



MARCELO A. RIQUERT dirección
CARLOS CHRISTIAN SUEIRO coordinación

Sistema penal e informática

CIBERDELITOS. EVIDENCIA DIGITAL. TICS

1

A 10 AÑOS DE LA LEY DE DELITOS INFORMÁTICOS. «FAKE NEWS»: CIBERCRIMINALIDAD Y LIBERTAD DE EXPRESIÓN. RESPONSABILIDAD PENAL DE LOS PROVEEDORES DE SERVICIO DE INTERNET. EL CIBERATAQUE «WANNACRY». EL «SEXTING». LA TUTELA DE LA INTEGRIDAD Y DISPONIBILIDAD DE LOS DATOS. LOS DERECHOS HUMANOS Y LAS TICS. LA NUEVA LEY DE LA NUBE «CLOUD ACT». EL TRATAMIENTO DE LA EVIDENCIA DIGITAL EN LOS PROCESOS PENALES. DERECHO INFORMÁTICO COMPARADO

autores **GUSTAVO E. ABOSO - FRANCISCO ALMENAR PINEDA - NORA A. CHERŃAVSKY
BRUNO CONSTANZO - NORBERTO DE LA MATA BARRANCO - JAVIER A. DE LUCA
ANA H. DI IORIO - DANIELA DUPUY - EDUARDO FERREYRA - SABRINA LAMPERTI
YAMILA Y. LUZZA - MARIANA KIEFER - DIÓGENES A. MOREIRA
PABLO H. LUIS MUNIAGURRIA - VICTOR H. PÒRTILLO - SPENCER TOTH SYDOW
FELIPE VILLAVICENCIO TERREROS**

CORTE SUPREMA BIBLIOTECA	
SIG. TOPOGRAFICA Q844	INVENTARIO 1433-18

**FORENSIA
DIGITAL**

h
hammurabi
JOSE LUIS DEPALMA EDITOR

ÍNDICE GENERAL

PRESENTACIÓN	9
ABREVIATURAS	21

A. DOCTRINA

1. DERECHO PENAL. PARTE GENERAL

1

LA TUTELA DE LA INTEGRIDAD Y DISPONIBILIDAD DE DATOS Y SISTEMAS INFORMÁTICOS: EL MODELO TRADICIONAL VINCULADO A UNA PROTECCIÓN ESTRICTAMENTE PATRIMONIAL, UN MAL REFERENTE

NORBERTO J. DE LA MATA BARRANCO

§ 1. Introducción	29
§ 2. Referentes legales internacionales y de derecho comparado	30
§ 3. Los ataques a datos y sistemas en el contexto de los delitos de daños	34
§ 4. Los ataques a datos y sistemas como delitos contra su integridad y disponibilidad	36
§ 5. Los datos y sistemas: el objeto de ataque de las conductas punibles	38
§ 6. El interés a tutelar	40
§ 7. El denominado delito de interferencia ilegal en datos	43
§ 8. El delito de interferencia ilegal en sistemas de información	48
§ 9. Reflexión final	49

2

«FAKE NEWS»: CIBERCRIMINALIDAD Y LIBERTAD DE EXPRESIÓN EN INTERNET

JAVIER AUGUSTO DE LUCA - YAMILA YAEL LUZZA

§ 1. Introducción	51
-------------------------	----

§ 2. Noticias falsas a través de los servidores de Internet	52
a) ¿Qué son las «fake news» y cómo detectarlas?	52
b) Noticias falsas, guerrilla comunicacional y democracia	53
§ 3. Control estatal: sobre la necesidad o no de intervención del derecho penal. Algunos estándares en el derecho internacional	55
§ 4. Responsabilidad de los intermediarios por los contenidos	63
§ 5. Conclusiones	70

3

RESPONSABILIDAD PENAL DE LOS PROVEEDORES DEL SERVICIO EN INTERNET

GUSTAVO EDUARDO ABOSO

§ 1. Introducción	73
§ 2. La autodeterminación informativa y el derecho «al olvido» en Internet	74
§ 3. La responsabilidad de los proveedores de servicio en la sociedad de la información a través de la jurisprudencia	78
a) «Cubby Inc. v. CompuServe Inc.» (1991)	80
b) «Zeran v. America Online Inc.» (1997)	80
c) Caso «CompuServer Deutschland» (1998)	83
d) Críticas al fallo del AG München en el caso «CompuServer Deutschland»	86
e) «United States v. Thomas»	88
§ 4. Creación de un «link» o enlace para la comisión de delitos	89
§ 5. Las leyes 25.690, 26.032 y 27.078	90
§ 6. La responsabilidad de los proveedores intermediarios de servicios en la jurisprudencia argentina	91
§ 7. La responsabilidad de los proveedores intermediarios de servicios en la jurisprudencia comunitaria: Google Spain, S.L. y Google Inc. / Agencia Española de Protección de Datos (AEPD) y Mario Costeja González (2014)	93
§ 8. Aplicación de las reglas de participación criminal a los proveedores de servicio de Internet	96
§ 9. El conocimiento fehaciente como presupuesto normativo de responsabilidad	106
§ 10. Responsabilidad de los establecimientos comerciales que brindan servicio de Internet	108
§ 11. Valoración final	109

4

UNA VISIÓN DESDE LOS DERECHOS HUMANOS SOBRE LAS TECNOLOGÍAS DE VIGILANCIA E INVESTIGACIÓN

EDUARDO FERREYRA

§ 1. Introducción	113
§ 2. Sistema universal de derechos humanos	115
§ 3. Sistema interamericano de derechos humanos	116

§ 4. El hackeo estatal	121
§ 5. Acceso transfronterizo de datos	124
§ 6. Conclusión	126

2. DERECHO PENAL. PARTE ESPECIAL

1

A DIEZ AÑOS DE LA LEY DE DELITOS INFORMÁTICOS.

BALANCE Y PROPUESTAS

NORA A. CHERÑAVSKY - PABLO H. GRIS MUNIAGURRIA

DIÓGENES A. MOREIRA

§ 1. Introducción	129
§ 2. La ley 26.388. Definiciones. Generalidades. Nuevos bienes tutelados	132
§ 3. La ley 26.388 y la adaptación de los tipos tradicionales. Evolución legislativa y jurisprudencial en diez años de su vigencia	135
a) Art. 128, CP: pornografía infantil por Internet	135
b) Art. 153, CP: violación de correspondencia digital. Secreto y privacidad de las comunicaciones	136
c) Art. 153 «bis», CP: acceso ilegítimo a datos o a un sistema informático	140
d) Art. 155, CP: difusión del contenido de una comunicación electrónica	141
e) Art. 157, CP: revelación de datos	144
f) Art. 157 «bis», CP: acceso ilegítimo, difusión o alteración de bases de datos personales	145
g) Art. 173, inc. 16, CP: estafa o fraude informático	146
h) Arts. 183 y 184, CP: daño informático	148
i) Art. 197, CP: interrupción o entorpecimiento de comunicaciones privadas o públicas	149
j) Art. 255, CP: sustracción / destrucción de medios de prueba	150
§ 4. Otros delitos informáticos previstos en leyes especiales	151
§ 5. Incriminación posterior a la sanción de la ley 26.388: el «grooming»	151
§ 6. Delitos tradicionales cometidos por medios informáticos	152
§ 7. Nuevos fenómenos delictivos y necesidad de nuevas incriminaciones	153
a) El robo de identidad digital	153
b) El «sexting»	154
c) «Revenge porn» o pornovenganza	154
§ 8. Reflexiones finales sobre el entorno virtual y la cooperación internacional. Conclusiones	156

2

**ALGUNAS CONSIDERACIONES SOBRE EL «SEXTING»
EN EL DERECHO PENAL ARGENTINO**

VÍCTOR HUGO PORTILLO

§ 1. Introducción	161
-------------------------	-----

§ 2. Concepto y magnitud del «sexting»	162
a) Concepto	162
b) Magnitud del fenómeno	163
§ 3. Marco regulatorio del «sexting» en el derecho penal argentino y el derecho comparado	164
a) El «sexting» en el derecho penal argentino	164
b) El «sexting» en el derecho penal español	167
§ 4. Análisis de casos judicializados sobre «sexting»	168
a) Caso «H.A. v. State of Florida», 2007	168
b) «Miller v. Skumanick»	169
§ 5. Análisis final	170
§ 6. Conclusión	171

3

EL CIBERATAQUE «WANNACRY» COMO MODALIDAD DE DELINCUENCIA INFORMÁTICA

FRANCISCO ALMENAR PINEDA

§ 1. Introducción	173
§ 2. Breve referencia a la evolución histórica de los delitos de «hacking»	175
a) Introducción	175
b) Concepto y rasgos de la delincuencia informática	176
c) Evolución normativa supranacional	177
§ 3. Concepto del delito de «hacking» y del denominado «WannaCry»	179
a) Concepto del delito de «hacking»	179
b) Concepto de «WannaCry»	180
§ 4. El tratamiento del «hacking» en el ordenamiento penal español	181
a) La situación antes de la reforma de 2010	181
b) La reforma de 2010	183
c) La reforma de 2015	184
§ 5. «WannaCry» en relación con el bien jurídico protegido y objeto material en el delito de «hacking»	185
a) Introducción	185
b) «WannaCry» como delito contra la intimidad	186
c) El objeto material afectado por «WannaCry»	189
§ 6. Naturaleza jurídica de «WannaCry»	191
§ 7. «WannaCry» en el art. 197 «bis», 1 del CP	194
a) Sujeto activo y pasivo	194
b) La conducta típica	195
c) La relevancia penal de las conductas de facilitar «WannaCry»	198
d) La conducta de mantenimiento en el sistema	199
e) Aspecto subjetivo	200
f) Formas de aparición	200

