

ÍNDICE GENERAL



ABREVIATURAS 17

A. DOCTRINA

1. DERECHO PENAL. PARTE GENERAL

| | | |
|----------|--|----|
| 1 | NEURODERECHOS Y CRIMINALIDAD INFORMÁTICA. DERECHOS HUMANOS EMERGENTES EN LA ERA DIGITAL | |
| | CARLOS CHRISTIAN SUEIRO | |
| | § 1. Introducción | 26 |
| | § 2. Rinterfaz cerebro-computadora (ICC). La transmisión de información de un organismo biológico a un organismo cibernético | 27 |
| | a) Conducción de vehículos automotores | 29 |
| | b) Pilotaje de aeronaves | 29 |
| | c) Control de robots | 30 |
| | d) Industria de los videojuegos | 30 |
| | e) Educación y pedagogía | 30 |
| | § 3. Derechos humanos emergentes en la era digital | 32 |
| | § 4. Neuroderechos y criminalidad informática | 36 |
| | a) Derecho a la privacidad mental | 38 |
| | b) Derecho a la integridad mental | 40 |
| | c) Derecho a la continuidad psicológica | 41 |
| | § 5. Criminalidad informática y el posible surgimiento de neurodelitos | 42 |
| | § 6. Conclusión | 43 |

| | | |
|----------|--|----|
| 2 | MODELO DE DISEÑO DE UNA POLÍTICA PÚBLICA EN MATERIA DE CIBERCRIMEN EN LA ARGENTINA: LA PROHIBICIÓN DE PUBLICACIÓN DE AVISOS DE OFERTAS O DE COMERCIO SEXUAL EN INTERNET | |
| | GUSTAVO SAIN | |
| | § 1. Los delitos informáticos la seguridad de las personas | 45 |
| | a) Seguridad humana y cibercrimen | 45 |
| | b) Las resoluciones técnico-legales de la ciberseguridad | 47 |
| | c) Las motivaciones económicas de las primeras respuestas frente al cibercrimen | 48 |
| | d) El cibercrimen y la «seguridad nacional» | 51 |
| | § 2. Estudio de caso: política de intervención del Ministerio de Justicia y Derechos Humanos de la Nación de la República Argentina por sobre publicaciones ilícitas en la web | 52 |
| | a) Prohibición de publicación de avisos de comercio sexual en avisos clasificados de medios gráficos | 52 |
| | b) Desempeño de la Oficina de Monitoreo de Publicación de Avisos de Comercio Sexual | 54 |
| | c) Publicación de avisos de oferta de comercio sexual en Internet y la web | 54 |
| | d) Líneas de acción estratégicas para la elaboración de una política de supervisión de avisos de comercio sexual en Internet | 55 |
| | a) Recomendaciones de tipo instrumentales | 59 |
| | b) Recomendaciones de tipo operativas | 63 |
| | § 3. Reflexiones finales | 73 |
| | — La necesidad de políticas integrales en materia de ciberseguridad | 73 |

3

LA REGULACIÓN PENAL EN MATERIA DE VIOLENCIA FAMILIAR Y DE GÉNERO TRAS LA REFORMA DE 2015. ESPECIAL REFERENCIA AL ÁMBITO TECNOLÓGICO

PAZ LLORIA GARCÍA

| | |
|--|-----|
| § 1. Introducción | 78 |
| § 2. La tutela penal de la violencia en el ámbito de las relaciones de pareja: evolución histórico-normativa | 79 |
| a) La falta de protección hasta 1989 | 79 |
| b) La regulación penal específica desde 1989 | 80 |
| c) El Código Penal de 1995 y sus reformas hasta 2015 | 81 |
| § 3. La reforma penal de 2015. El derecho vigente | 86 |
| a) Modificaciones relativas a la parte general. Especial referencia a la agravante de discriminación por razón de género | 86 |
| b) Modificaciones relativas a la parte especial | 91 |
| 1. Lesiones | 91 |
| 2. Integridad moral | 94 |
| 3. Amenazas y coacciones | 96 |
| 4. Acoso predatorio («stalking») | 98 |
| 5. La difusión in consentida de imágenes íntimas («sexting») | 103 |
| § 4. Algunas reflexiones finales | 112 |

