación	359

BIBLIOGRAFÍA GENERAL

363