§ 8. Las relaciones concursales derivadas de «WannaCry»	205
§ 9. «WannaCry» como conducta cometida en el seno de organización o grupo criminal	208
§ 10. Conclusiones	211

3. DERECHO PROCESAL PENAL

1

LA NUEVA LEY «CLOUD ACT». SU IMPACTO EN INVESTIGACIONES EN ENTORNOS DIGITALES

DANIELA DUPUY - MARIANA KIEFER

§ 1. Planteamiento del problema	219
§ 2. Acuerdos de Asistencia Legal Mutua «MLAT»	222
§ 3. Contexto legal en Estados Unidos: Ley de Privacidad de Comunicaciones Electrónicas y Ley de Comunicaciones Almacenadas	224
§ 4. El caso «Microsoft/Ireland» como precedente de la «Cloud Act»	226
§ 5. Una respuesta legislativa: la «Cloud Act»	231
§ 6. Críticas versus respaldos a la «Cloud Act»	235
§ 7. Conclusión	236

B. FORENSIA DIGITAL

1

EL TRATAMIENTO DE LA EVIDENCIA DIGITAL EN LOS PROCESOS PENALES

BRUNO CONSTANZO - SABRINA LAMPERTI

ANA HAYDÉE DI IORIO

§ 1. Introducción	239
§ 2. La evidencia digital en la legislación argentina	240
a) Contexto general	240
b) Evolución normativa	242
1. Provincia de Neuquén	243
2. Provincia de Río Negro	244
3. Provincia de Buenos Aires	246
4. Procuración General de la Nación. Ministerio Público Fiscal	254
5. Provincia de Corrientes	255
6. Provincia de Salta	255
7. Ministerio de Seguridad de la Nación	256
8. Ministerio de Justicia y DDHH de la Nación. Consejo de procuradores, fiscales, defensores y asesores generales de la República Argentina. Consejo Federal de Política Criminal	257

§ 3. Aspectos a considerar desde la perspectiva técnica informática	258
a) Evidencia digital en Internet	258
b) Evidencia digital en memoria principal o memoria volátil	260
c) Evidencia digital en memoria persistente o disco	261
d) Evidencia digital en dispositivos móviles	262
§ 4. Conclusiones	263

C. DERECHO INFORMÁTICO COMPARADO

1

LOS DELITOS INFORMÁTICOS EN LA LEGISLACIÓN PENAL PERUANA

FELIPE VILLAVICENCIO TERREROS

§ 1. Alcances generales	267
a) Introducción	267
b) Concepto y modalidades	269
c) Bien jurídico tutelado	270
d) El perfil del ciberdelincuente	271
e) Las personas jurídicas como sujeto activo y sujeto pasivo	273
§ 2. La Ley de Delitos Informáticos en la legislación penal peruana	274
a) Antecedente de los delitos informáticos	274
b) La ley 30.096	275
1. Objetivo y finalidad de la ley	275
2. Modalidades típicas previstas en la ley	276
3. Circunstancias modificativas de responsabilidad	282
4. Exención de responsabilidad	283

2

EL IMPACTO DE LA INFORMÁTICA EN EL SISTEMA JURÍDICO PENAL BRASILEÑO

SPENCER TOTH SYDOW

§ 1. Introducción	285
§ 2. Derecho y tecnología	285
§ 3. «Malum prohibitum» y «malum in se»	286
§ 4. El sistema jurídico brasileño en la era de la virtualidad	287
§ 5. Dificultades modernas	294
§ 6. Conclusiones	295

D. SELECCIÓN DE JURISPRUDENCIA

I. «Grooming» (art. 131, CP)	299
------------------------------------	-----

1. Acción típica de «Grooming». Contacto telemático o a través de sistemas de transmisión de información	299
2. Competencia de la Justicia en lo Penal Contravencional y de Faltas de la Ciudad de Buenos Aires	299
II. Pornografía infantil (art. 128, CP)	299
1. Rechazo de la suspensión de proceso a prueba en casos de difusión o comercialización de pornografía infantil	299
2. Competencia de la Justicia en lo Penal, Contravencional y de Faltas de la Ciudad de Buenos Aires, respecto de distribución de pornografía infantil	300
3. Jurisdicción y competencia provincial si la conexión a Internet para distribuir pornografía infantil se realizó desde el territorio de una provincia	300
III. Delitos cometidos contra base de datos personales (art. 157 «bis», CP)	300
— Competencia del fuero federal en caso de violación de base de datos personales	300
IV. Defraudación informática (art. 173, inc. 16, CP)	300
— Adecuación típica de la conducta a la figura de defraudación informática. Técnicas de manipulación del sistema	300
V. Daño informático (art. 183, CP)	301
— Competencia de la Justicia Nacional en el supuesto de códigos maliciosos o accesos remotos que causen daño en sitios de una empresa extranjera	301
VI. Daño informático agravado (art. 184, CP)	301
— Prueba digital. Peritaje en un daño informático agravado	301

E. COMENTARIOS BIBLIOGRÁFICOS

1

**NUEVOS DESAFÍOS DE LA EVIDENCIA DIGITAL:
ACCESO TRANSFRONTERIZO Y TÉCNICAS DE ACCESO REMOTO
A DATOS INFORMÁTICOS**

MARCOS SALT	305
-------------------	-----

2

**DELITOS INFORMÁTICOS. INVESTIGACIÓN CRIMINAL,
MARCO LEGAL Y PERITAJE**

GUSTAVO SAIN - HORACIO AZZOLIN	307
--------------------------------------	-----

BIBLIOGRAFÍA GENERAL	309
PAUTAS EDITORIALES	319

MARCELO A. RIQUERT dirección
CARLOS CHRISTIAN SUEIRO coordinación

Sistema penal e informática

CIBERDELITOS. EVIDENCIA DIGITAL. TICS

2

NEURODERECHOS Y CRIMINALIDAD INFOMÁTICA («HACKEO» MENTAL).
DISEÑO DE POLÍTICA PÚBLICA EN CIBERCRIMEN. REGULACIÓN PENAL EN MATERIA
DE GÉNERO EN EL ÁMBITO TECNOLÓGICO. «PHISHING». EL USO DE «BITCOINS»
PARA LAVAR ACTIVOS. INVESTIGACIÓN EN FUENTES ABIERTAS EN EL PROCESO
PENAL (OSINT). AUTOINCRIMINACIÓN Y NUEVAS TECNOLOGÍAS. ALLANAMIENTO
DE DISPOSITIVOS. BUENAS PRÁCTICAS EN EXTRACCIÓN DE EVIDENCIA DIGITAL.
DELITOS INFORMÁTICOS EN EL DERECHO COMPARADO

autores **JUAN ARGIBAY MOLINA - MARCOS CANDIOTTO**
BENJAMÍN CHONG CASTILLO - NORA A. CHERÑAVSKY - BRUNO CONSTANZO
ANA HAYDÉE DI IORIO - HUGO GARCÍA - PABLO H. GRIS MUNIAGURRIA
SABRINA LAMPERTI - MARÍA BELÉN LINARES - PAZ LLORIA GARCÍA
JUAN MANUEL MATTEO - DIÓGENES A. MOREIRA - VÍCTOR HUGO PORTILLO
MARCELO A. RIQUERT - GUSTAVO SAIN - CARLOS CHRISTIAN SUEIRO
SANTIAGO TRIGO - BRAIAN MATÍAS WERNER

**FORENSIA
DIGITAL**

h
hammurabi
JOSE LUIS DEPALMA EDITOR

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 y 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 GENERO 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 inconsentida 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. CHERŃAVSKY
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. RIQUERT

§ 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 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

2**DELITOS CONTRA LA INTIMIDAD INFORMÁTICA**

PABLO ANDRÉS PALAZZI

..... 333

BIBLIOGRAFÍA GENERAL

335 ✓

PAUTAS EDITORIALES

345



MARCELO A. RIQUERT dirección
CARLOS CHRISTIAN SUEIRO coordinación

Sistema penal e informática

CIBERDELITOS. EVIDENCIA DIGITAL. TICS

3

ALGORITMOS INTELIGENTES AL SERVICIO DEL DERECHO. LA INTELIGENCIA ARTIFICIAL EN LA CONDUCCIÓN VEHICULAR. INGENIERÍA SOCIAL: RESPONSABILIDAD CIVIL Y PENAL. TECNOLOGÍAS DE RECONOCIMIENTO FACIAL COMO HERRAMIENTAS CONTRA EL DELITO. AGENTE ENCUBIERTO INFORMÁTICO. PREVENCIÓN DEL «FORUM SHOPPING» MEDIANTE TIC. SERVICIOS INFORMÁTICOS FORENSES. DELITOS: INFORMÁTICOS FINANCIEROS; DE «CHILD GROOMING»; DE «PORNOVENGANZA»; DE ACCESO AL CORREO DE VÍCTIMAS DE VIOLENCIA DE GÉNERO

autores **GUSTAVO EDUARDO ABOSO - CARLOS ALBERTO CEREZOLI
BENJAMÍN CHONG CASTILLO - PABLO CISTOLDI - BRUNO CONSTANZO
ANA HAYDÉE DI IORIO - EDUARDO FERREYRA - MARÍA DE LOS MILAGROS FRANCO
MIGUEL MAXIMILIANO GALIANA - ESTEFANÍA GASPARINI NEVES - NICOLÁS GRANDI
HORACIO ROBERTO GRANERO - MAXIMILIANO MACEDO - MARCELO A. RIQUERT
CARLOS CHRISTIAN SUEIRO - MARCELO TEMPERINI - SANTIAGO TRIGO
DIEGO ALONSO VERGARA VACAREZZA - BRAIAN MATÍAS WERNER**