2. DERECHO PENAL. PARTE ESPECIAL

1

«PHISHING»: ABORDAJE DEL FENÓMENO DESDE LA PREVENCIÓN Y LA INVESTIGACIÓN

PABLO H. GRIS MUNIAGURRIA - NORA A. CHERÑAVSKY DIÓGENES A. MOREIRA

| | |
|--|-----|
| § 1. Introducción. La regulación actual del fenómeno y la proyectada | 117 |
| § 2. El caso | 123 |
| § 3. ¿Cómo abordar el problema del «phishing»? | 130 |
| § 4. Conclusión | 132 |

2

EL USO DE «BITCOINS» PARA LAVAR ACTIVOS. APROXIMACIÓN A UNA TÉCNICA DELICTIVA

MARÍA BELÉN LINARES

| | |
|--|-----|
| § 1. Sistemática adoptada | 136 |
| § 2. Consideraciones preliminares sobre la «bitcoin» | 136 |
| a) Concepto y caracterización | 136 |
| b) Tratamiento normativo en la Argentina | 137 |
| c) «Excursus»: Malta y una posible regulación para la Argentina | 140 |
| 1. Proyecto de ley MDIA (Autoridad de Innovación Digital de Malta) | 140 |
| 2. Acuerdo de Arreglos Tecnológicos y Proveedores de Servicios (TAS) | 140 |
| 3. Proyecto de ley de monedas virtuales (VC) | 141 |
| § 3. «Bitcoins» y lavado de activos | 142 |
| a) Descripción de la maniobra delictiva | 142 |
| 1. BTC como una herramienta para lavar activos de origen criminal | 142 |
| 2. Relato de un caso: Silk Road | 144 |
| b) Observaciones técnicas acerca de la maniobra delictiva | 145 |
| c) Valoración personal | 147 |
| § 4. Reflexiones | 148 |

3. DERECHO PROCESAL PENAL

1

INVESTIGACIÓN CON FUENTES ABIERTAS DE INFORMACIÓN EN EL PROCESO PENAL (OSINT)

MARCOS CANDIOTTO - JUAN ARGIBAY MOLINA

| | |
|--|-----|
| § 1. Introducción | 154 |
| § 2. Aproximación al concepto de la OSINT | 155 |
| § 3. ¿Qué herramientas se utilizan en una investigación con fuentes abiertas? | 159 |
| a) Anonimato | 159 |
| b) Utilización de motores de búsqueda en Internet | 161 |
| c) Búsqueda de personas | 161 |
| d) Búsqueda en el pasado | 162 |
| e) Bases de información («leaks») | 162 |
| f) Resguardar resultados | 162 |
| g) Tablero de control y «software» de análisis de datos | 163 |
| § 4. Entonces, ¿qué es, concretamente, una investigación con fuentes abiertas? | 163 |
| § 5. ¿Qué tensiones plantea una investigación con fuentes abiertas? | 164 |
| § 6. ¿Información o evidencia? | 171 |
| § 7. Conclusión | 175 |

2

AUTOINCRIMINACIÓN Y NUEVAS TECNOLOGÍAS

VÍCTOR HUGO PORTILLO - JUAN MANUEL MATTEO

| | |
|---|-----|
| § 1. Introducción | 178 |
| § 2. Magnitud de la problemática. Algunos casos tomados de la jurisprudencia norteamericana y local | 178 |
| § 3. Breve reflexión sobre el derecho a no autoincriminarse | 180 |
| § 4. El principio de libertad probatoria en el proceso penal | 183 |
| § 5. Autoincriminación y la posibilidad de solicitar al imputado el acceso a un dispositivo cifrado | 186 |
| § 6. Conclusión | 189 |

3

EL ALLANAMIENTO DE DISPOSITIVOS COMO UN NUEVO ALLANAMIENTO DE DOMICILIO EN LA ERA DIGITAL

BRAIAN MATÍAS WERNER

| | |
|--|-----|
| § 1. Introducción. Cada sociedad se regula por su derecho penal | 191 |
| § 2. La necesidad de un cambio de paradigma para el debate jurídico | 193 |
| § 3. Marco legal del domicilio y la garantía que protege su inviolabilidad | 194 |
| a) La inviolabilidad del domicilio | 195 |
| b) El domicilio electrónico | 195 |
| c) Algunos antecedentes jurisprudenciales | 197 |
| § 4. Marco legal del allanamiento | 199 |
| § 5. Cuestiones de competencia. La problemática del «lugar del hecho» | 201 |
| § 6. Cómo debe operar el principio de proporcionalidad | 204 |
| § 7. La problemática con el allanamiento remoto | 205 |