**FORENSIA
DIGITAL**

hammurabi

JOSE LUIS DEPALMA EDITOR

ÍNDICE GENERAL

ABREVIATURAS	19
--------------------	----

A. DOCTRINA

1. DERECHO PENAL. PARTE GENERAL

1

LA INTELIGENCIA ARTIFICIAL APLICADA AL DERECHO Y EL DILEMA DE LOS ALGORITMOS INTELIGENTES

HORACIO ROBERTO GRANERO

§ 1. El derecho, la técnica y el caos	27
§ 2. La técnica al servicio del abogado	29
a) Un poco de historia	29
b) La búsqueda de soluciones en la tecnología	30
1. Los sistemas expertos: una solución solo parcial para casos puntuales	30
2. ¿La inteligencia artificial: hacia un nuevo concepto de verdad jurídica?	32
§ 3. El concepto de entropía y su utilización como herramienta al servicio del derecho ..	34
§ 4. Un modelo de Inteligencia Artificial desarrollado sobre la base del Código de Ham- murabi	37
§ 5. Sherlock-Legal	38
§ 6. Un futuro de participación entre humanos y algoritmos inteligentes. Su aplicación en el derecho penal	39
§ 7. Conclusión: ¿puede la tecnología ayudar realmente al hombre de derecho?	43

2**LOS DILEMAS ACTUALES DE LA INTELIGENCIA ARTIFICIAL
EN EL CAMPO DE LA CONDUCCIÓN VEHICULAR**

NICOLÁS GRANDI

§ 1. Introducción	48
§ 2. Dilema de control	49
§ 3. Algoritmo de choque	53
§ 4. Conclusión	64

3**ASPECTOS LEGALES DE LA INGENIERÍA SOCIAL:
ANÁLISIS SOBRE LA RESPONSABILIDAD CIVIL
Y PENAL DEL INGENIERO SOCIAL**

MARCELO TEMPERINI - MAXIMILIANO MACEDO

§ 1. Introducción	68
§ 2. La ingeniería social: definiciones	69
— Descripción propia	70
§ 3. Ingeniería social desde la seguridad de la información	70
a) Ataques de ingeniería social que afectan la disponibilidad	71
b) Ataques de ingeniería social que afectan la integridad	71
c) Ataques de ingeniería social que afectan la confidencialidad	71
d) Objetivos	71
e) Metodología y técnicas	72
f) Medios de ataque	73
§ 4. ¿Hay o no contrato? Esa es la cuestión	74
§ 5. Responsabilidad penal	75
a) Estafa o defraudación	76
b) Suplantación de identidad digital	77
c) Acceso indebido a sistemas o datos informáticos	78
d) Acceso ilegítimo a bancos de datos personales	80
e) Acceso indebido a datos confidenciales	82
§ 6. Responsabilidad civil	83
— Confidencialidad de la información	84
§ 7. Claves para realizar un contrato de ingeniería social	86
a) Consentimiento por escrito	87
b) ¿Quién aprueba? Personas que aprueban la contratación del servicio	87
c) Definición de objetivos	87
d) Locaciones	88
e) Inteligencia	88
f) Ventana temporal	88
g) Identidades a utilizar	88
h) Aprobación de ataques	89
i) Filtros y alertas	89

ÍNDICE GENERAL

11

j) Causas de cancelación	89
k) Prohibiciones	89
l) Autorización: carta blanca	90
§ 8. Conclusiones	90

2. DERECHO PENAL. PARTE ESPECIAL

1

EL DELITO DE «CHILD GROOMING» Y SU IMPACTO EN EL ORDENAMIENTO JURÍDICO ARGENTINO

MIGUEL MAXIMILIANO GALLIANA

§ 1. Introducción	94
§ 2. Impacto en nuestro derecho interno	96
§ 3. Análisis dogmático de la figura	98
§ 4. Propuestas legislativas	105

3. DERECHO PROCESAL PENAL

1

UN ACERCAMIENTO AL RECONOCIMIENTO FACIAL COMO MEDIO DE PRUEBA EN EL PROCESO PENAL

BRAIAN MATÍAS WERNER

§ 1. Introducción a la problemática	112
§ 2. Cuestiones relativas a la protección de datos personales	114
§ 3. El posible uso del reconocimiento facial como elemento de prueba en el proceso penal	117
§ 4. Medios de investigación y medios de prueba	119

2

EL OJO BLINDADO. UNA PERSPECTIVA DE DERECHOS FUNDAMENTALES SOBRE EL USO DE TECNOLOGÍA DE RECONOCIMIENTO FACIAL POR PARTE DE FUERZAS DE SEGURIDAD

EDUARDO FERREYRA

§ 1. Introducción	128
§ 2. Tres maneras de enfocar el problema	129
§ 3. Aspectos sustanciales	130
§ 4. Aspectos formales	133
§ 5. Aspectos procedimentales	135
§ 6. Conclusión	137

3**ESTUDIO DEL AGENTE ENCUBIERTO INFORMÁTICO
COMO ESPECIAL TÉCNICA DE INVESTIGACIÓN
DEL ORDENAMIENTO JURÍDICO DE ESPAÑA**

CARLOS ALBERTO CEREZOLI

§ 1. Introducción	139
§ 2. Consideraciones sobre la criminalidad organizada como fenómeno que preocupa a la comunidad internacional	140
§ 3. Consideraciones generales sobre el agente encubierto y el agente encubierto informático	143
§ 4. El agente encubierto y el agente encubierto informático en la Ley de Enjuiciamiento Criminal	149
§ 5. A modo de conclusión	159

4**EL AGENTE ENCUBIERTO INFORMÁTICO
EN LA REPÚBLICA ARGENTINA**

ESTEFANÍA GASPARINI NEVES

§ 1. Introducción	163
§ 2. La incorporación del agente encubierto como técnica legislativa de investigación ..	171
§ 3. Acerca de la necesidad de actualizar la figura del agente encubierto en la República Argentina	173

5**EL RECONOCIMIENTO FACIAL COMO HERRAMIENTA
CONTRA EL DELITO. ALGUNAS EXPERIENCIAS
Y CONTROVERSIAS EN EL MUNDO**

DIEGO ALONSO VERGARA VACAREZZA

§ 1. Reconocimiento facial	180
§ 2. Experiencias en algunos lugares del mundo	180
a) Los márgenes de error	183
b) ¿Cómo funcionan los programas de reconocimiento facial?	185
§ 3. «El futuro llegó, hace rato»	186
§ 4. Conclusiones	188

6**PREVENCIÓN DEL «FORUM SHOPPING»
MEDIANTE TECNOLOGÍAS DE LA INFORMACIÓN
Y LA COMUNICACIÓN (TIC)**

MARÍA DE LOS MILAGROS FRANCO

§ 1. Presentación del tema	192
----------------------------------	-----

ÍNDICE GENERAL

13

§ 2.	Estado actual de la situación	193
a)	Lo que sucede hoy en la justicia penal en Capital Federal	193
b)	El problema	193
c)	¿Qué dispone el nuevo Código Procesal Penal Federal (CPPF) al respecto?	195
d)	Propuesta de mejora	195
§ 3.	Estudio de factibilidad realizado para la mejora	197
a)	Análisis de factibilidad	198
b)	Implementación	199
1.	Capacitación	199
2.	Mantenimiento del sistema	199
3.	Control	199
4.	Obstáculos	199
5.	Ventajas	199
§ 4.	Diagramas de flujo del proceso penal actual y del proceso penal con la propuesta de mejora	200
a)	Diagrama de flujo del proceso de denuncia actual	200
b)	Diagrama de flujo del proceso con la propuesta de mejora	201
§ 5.	Conclusión	202

B. FORENSIA DIGITAL

1

LABORATORIOS DE INFORMÁTICA FORENSE.

SERVICIOS, INFRAESTRUCTURA

Y ASPECTOS TÉCNICOS

ANA HAYDÉE DI IORIO - SANTIAGO TRIGO

BRUNO CONSTANZO - PABLO CISTOLDI

§ 1.	Introducción	206
§ 2.	Servicios informáticos forenses	207
a)	Contexto general	207
b)	Planificación estratégica, organización y gestión	208
c)	Servicios periciales	213
1.	Servicios del rol o función de asesoramiento	215
2.	Servicios del rol o función de investigación	215
3.	Servicios del rol o función pericial	216
4.	Otros servicios vinculados	219
§ 3.	Infraestructura tecnológica	219
a)	Equipos de computación	219
b)	Infraestructura de red	223
§ 4.	Infraestructura edilicia	223
§ 5.	Conclusiones	226

C. DERECHO INFORMÁTICO COMPARADO

1

DELITOS INFORMÁTICOS FINANCIEROS EN MÉXICO

BENJAMÍN CHONG CASTILLO

§ 1. Breve introducción a los delitos informáticos en materia financiera	232
§ 2. Delitos informáticos especiales en materia financiera	234
a) Falsificación	235
1. Falsificación sobre medios de tecnología financiera	235
I. Acción típica	235
II. Sujetos de la acción típica	236
III. Tipicidad subjetiva	236
2. Uso de aparatos tecnológicos con fines de falsificación	236
I. Acción típica	237
II. Sujetos de la acción típica	237
3. Falsificación de estados financieros	237
I. Acción típica	238
II. Sujetos de la acción típica	238
b) Acceso ilícito a sistemas y equipos informáticos en materia financiera	238
1. Acceso ilícito a sistemas y equipos informáticos del sistema bancario mexicano	238
I. Acción típica	239
II. Sujetos de la acción típica	239
2. Acceso ilícito a sistemas sobre el mercado de valores	239
I. Acción típica	240
II. Sujetos de la acción típica	240
3. Acceso ilícito al sistema sobre instituciones de tecnología financiera	240
I. Acción típica	240
II. Sujetos de la acción típica	240
c) Suplantación de identidad	240
1. Suplantación de identidad sobre instituciones de crédito	241
I. Acción típica	241
II. Sujetos de la acción típica	241
2. Suplantación de identidad sobre instituciones de tecnología financiera	241
I. Acción típica	241
II. Sujetos de la acción típica	242
d) Daño informático	242
1. Daño informático contra la supervisión	243
I. Acción típica	243
II. Sujetos de la acción típica	244
2. Daño informático para la manipulación	244
I. Acción típica	244
II. Sujetos de la acción típica	245

e) Delitos para la protección del patrimonio en el ecosistema «fintech»	245
1. Disposición indebida de recursos sobre tecnología financiera	245
I. Acción típica	245
II. Sujetos de la acción típica	246
2. Desvío de recursos sobre tecnología financiera	246
I. Acción típica	246
II. Sujetos de la acción típica	247
3. Uso indebido de activos virtuales	248
I. Acción típica	248
II. Sujetos de la acción típica	248
§ 3. Breve introducción a los delitos informáticos en materia financiera	248

D. SELECCIÓN DE JURISPRUDENCIA

1. ANÁLISIS DE FALLOS

1

EL RESGUARDO DE LA INTIMIDAD EN LA SOCIEDAD DE LA INFORMACIÓN Y EL DELITO DE «PORNOVENGANZA» («SEXTING» O «NON-CONSENSUAL PORNOGRAPHY»)

GUSTAVO EDUARDO ABOSO

§ 1. Introducción	255
§ 2. Análisis de la sentencia del 24 de febrero de 2020 dictada por el Tribunal Supremo español	260
§ 3. El delito de «pornovenganza» en el Código Penal español	261
§ 4. El delito de «pornovenganza» en la legislación comparada	263
a) Filipinas	263
b) Alemania	264
c) Francia	266
d) Estados Unidos de América	267
e) Reino Unido y Norte de Irlanda	268
f) Italia	268
g) Australia	269
h) Canadá	269
i) Nueva Zelanda	269
§ 5. La «pornovenganza» en la legislación nacional	270
§ 6. La libertad de expresión y la protección de la intimidad	273
§ 7. Responsabilidad penal de los titulares de los medios de difusión	275
§ 8. Distinción de la «pornovenganza» del «sexting», «grooming», distribución de pornografía infantil y «cybermobbing»	278
§ 9. Lineamientos para una futura reforma penal	281
§ 10. Epílogo	285

2**VIOLENCIA DE GÉNERO Y ACCESO ILEGAL
AL CORREO ELECTRÓNICO DE LA VÍCTIMA**

GUSTAVO EDUARDO ABOSO

§ 1. Introducción	289
§ 2. Los hechos	290
§ 3. La sentencia del TEDH en materia de violencia de género, en especial respecto del acceso ilegal al servicio de mensajería de la víctima	291
§ 4. El acceso ilegal al sistema de mensajería electrónica de la víctima como reflejo de la dominación del excónyuge	293
§ 5. Los mensajes y archivos de audio como prueba directa de la existencia de violencia de género	295
§ 6. El acceso ilegal en el contexto de procesos de divorcio y despidos laborales	297
a) El acceso ilegal en los casos de divorcios	297
b) El acceso ilegal en los casos de despidos laborales	298
§ 7. Palabras finales	300

2. FALLOS SELECCIONADOS**I. JURISPRUDENCIA NACIONAL**

A. Sumarios	303
1. Pornografía infantil	303
2. Defraudación informática (art. 176, inc. 16)	304
3. «Grooming» (art. 131, CP)	304

II. JURISPRUDENCIA EXTRANJERA

A. Estados Unidos de América	305
— Prueba digital. Datos biométricos. Desbloqueo compulsivo de teléfono celular inteligente. Derecho a la privacidad. Prohibición de autoincriminación	305
B. Holanda o Países Bajos	308
— Inteligencia artificial. Sesgos algorítmicos. Transparencia algorítmica. Derecho a la privacidad o intimidad. Derecho de defensa en juicio. Derecho a no ser discriminado. Vigilancia omnipresente irrestricta de la ciudadanía	308

E. COMENTARIOS BIBLIOGRÁFICOS**1****VIOLENCIA CONTRA LA MUJER
EN LA ERA DEL CIBERESPACIO**

MARCELO A. RIQUERT

313

ÍNDICE GENERAL	17
2	
DERECHO PENAL: PARTE GENERAL. PARTE ESPECIAL.	
LIBRO AUDIOVISUAL	
MARCO ANTONIO TERRAGNI	
-----	315
3	
NEUROCIENCIAS Y DERECHO (VOL. 1)	
DANIEL PASTOR - MARÍA ROCA	
LAURA DEANESI - MARTÍN D. HAISSINER	
-----	317
4	
DERECHO Y TECNOLOGÍA (VOL. 1)	
CARLOS J. ORDOÑEZ	
-----	319
5	
NEUROCIENCIAS, TECNOLOGÍAS DISRUPTIVAS	
Y TRIBUNALES DIGITALES	
MARTÍN D. HAISSINER - DANIEL R. PASTOR	
-----	321
BIBLIOGRAFÍA GENERAL -----	323
PAUTAS EDITORIALES -----	331



MARCELO A. RIQUERT dirección
CARLOS CHRISTIAN SUEIRO coordinación

Sistema penal e informática

CIBERDELITOS. EVIDENCIA DIGITAL. TICS

CORTE SUPREMA BIBLIOTECA	
SIG TOPOGRAFICA Q919	INVENTARIO 153.673

4

CIBERSEGURIDAD. «FAKE NEWS». PROGRAMACIÓN ÉTICA.
INTRUSISMO INFORMÁTICO. SUSTITUCIÓN DE IDENTIDAD. ACOSO LABORAL
Y LAS NUEVAS TECNOLOGÍAS. LAVADO DE ACTIVOS Y CRIPTOMONEDAS. DELITOS
CONTRA LA COMPETENCIA. FRAUDES, SABOTAJE Y EXTORSIÓN «ONLINE».
PERICIA INFORMÁTICA. LIBERTAD DE EXPRESIÓN Y DISCURSO DE ODIOS.
SISTEMAS DE RECONOCIMIENTO FACIAL. DERECHO A LA INTIMIDAD.
VIGILANCIA ELECTRÓNICA

autores **HENRIQUE ABI-ACKEL TORRES - GUSTAVO E. ABOSO - URIEL BEKERMAN
MATEO BRODSKY - JUAN E. CARRIÓN DÍAZ - PABLO CISTOLDI - JUAN E. DIAK
ANA DI IORIO - PATRICIA GALLO - SANTIAGO GAMARRA CALELLO
ALANA GUIMARÃES MENDES - NICOLÁS M. GRANDI - SABRINA LAMPERTI
PAZ LLORIA GARCÍA - SABRINA N. MAÑAS - NOELIA V. MITELLI - JUAN MOLINAS
JULIANA OLIVEIRA DOMINGUES - MAGDALENA ORLOFF - MARIANA M. PICCIRILLI
JONATHAN A. POLANSKY - EDUARDO SAAD-DINIZ - CARLOS C. SUEIRO - SANTIAGO TRIGO
GABRIELA ULAS - DIEGO VERGARA VACCAREZZA - ALFREDO H. VANINETTI**

**FORENSIA
DIGITAL**

h
hammurabi
JOSE LUIS DEPALMA EDITOR



ÍNDICE GENERAL

SEMBLANZA. VIDA Y OBRA DEL DR. FELIPE VILLAVICENCIO TERREROS, por JUAN ELÍAS CARRIÓN	19
ABREVIATURAS	27

A. DOCTRINA

1. DERECHO PENAL. PARTE GENERAL

1

CIBERSEGURIDAD EN ARGENTINA: LA PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS

URIEL BEKERMAN

§ 1. Vulnerabilidades de una sociedad de información	35
§ 2. Una noción de la ciberseguridad	38
§ 3. Un breve repaso histórico general	39
§ 4. El tratamiento específico de la ciberseguridad en la Argentina	43
§ 5. Conclusiones	50

2

«FAKE NEWS» EN TIEMPOS DE CORONAVIRUS

MATEO BRODSKY

§ 1. Introducción	54
a) Pandemia COVID-19 y <i>fake news</i>	57
b) Fuentes fieles de información en la lucha bacteriológica global	58
c) <i>Fake news</i> y su adecuación a la figura de incitación a la conmoción pública (art. 211 del Código Penal)	60

d) Política criminal en la era digital. El patrullaje físico de calles y ciberpatrullaje intangible del ciberespacio	63
§ 2. Conclusión	66

3

**HACIA UN NUEVO PARADIGMA EN EL CIBERCRIMEN:
¿POR QUÉ DEBEMOS REGULAR LOS NEURODERECHOS?**

MARIANA M. PICCIRILLI - JUAN ESTEBAN DIAK

§ 1. Introducción	70
§ 2. Bienvenido al mundo, <i>homo symbolicus</i>	72
§ 3. ¿El mundo jurídico al rescate?	78
§ 4. El universo en una cáscara de nuez	83
§ 5. Conclusión: la quinta revolución industrial y el derecho penal	87

4

**PROGRAMACIÓN ÉTICA Y RESPONSABILIDAD PENAL
POR EL PRODUCTO. UN VÍNCULO POSIBLE
PARA ANALIZAR LA RESPONSABILIDAD CRIMINAL
EN LA INTELIGENCIA ARTIFICIAL**

NICOLÁS M. GRANDI

§ 1. Introducción	91
§ 2. La IA y la responsabilidad penal por el producto	93
§ 3. Transparencia y explicabilidad de la IA	94
§ 4. Categoría ontológica de la IA	96
§ 5. Inmaterialidad de la IA	97
§ 6. Dilema de los múltiples actores	97
§ 7. Programación ética de la IA	99
§ 8. Responsabilidad por las acciones llevadas adelante por la IA	103
§ 9. Conclusión	106

2. DERECHO PENAL. PARTE ESPECIAL

1

INTRUSISMO INFORMÁTICO EN LA REVOLUCIÓN 4.0

SABRINA NOELIA MAÑAS

§ 1. Introducción	114
§ 2. Fundamento de punibilidad	114
§ 3. Bien jurídico protegido	117
§ 4. Constitución Argentina e instrumentos internacionales	120
§ 5. Análisis del tipo penal: intrusismo informático	122

§ 6. Tipo objetivo	122
a) Verbo típico	122
— Acceder	122
b) Objeto del acceso	124
1. Sistema informático (todo o parte de este) o un dato informático	124
2. Ese sistema o dato informático o servicio debese ajeno y restringido	125
3. Extenderse en la autorización	126
c) Sujeto activo	127
d) Sujeto pasivo	128
e) Tipo doloso	128
f) Consumación y tentativa	129
§ 7. Ejercicio de la acción	132
§ 8. Agravantes	135
a) Sistema o dato informático de un organismo público estatal	135
b) Proveedor de servicios públicos	135
c) Proveedor de servicios financieros	136
§ 9. Proyecto de Reforma Código Penal 2019	136
§ 10. Agravante de funcionario público	137
§ 11. Proyecto de Reforma Código Penal 2019	138
§ 12. Ley 25.520 de Inteligencia Nacional (modificada por ley 27.126)	138
§ 13. Causas de justificación	139
§ 14. Vacío legislativo adjetivo	140
§ 15. Conclusión	142

2

**LA SUSTITUCIÓN DE IDENTIDAD. LA NECESIDAD
DE SU INCORPORACIÓN COMO TIPO PENAL
EN EL MUNDO DIGITAL**

NOELIA V. MITELLI - MAGDALENA ORLOFF

§ 1. Introducción: los desafíos del derecho en la era tecnológica	144
§ 2. La sustitución de identidad	147
§ 3. Antecedentes nacionales: aproximación al tratamiento legislativo de la figura de sustitución de identidad en el derecho interno	149
§ 4. Tipo penal de sustitución de identidad propuesto por el Proyecto de Reforma Integral del Código Penal de la Nación (decr. PEN 103/17)	152
§ 5. Propuesta de tipificación del tipo penal de sustitución de identidad	154
§ 6. Propuesta de política criminal tendiente a lograr la eficiencia de la prevención de actos de sustitución de identidad	156
a) Regulación de la prueba digital a nivel procesal	156
b) Alfabetización digital de la ciudadanía	157
c) Propuesta de unidad policial cibercrimen especializada en identificación biométrica (potencialmente sistema de inteligencia artificial)	157
d) Obligación del empleador de capacitar a sus empleados en manipulación de datos digitales (el Estado puede imponerse en la Administración pública mediante acordadas, ordenanzas, pero el sector privado debe incentivarlo)	158

1. Crear campañas de capacitación en la Administración pública sobre buenas prácticas en la manipulación de dispositivos digitales y protección de datos personales	158
2. Crear políticas de favorecimiento a nivel laboral y de exenciones tributarias para los empleadores privados que dicten cursos de capacitación a empleados sobre buenas prácticas en la manipulación de dispositivos digitales y protección de datos personales	158
3. Creación de un Comité de <i>habeas data</i>	158
e) Especialización de jueces y fiscales en ciberseguridad	158
§ 7. Conclusión	159

3

EL DERECHO PENAL FRENTE AL ACOSO LABORAL Y A LAS NUEVAS TECNOLOGÍAS

PATRICIA GALLO

§ 1. La problemática del acoso laboral	162
a) Introducción	162
b) El concepto de acoso laboral	165
c) El acoso laboral y las nuevas tecnologías	166
§ 2. Características del acoso laboral	167
a) Elementos definitorios del acoso laboral	167
b) Clases de acoso laboral	171
c) Distinción entre el acoso laboral descendente y el acoso laboral horizontal	172
d) Efectos perjudiciales del acoso laboral	177
§ 3. El acoso laboral y el derecho penal	179
a) Justificación de la intervención penal frente a las conductas de acoso laboral	179
b) El bien jurídico protegido en el delito de acoso laboral	182
c) Las nuevas tecnologías y la mayor gravedad del acoso laboral	182
§ 4. A modo de conclusión	184

4

FORMAS MODERNAS DE FINANCIAMIENTO DEL TERRORISMO: CONSIDERACIONES ESPECIALES PARA LAS NUEVAS TECNOLOGÍAS Y PARA EL LAVADO DE DINERO

HENRIQUE ABI-ACKEL TORRES - ALANA GUIMARÃES MENDES

§ 1. Introducción	188
§ 2. Expansión del derecho penal	188
§ 3. Punto de inicio: terrorismo y nuevas tecnologías	191
§ 4. Financiación del terrorismo mediante blanqueo de capitales	194
§ 5. Consideraciones finales	198

5

LAVADO DE ACTIVOS Y CRIPTOMONEDAS: EN BUSCA DE UN «COMPLIANCE» EFICIENTE

GABRIELA ULAS

§ 1. Introducción	202
§ 2. Lavado de activos de origen delictivo en la República Argentina	203
§ 3. Criptomonedas: ese medio tan utilizado y tan temido	206
§ 4. Dos casos que señalaron el problema	208
a) The Silk Road	208
b) Liberty Reserve SA	209
§ 5. Propuesta: un manual de procedimientos para operaciones con criptomonedas	210
a) Capacitaciones	211
b) Definiciones	211
c) Procedimientos	212
1. Políticas de prevención	212
2. Conocimiento del cliente	212
3. Determinación del perfil del cliente	214
4. Aceptación o rechazo del cliente	215
5. Clasificación de clientes	215
6. Auditorías de control	216
I. Control de las partidas conciliatorias	216
II. Control del rubro inversiones	217
III. Control de la valuación	217
7. Matriz de riesgo	217
8. Monitoreo	218
9. Conservación de documentación. Evaluación de operaciones con monedas virtuales	218
10. ROS	220
§ 6. Conclusiones	221

6

DELITOS CONTRA LA COMPETENCIA COMETIDOS POR SISTEMAS DE INTELIGENCIA ARTIFICIAL: DE LA FICCIÓN A LOS PROGRAMAS DE «COMPLIANCE»

EDUARDO SAAD-DINIZ - JULIANA OLIVEIRA DOMINGUES

§ 1. Introducción	224
§ 2. <i>Big Data</i> , inteligencia artificial y los posibles ilícitos contra la libre competencia — Inteligencia artificial y el CADE	227
§ 3. El control social de los ilícitos contra la libre competencia	231
a) Repensando alternativas: las limitaciones humanas frente a los agentes inteligentes	234
b) <i>Compliance</i> e inteligencia artificial	237
§ 4. Entre los sistemas inteligentes y el comportamiento ético	239