B. FORENSIA DIGITAL

1

BUENAS PRÁCTICAS EN LA EXTRACCIÓN Y TRATAMIENTO DE EVIDENCIA DIGITAL

ANA HAYDÉE DI IORIO - SABRINA LAMPERTI SANTIAGO TRIGO - BRUNO CONSTANZO

| | |
|--|-----|
| § 1. Introducción | 212 |
| § 2. Fases de PURI | 213 |
| § 3. Actividades y tareas de PURI | 214 |
| § 4. Técnicas y herramientas de PURI | 215 |
| § 5. PURI: Detalle de actividades y tareas | 216 |
| § 6. Conclusiones | 222 |

C. DERECHO INFORMÁTICO COMPARADO

1

LOS DELITOS INFORMÁTICOS EN EL SISTEMA PENAL MEXICANO

BENJAMÍN CHONG CASTILLO

| | |
|---|-----|
| § 1. Breve introducción al sistema jurídico penal mexicano | 228 |
| § 2. Legislación mexicana en materia de delitos informáticos | 230 |
| a) Ataque a las vías de comunicación | 231 |
| 1. Sabotaje | 231 |
| I. Acción típica | 231 |
| II. Sujetos de la acción típica | 231 |
| III. Tipicidad subjetiva | 231 |
| 2. Informe ilícito del uso de medios de comunicación | 232 |
| I. Acción típica | 232 |
| II. Sujetos de la acción típica | 232 |
| III. Tipicidad subjetiva | 232 |
| 3. Daño de elementos de vías de comunicación | 232 |
| I. Acción típica | 232 |
| II. Sujetos de la acción típica | 233 |
| III. Tipicidad subjetiva | 233 |
| 4. Resistencia de particulares en materia de vías de comunicación | 233 |
| I. Acción típica | 233 |
| II. Sujetos de la acción típica | 234 |
| III. Tipicidad subjetiva | 234 |
| b) Violación de correspondencia y de la privacidad | 234 |
| 1. Violación de correspondencia | 235 |
| I. Acción típica | 235 |
| II. Sujetos de la acción típica | 235 |
| III. Tipicidad subjetiva | 235 |
| 2. Revelación de secretos | 235 |
| — Acción típica | 236 |
| 3. Acceso ilícito a sistemas y equipos informáticos | 236 |
| I. Acceso ilícito a sistemas y equipos informáticos de particulares | 236 |
| I.1. Acción típica | 236 |
| I.2. Sujetos de la acción típica | 237 |
| I.3. Tipicidad subjetiva | 237 |
| II. Acceso ilícito a sistemas y equipos informáticos del Estado | 237 |
| II.1. Acción típica | 237 |
| II.2. Sujetos de la acción típica | 238 |
| II.3. Tipicidad subjetiva | 238 |

| | |
|--|-----|
| III. Acceso ilícito a sistemas y equipos informáticos del sistema financiero | 238 |
| III.1. Acción típica | 239 |
| III.2. Sujetos de la acción típica | 239 |
| III.3. Tipicidad subjetiva | 239 |
| c) Delitos contra el libre desarrollo de la personalidad | 240 |
| 1. Comunicación de contenido sexual a personas menores de dieciocho años de edad o a personas que no tienen capacidad para comprender el significado del hecho o a personas que no tienen la capacidad para resistirlo | 240 |
| 2. Corrupción de menores | 240 |
| 3. Pornografía Infantil | 241 |
| I. Sujetos de la acción típica | 242 |
| II. Tipicidad subjetiva | 242 |
| d) Delitos en materia de derechos de autor | 242 |
| 1. Acción típica | 242 |
| 2. Sujetos de la acción típica | 242 |
| 4. Tipicidad subjetiva | 242 |
| e) Delitos sobre protección de datos personales | 243 |
| 1. Acción típica | 243 |
| 2. Sujetos de la acción típica | 243 |
| 4. Tipicidad subjetiva | 243 |
| § 3. Evidencia digital | 243 |
| § 4. Conclusiones | 244 |