7

**CIBERCRIMINALIDAD Y DELITOS
CONTRA LA PROPIEDAD**FRAUDES, SABOTAJE Y EXTORSIÓN «ONLINE»
EN LA MODERNA SOCIEDAD DE LA TECNOLOGÍA

GUSTAVO E. ABOSO

§ 1. Introducción	241
§ 2. El bien jurídico patrimonio. Concepto y alcance	244
§ 3. Utilización fraudulenta de tarjeta de compra, crédito o débito	249
— Modalidades de falsificación de tarjetas para su uso fraudulento	255
— <i>Skimming</i>	255
§ 4. Fraude o estafa informático (<i>Computerbetrug</i>)	259
a) <i>Phishing</i>	269
— El intermediario financiero, "mulero informático" (<i>Finanzagent</i>)	272
b) <i>Pharming</i>	274
§ 5. Aspectos generales del fraude informático	275
a) Ausencia de consentimiento	275
b) Sujeto pasivo	275
c) Perjuicio patrimonial	276
d) Autoría y participación	280
e) Tipicidad subjetiva	282
f) Consumación y tentativa	282
§ 6. Otras formas de presuntos fraudes informáticos	283
§ 7. Daño o sabotaje informático	285
a) Delito de facilitación de programas dañinos	285
b) Daño informático cualificado	301
§ 8. Extorsión <i>online</i> (<i>online extortion</i>)	301
§ 9. Derecho comparado	302
§ 10. Valoración final	303

3. DERECHO PROCESAL PENAL

1

**PROCESOS PENALES PREDICTIVOS.
LA INFLUENCIA DE LA INTELIGENCIA ARTIFICIAL
Y SUS POSIBLES LÍMITES**

JUAN MOLINAS

§ 1. Introducción	310
§ 2. Génesis de la predicción: el actuarialismo penal	311

§ 3. Inteligencia artificial y derecho penal	315
a) El concepto de inteligencia artificial y su evolución	315
b) ¿Cómo funciona la IA?	317
§ 4. Justicia predictiva	318
§ 5. Policía predictiva	321
§ 6. Experiencias predictivas actuales a nivel global	324
a) Estados Unidos de América, el caso "Loomis" y la "lista estratégica de sujetos"	324
b) El sistema de crédito social chino	327
c) Alemania: PRECOBS, SKALA y la Ley de Policía Predictiva	329
§ 7. Problemas derivados del uso desmedido de la IA	330
a) Afectaciones constitucionales	330
b) ¿Puede un algoritmo reemplazar a un juez?	333
§ 8. Conclusión	335

B. FORENSIA DIGITAL

1

**PERICIA INFORMÁTICA, PLAN DE INVESTIGACIÓN
Y PUNTOS DE PERICIA**PABLO CISTOLDI - SABRINA LAMPERTI
SANTIAGO TRIGO - ANA DI IORIO

§ 1. Función de los expertos forenses	342
§ 2. Abordaje, plan de investigación, teoría del caso y aporte experto	343
§ 3. Pautas a considerar en el planteo de los puntos periciales	344
a) ¿Qué se necesita saber o probar?	344
b) ¿Para qué fin se usará esa evidencia? ¿Es relevante?	344
c) ¿Dónde se encuentra la evidencia?	346
1. Disco rígido o disco de estado sólido	346
2. Memoria principal	347
3. Dispositivos de almacenamiento persistente extraíbles	348
4. Volcado de paquetes de tráfico de red	348
5. Sinergia entre los componentes	349
— Caso ejemplo	349
6. Otros dispositivos	350
d) ¿Quién tiene la evidencia?	351
e) ¿Cómo se obtiene?	351
f) ¿Cuándo y de qué forma se incorpora?	352
g) ¿Qué herramientas se requieren para hacer la pericia?	353
h) ¿Qué conocimientos específicos se requieren por parte del perito que interviene?	353
§ 4. Puntos de pericia. Buenos y malos ejemplos	356
a) Pericia sobre clonadores	356
b) Pericia informática genérica	356

c) Pericia informática. Temas inmobiliarios	357
d) Pericia informática. Imágenes de abuso sexual infantil	358
e) Malos ejemplos	359
f) Punto discutible	360
— "Cualquier otro dato de interés"	360
§ 5. Reflexión	360

C. DERECHO INFORMÁTICO COMPARADO

1

DELITOS EN EL CIBERESPACIO: CONCEPTO Y CARACTERÍSTICAS

PAZ LLORIA GARCÍA

§ 1. Introducción	366
§ 2. La revolución tecnológica y la aparición de Internet	366
§ 3. Concepto de los delitos tecnológicos	368
§ 4. Características de los delitos tecnológicos	373
a) La dificultad en la persecución	373
b) El incremento de injusto	374
§ 5. Sistema de protección	376
§ 6. Conclusión	376

D. SELECCIÓN DE JURISPRUDENCIA

1. ANÁLISIS DE FALLOS

1

LIBERTAD DE EXPRESIÓN, DISCURSO DE ODIOS Y DERECHO PENAL EN LA SOCIEDAD DE LA TECNOLOGÍA

¿COMPARTIR O DAR «LIKE» A UNA PUBLICACIÓN
EN FACEBOOK PUEDE SER DIFAMATORIO?

GUSTAVO EDUARDO ABOSO

§ 1. Introducción	383
§ 2. La sentencia del Tribunal Superior Federal Suizo	384
§ 3. La libertad de expresión en el mundo virtual	385
§ 4. La libertad de expresión y sus límites	392
§ 5. Los discursos de odio como antítesis de la libertad de expresión	400
§ 6. El negacionismo y la libertad de expresión	410

§ 7. Apología del terrorismo y libertad de expresión	427
§ 8. Discriminación y libertad de expresión	431
§ 9. La regulación de los deberes de los proveedores del servicio de Internet en relación con el discurso del odio	440
§ 10. Conclusiones	443

2

SISTEMAS DE RECONOCIMIENTO FACIAL EN EL PROCESO PENAL

ANOTACIONES AL FALLO «OBSERVATORIO
DE DERECHO INFORMÁTICO ARGENTINO O.D.I.A.
C. GCBA S/ACCESO A LA INFORMACIÓN»

DIEGO VERGARA VACCAREZZA - SANTIAGO GAMARRA CALELLO

§ 1. Introducción	447
§ 2. Los sistemas de reconocimiento facial	448
— Concepto y características	448
§ 3. Implementación y regulación de los sistemas de reconocimiento facial (SRF)	450
a) Estado de situación en el orden internacional. Casos emblemáticos	450
— El caso "R. Bridges v. CC South Wales Police"	454
b) Argentina: su reciente implementación en la Ciudad Autónoma de Buenos Aires	455
§ 4. El caso "O.D.I.A. c. CABA"	459
a) Hechos y decisión judicial	459
b) Acceso a la información pública y tecnologías de vigilancia	460
§ 5. Análisis de los aspectos relevantes de la decisión	461
a) Reconocimiento facial y detención de prófugos imputados por delitos de especial severidad	461
b) Sobre la transparencia de los sistemas inteligentes de la Administración pública	466
— Transparencia de los modelos de IA y protección de datos personales	468
c) Del reconocimiento facial de prófugos a la predicción criminal y el análisis forense de evidencia digital almacenada	471
§ 6. Conclusiones	476

2. FALLOS SELECCIONADOS

JURISPRUDENCIA NACIONAL

— Sumarios	481
1. Atipicidad de acceso ilegítimo, daño y defraudación informática	481
2. Defraudación informática (art. 173, inc. 15, CP)	483
3. Defraudación con tarjetas de crédito y débito (art. 173, inc. 15, CP)	483
4. Defraudación informática (art. 173, inc. 16, CP)	484

E. COMENTARIOS BIBLIOGRÁFICOS

1

DERECHO A LA INTIMIDAD EN LA ERA DIGITAL. DERECHOS PERSONALÍSIMOS

ALFREDO H. VANINETTI

----- 489

2

VIGILANCIA ELECTRÓNICA Y OTROS MODERNOS MEDIOS DE PRUEBA

CARLOS CHRISTIAN SUEIRO

----- 491

3

GARANTÍAS CONSTITUCIONALES DEL PROCEDIMIENTO PENAL EN ENTORNO DIGITAL

JONATHAN A. POLANSKY

----- 499

4

VIGILANCIA ELECTRÓNICA ASISTIDA POR INTELIGENCIA ARTIFICIAL (IA)

CARLOS CHRISTIAN SUEIRO

----- 501

BIBLIOGRAFÍA GENERAL -----

505

PAUTAS EDITORIALES -----

525



MARCELO A. RIQUERT dirección
CARLOS CHRISTIAN SUEIRO coordinación

Sistema penal e informática

CIBERDELITOS. EVIDENCIA DIGITAL. TICS

5

RESPONSABILIDAD PENAL DERIVADA DEL USO DE VEHÍCULOS AUTÓNOMOS.
INTERRUPCIONES GENERALES DE INTERNET. VULNERABILIDAD DE LAS APLICACIONES
DE VIDEOLLAMADAS. DEFENSA PÚBLICA OFICIAL 4.0. LA INTELIGENCIA
ARTIFICIAL AL SERVICIO DE LA DEFENSA PÚBLICA. CIUDAD INTELIGENTE, POLICÍA
DEL FUTURO Y CAPITAL CIBERNÉTICO. CRIPTOMONEDAS EN EL DERECHO PENAL
NACIONAL. NUEVAS MODALIDADES DE DEFRAUDACIÓN INFORMÁTICA.
CIBERCRIMINALIDAD FINANCIERA Y «PHISHING» BANCARIO. ALTERACIÓN DOLOSA
DE REGISTROS FISCALES. EVIDENCIA DIGITAL Y CADENA DE CUSTODIA.
HISTORIA CLÍNICA ELECTRÓNICA Y CRIMINALIDAD INFORMÁTICA

autores **GUSTAVO EDUARDO ABOSO - GUIDO BASTUS - URIEL BEKERMANN**
PABLO ADRIÁN CISTOLDI - AGUSTÍN DÍAZ CAFFERATA - ANA HAYDÉE DI IORIO
JULIO C. DUHALDE - CANDELA BELÉN FERNÁNDEZ RASILLO - JOSÉ SANTIAGO FRANCO
MARÍA DE LOS MILAGROS FRANCO - AMPARO GIUFFRÉ - GUILLERMO OSCAR GOBBI
MARÍA CANDELA MALDONADO - SABRINA MAÑAS - MARCELO A. RIQUERT
LEONARDO FABIÁN SAI - CARLOS CHRISTIAN SUEIRO

FORENSIA DIGITAL	CORTE SUPREMA BIBLIOTECA	
	SIG. TOPOGRAFICA Q 950	INVENTARIO 166425



hammurabi
JOSE LUIS DEPALMA EDITOR



ÍNDICE GENERAL

ABREVIATURAS	19
---------------------------	----

A. DOCTRINA

1. DERECHO PENAL. PARTE GENERAL

1

INTERRUPCIONES GENERALES DE INTERNET

SU PROBLEMÁTICA DESDE EL DERECHO INTERNACIONAL

DE LOS DERECHOS HUMANOS

GUILLERMO OSCAR GOBBI

§ 1. Introducción	29
§ 2. Internet y contexto actual	31
§ 3. Aproximación desde el derecho internacional de los derechos humanos	37
a) Las obligaciones estatales a la luz del DIDH	38
b) La protección desde el Sistema Universal de Derechos Humanos (SUDH)	39
c) La Declaración Universal de Derechos Humanos	39
d) El Pacto Internacional de Derechos Civiles y Políticos	40
1. Internet y el contenido del derecho a la libertad de expresión y a recibir información	40
2. Las restricciones al acceso a la información en el <i>PIDCP</i>	42
3. El principio <i>pro persona</i>	42
e) El Pacto Internacional de Derechos Económicos Sociales y Culturales	44
1. Exigibilidad de los DESC	45
2. El acceso a la información y los DESC	46
3. Interrelación entre los DESC y los Objetivos de Desarrollo Sustentable	47

f) Pronunciamientos relevantes de organismos del Sistema Universal de Derechos Humanos	49
— Informes de la Relatoría sobre Libertad de Expresión de Naciones Unidas ..	49
I. Informe del relator Abid Hussain del 13 de febrero de 2001 (E/CN.4/2001/64)	50
II. Informe del relator Abid Hussain del 30 de enero de 2002 (E/CN.4/2002/75)	50
III. Informe del relator Frank La Rue de 20 de abril de 2010 (A/HRC/14/23) ..	51
IV. Informe del relator Frank La Rue del 10 de agosto de 2011 (A/66/290) ..	51
V. Informe del relator David Kaye de 6 de septiembre de 2016 (A/71/373) ..	52
VI. Informe del relator David Kaye del 18 de agosto de 2017 (A/72/350)	53
g) La Convención Americana de Derechos Humanos y el acceso a Internet	53
— El análisis de proporcionalidad	54
h) Pronunciamientos relevantes de órganos del Sistema Interamericano de Derechos Humanos sobre las interrupciones al servicio de Internet	55
§ 4. Legislación argentina vinculada a las restricciones generales al acceso a Internet ..	57
§ 5. Conclusiones	59

2

VULNERABILIDAD DE APLICACIONES DE VIDEO LLAMADAS Y COMPETENCIA DE LA VÍCTIMA

PRIMERAS APROXIMACIONES Y REFLEXIONES

JOSÉ SANTIAGO FRANCO - MARÍA DE LOS MILAGROS FRANCO

§ 1. Introducción	66
§ 2. Una primera aproximación sobre la seguridad informática	67
§ 3. Sobre la criptografía	68
§ 4. Aplicaciones de videollamadas y la seguridad. El caso de Zoom	69
§ 5. Aplicaciones de videollamadas que pueden ser utilizadas como alternativa	72
a) Google Duo	72
b) Messenger	72
c) Skype	72
d) Jitsi Meet	72
e) Teams	73
f) Line	73
§ 6. Marco legal	73
§ 7. Competencia de la víctima	75
a) Concepto	75
b) Ubicación sistemática del problema	76
§ 8. Alcances y presupuestos a tener en cuenta de la competencia de la víctima	78
a) Causalidad	78
b) Dominabilidad y posibilidad de usos alternativos	80

§ 9. Diferentes tesis del comportamiento del ofendido	81
a) Conducta jurídicamente relevante (o imputación objetiva del comportamiento)	82
b) Imputación de la conducta e imputación del resultado	86
c) Relación con el resultado	88
§ 10. Conclusiones	91

3

DEFENSORÍA PÚBLICA OFICIAL 4.0

LA IA AL SERVICIO DE LA DEFENSA: UNA HERRAMIENTA PARA GARANTIZAR EL ACCESO A LA JUSTICIA E IGUALAR LAS ARMAS

SABRINA MAÑAS - AMPARO GIUFFRÉ

§ 1. Introducción	94
§ 2. Institución pública a aplicar IA: Defensoría Pública Oficial	95
a) Descripción del organismo seleccionado	95
b) Una Defensoría Pública de Brasil — pionera en la utilización de IA—	96
§ 3. Marco teórico	98
a) TIC's e Inteligencia Artificial, breve reseña	98
b) Aproximación al concepto de Inteligencia Artificial (IA)	100
c) Herramientas de IA seleccionadas para implementar en la Defensoría Pública. Tareas automatizables. Árboles de decisión	103
§ 4. Proyecto de innovación	104
a) Chatbot defensoría externo	105
b) Chatbot defensoría interno	106
1. Automatización de tareas administrativas	106
2. Automatización de planteos jurídicos con árboles de decisión	106
c) API complementaria	108
§ 5. Conclusión	109

4

EN EL EXTERIOR DE LA CIUDAD INTELIGENTE: POLICÍA DEL FUTURO Y CAPITAL CIBERNÉTICO

LEONARDO FABIÁN SAI

§ 1. El último hombre es un <i>cyborg</i>	112
§ 2. La ciudad inteligente del capital cibernético	116
§ 3. El caso de la empresa Axon: la policía inteligente como automatización de la persecución penal	121
§ 4. De la exterioridad fantasmagórica al <i>gaming</i> de la ciudad inteligente	125

5

**APROXIMACIÓN A LAS CRIPTOMONEDAS:
CUESTIONES BÁSICAS Y ANÁLISIS
BAJO EL DERECHO PENAL NACIONAL**

AGUSTÍN NICOLÁS PANTANO

§ 1. Introducción	130
§ 2. Un abordaje a las criptomonedas	132
a) Surgimiento de las criptomonedas. Qué problemas pretendió solucionar	132
b) Cuáles son las características de las criptomonedas	133
1. Criptografía	133
2. <i>Blockchain</i> descentralizada	135
3. Intercambios puerto a puerto (P2P)	137
c) Consecuencias del uso de esta tecnología	138
1. Qué beneficios apareja el uso de estas tecnologías	138
I. Altos estándares de seguridad	138
II. Un fenómeno global, desformalizado y descentralizado	139
III. Irreversibilidad: acceso y transferencias	140
2. Por qué la adopción fue masiva en nuestro país	141
d) Cómo se utilizan las criptomonedas en la vida cotidiana	143
1. Activos digitales. Medios de inversión. Soluciones financieras	144
2. Medio de pago o moneda de curso legal	144
3. <i>Exchanges</i> o mercados de intercambio	144
4. Redes descentralizadas de <i>blockchain</i>	144
5. NFT's. Aplicación	145
6. Cadenas de suministro	146
7. <i>Stable-coins</i>	146
e) Criptomonedas y sistemas de justicia	146
1. El sistema judicial	146
2. Sistemas privados y descentralizados de resolución de conflictos	148
§ 3. Criptomonedas y derecho penal	149
a) Regulación y reconocimiento en el derecho local	149
b) Fenómenos de su tecnología que presentan un problema para el derecho penal local. Formas de abordarlo	153
1. Interjurisdiccionalidad	153
2. Anonimato y desregularización	154
3. Facilidad y velocidad para transferir activos	155
4. Imposibilidad de confiscarlos por su tecnología y <i>nemo tenetur</i>	155
5. El problema de la terminología a la luz del principio de legalidad	156
c) La tecnología que aportan las criptomonedas y la comisión de delitos del Código Penal	156
1. Lavado de activos	156
2. Estafas y otras defraudaciones	159
3. El <i>hacking</i> . Acceso no autorizado. ¿Hurtos y defraudación informática?	162