2

LEGISLACIÓN SOBRE DELITOS INFORMÁTICOS EN ARGENTINA Y PARAGUAY: ESQUEMA COMPARATIVO

MARCELO A. RIQUELT

| | |
|--|-----|
| § 1. Introducción | 247 |
| § 2. Un estándar internacional básico: El Convenio de Budapest | 248 |
| § 3. La normativa sobre cibercriminalidad en la Argentina y Paraguay | 252 |
| a) Infracciones contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos | 252 |
| 1. Acceso ilícito (art. 2°) | 252 |
| 2. Interceptación ilícita (art. 3°) | 254 |
| 3. Atentados contra la integridad de los datos (art. 4°) | 256 |
| 4. Atentados contra la integridad del sistema (art. 5°) | 259 |
| 5. Abuso de equipos e instrumentos técnicos (art.6°) | 260 |
| b) Infracciones informáticas | 263 |
| 1. Falsedad informática (art. 7°) | 263 |
| 2. Estafa informática (art. 8°) | 265 |
| c) Infracciones relativas al contenido | 267 |
| d) Infracciones vinculadas a los atentados a la propiedad intelectual y a los derechos afines | 273 |
| § 4. Colofón | 277 |

D. SELECCIÓN DE JURISPRUDENCIA

1. ANÁLISIS DE FALLOS

EL DENOMINADO «GROOMING»:

UNA NUEVA MODALIDAD DE ACOSO EN LA ERA DIGITAL

HUGO GARCÍA

| | |
|--|-----|
| § 1. El fallo | 283 |
| § 2. Aspectos relevantes de la decisión judicial y el delito de «grooming» | 284 |
| a) Antecedentes o genealogía del tipo penal | 284 |
| b) Definición de «grooming» | 285 |
| c) Características | 286 |
| d) El elemento subjetivo del tipo y su aplicación al fallo en análisis | 287 |
| § 3. Conclusiones | 289 |

2. FALLOS SELECCIONADOS

I. JURISPRUDENCIA NACIONAL

| | |
|---|-----|
| A. Sumarios | 293 |
| 1. Defraudación informática (art. 173, inc. 16, CP) | 293 |
| 2. Delitos cometidos contra base de datos personales (art.157 bis, inc.1°,CP) | 293 |
| B. Fallos «in extenso» | 294 |
| 1. TCPBA. Sala I, 14/3/19, «Luna, Jonatan o Luna, Yonatan Omar s/Recurso de casación», causa n° 87.583, reg. N° 262 | 294 |
| 2. Juzgado de Control y Faltas, Córdoba, 9/4/19, «Cipolla Sánchez, Mariano Hernán | 294 |
| p.s.a Infracción a la ley 10.326 (Código de Convivencia Ciudadana)», expte. SAC Penal n° 7.940.775 | 308 |

II. JURISPRUDENCIA EXTRANJERA

| | |
|---|-----|
| A. Estados Unidos de América | 322 |
| — Prueba digital. Medidas de coerción. Derecho a la privacidad. Expectativa de privacidad. Obtención de evidencia digital. Secuestro de información de teléfonos celulares o terminales móviles | 322 |
| — Prueba digital e inteligencia artificial: Determinación de la pena mediante programas autónomos basados en inteligencia artificial. Determinación de grado de reincidencia mediante inteligencia artificial | 324 |
| B. Unión Europea | 325 |
| — Datos abiertos o de acceso público. Datos restringidos. Datos de contacto. Datos de tráfico. Datos de contenido. IP dinámica. Expectativa de privacidad. Orden judicial | 325 |
| — Prueba digital. Pornografía infantil. Inspección del disco rígido de una PC. Reparación de ordenador(PC, Notebook, Netbook, Ultrabook). Expectativa de privacidad. Debido proceso. Orden judicial | 326 |

E. COMENTARIOS BIBLIOGRÁFICOS

1

DERECHO PENAL CIBERNÉTICO. LA CIBERCRIMINALIDAD Y EL DERECHO PENAL EN LA MODERNA SOCIEDAD DE LA INFORMACIÓN Y LA TECNOLOGÍA DE LA COMUNICACIÓN

GUSTAVO E. ABOSO

331

333

2
DELITOS CONTRA LA INTIMIDAD INFORMÁTICA
PABLO ANDRÉS PALAZZI

BIBLIOGRAFÍA GENERAL
PAUTAS EDITORIALES

335
345