4. Delitos cambiarios	163
I. Entidades financieras	163
II. Personas humanas	164
5. Delitos financieros	165
6. Delitos tributarios	167
d) Las criptomonedas como modo de facilitar la comisión de otros delitos. Cuestiones adicionales	169
1. Medio para transaccionar objetos prohibidos en alguna medida por la ley	169
2. Mineros y medioambiente	169
e) Decomiso de cryptoactivos. Gestión judicial de patrimonio incautado	170
§ 4. Palabras finales	171

2. DERECHO PENAL. PARTE ESPECIAL

1

**NUEVAS MODALIDADES DE DEFRAUDACIÓN INFORMÁTICA
EN EL TELETRABAJO**

CAROLINA DE SOUSA MATIAS

§ 1. Introducción	175
§ 2. Defraudación informática	178
a) Antecedentes nacionales: Leyes 26.388, 26.685, 26.904, 27.411 y 27.436	178
b) Defraudación informática	180
c) Bien jurídico protegido	180
d) Acción típica	181
e) El sujeto de la acción típica	184
f) Tipicidad subjetiva	185
g) Consumación y tentativa	185
§ 3. Nuevas modalidades de defraudaciones informáticas y su problemática	186
a) Defraudaciones cometidas a través de la utilización de código QR	186
b) Criptomonedas - Bitcoin	188
c) Defraudaciones informáticas mediante falsa amenaza de distribución de imágenes íntimas	190
§ 4. Proyecto de reforma integral al Código Penal de la Nación (Decreto PEN 103/17)	191
§ 5. Conclusiones finales	194

2

**CIBERCRIMINALIDAD FINANCIERA Y «PHISHING» BANCARIO:
DIAGNÓSTICO Y HERRAMIENTAS DE TUTELA JUDICIAL**

URIEL BEKERMÁN - GUIDO BASTUS

§ 1. Las grandes entidades financieras como infraestructuras críticas	196
---	-----

§ 2. La importancia de la privacidad y seguridad de los datos personales financieros	198
§ 3. El caso del <i>phishing</i> bancario	200
§ 4. Posiciones encontradas sobre la responsabilidad institucional y la participación de la víctima	200
§ 5. Las medidas adoptadas por el BCRA	201
§ 6. Herramientas de tutela administrativa para los usuarios	202
§ 7. Herramientas de tutela judicial en sede penal	203
§ 8. Herramientas de tutela judicial en sede civil y comercial	205
§ 9. Conclusiones	206

3

ALTERACIÓN DOLOSA DE REGISTROS DEL FISCO VERSUS LA TRANSMISIÓN INFORMÁTICA DE DATOS INSINCEROS

MARÍA CANDELA MALDONADO - A. AGUSTÍN DÍAZ CAFFERATA

§ 1. Problemática actual	210
§ 2. Correcta subsunción de la conducta prevista en el art. 11, inc. a) del Régimen Penal Tributario	213
a) El bien jurídico tutelado en el art. 11 del Régimen Penal Tributario: La intangibilidad de los registros del Fisco	213
b) La tipicidad objetiva. Concepto de "registro informático" en el ordenamiento legal	216
c) Los registros informáticos de AFIP	218
d) Ámbito de actuación de los medios comisivos	221
§ 3. Breve mención a la desproporcionalidad de las penas en el Régimen Penal Tributario	223
§ 4. Diferentes escenarios y su posible respuesta punitiva desde una visión integral y de mínima intervención del derecho penal como <i>ultima ratio</i>	225
a) El ámbito contravencional - tributario	225
b) El ámbito penal - tributario	226
§ 5. El tratamiento jurisprudencial reciente de la figura	226
a) Cámara Nacional en lo Penal Económico, Sala B	226
b) Juzgado Federal n° 3 de la Ciudad de Córdoba	228
c) Cámara Federal de la Ciudad de Córdoba, Sala B	229
§ 6. Conclusiones	230

4

HISTORIA CLÍNICA ELECTRÓNICA Y CRIMINALIDAD INFORMÁTICA

CANDELA BELÉN FERNÁNDEZ RASILLO

§ 1. Introducción	234
-------------------	-----

§ 2. La historia clínica electrónica	234
§ 3. Los ciberdelitos vinculados al acceso ilegítimo y modificación de la historia clínica electrónica	240
a) El acceso ilegítimo a las bases de datos personales de los centros de salud	243
b) Revelación de secretos de profesionales de la salud o funcionarios públicos	249
§ 4. Propuesta de un tipo penal específico de tutela de bases de datos de centros de salud	253
§ 5. Conclusión	254

3. DERECHO PROCESAL PENAL

1

LA EVIDENCIA DIGITAL, LA PRUEBA DE ESE ORIGEN, LA INFORMÁTICA FORENSE Y LA CADENA DE CUSTODIA: PROPUESTAS DE DEFINICIÓN

JULIO C. DUHALDE

§ 1. Introducción	259
§ 2. ¿Qué es la evidencia digital?	265
a) La evidencia y la prueba	266
b) ¿Qué dicen los códigos procesales penales sobre la evidencia digital?	272
§ 3. ¿Qué es la informática forense?	275
§ 4. Cadena de custodia	277
§ 5. Conclusiones	283

B. FORENSIA DIGITAL

1

PRUEBA CIENTÍFICA, MÁXIMAS DE LA EXPERIENCIA Y RAZONAMIENTO PROBATORIO: UN SISTEMA DE FRONTERAS MÓVILES. APORTES DESDE LA INFORMÁTICA

ANA HAYDÉE DI IORIO - PABLO ADRIÁN CISTOLDI

§ 1. Introducción	288
§ 2. Los fenómenos informáticos	289
§ 3. La informática forense y la evidencia digital	290
— Un ejemplo	292
§ 4. Sentido común, prueba científica y prueba pericial	293
a) Un sistema de fronteras móviles	294
b) El razonamiento probatorio ante un marco inestable	298
c) Necesitamos un perito, pero... ¿cuál perito?	300
d) Verdad y participación procesal: garantías y exigencias	302

§ 5. Informática, Ciencias de la Información y razonamiento probatorio	303
§ 6. Convergencia entre ciencia y justicia: reflexiones y caminos posibles	307
a) Convergencia procesal	307
b) Convergencia interinstitucional	308
c) Convergencia académica	309
§ 7. Algunas posibles líneas de intercambios fructíferos	310
a) Aportes pertinentes al concepto de pertinencia probatoria	310
b) Tutorías de ciencias	311
c) Evidencia digital, información y prueba	312
§ 8. Reflexiones finales	313

C. DERECHO INFORMÁTICO COMPARADO

1

LA RESPONSABILIDAD PENAL DERIVADA DEL USO DE AUTOMÓVILES AUTÓNOMOS, CON ESPECIAL REFERENCIA A LA NUEVA REGULACIÓN FRANCESA

GUSTAVO EDUARDO ABOSO

§ 1. Introducción	317
§ 2. La nueva regulación de los vehículos autónomos en la legislación penal francesa	320
§ 3. La regulación del vehículo robótico en la ley de tránsito francesa	321
§ 4. La responsabilidad penal derivada del siniestro vial producido con el vehículo robótico	324
§ 5. El caso "Herzberg" y la primera víctima mortal de un sistema operativo aplicado a la conducción automatizada	341
§ 6. La autopuesta en peligro voluntaria del conductor del automotor robótico	342
§ 7. La conducción automatizada en nuestra ley penal	343
§ 8. Palabras finales	345

D. SELECCIÓN DE JURISPRUDENCIA

1. ANÁLISIS DE FALLOS

1

CRIPATOMONEDAS Y DELITO: APUNTES INICIALES

MARCELO A. RIQUERT

§ 1. Introducción	351
§ 2. Las criptomonedas y su funcionalidad para el delito	355

§ 3. Entre fraudes, pedidos de regulación y prohibiciones	359
§ 4. Consideración legal en Argentina	362
a) Algunas referencias generales	363
b) Primeras repercusiones en la jurisprudencia penal	367
§ 5. Colofón	369
§ 6. Texto de la sentencia	369

2. FALLOS SELECCIONADOS

JURISPRUDENCIA NACIONAL

— Sumarios	375
1. <i>Grooming</i> (art. 131, CP)	375
2. Defraudación informática (art. 173, inc. 16, CP)	376
3. Acceso ilegítimo a un sistema informático (art. 153 bis, CP)	376

JURISPRUDENCIA INTERNACIONAL

— "Van Buren v. Estados Unidos"	379
---------------------------------------	-----

E. COMENTARIOS BIBLIOGRÁFICOS

1

ACOSOS EN LA RED A NIÑOS, NIÑAS Y ADOLESCENTES

AA.VV.	383
-------------	-----

2

CIBERCRIMEN III

AA.VV.	385
-------------	-----

3

VIOLENCIA SOBRE LA MUJER EN EL SIGLO XXI: VIOLENCIA DE CONTROL Y NUEVAS TECNOLOGÍAS. HABITUALIDAD, «SEXTING» Y «STALKING»

PAZ LLORIA GARCÍA	389
-------------------------	-----

BIBLIOGRAFÍA GENERAL	393
PAUTAS EDITORIALES	407