MARCELO A. RIQUERT dirección
CARLOS CHRISTIAN SUEIRO coordinación

Sistema penal e informática

CIBERDELITOS. EVIDENCIA DIGITAL. TICS

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 ODIO. 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

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 *fake news* ____ 57
b) Fuentes fieles de información en la lucha bacteriológica global ____ 58
c) *Fake news* 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, *homo symbolicus* ____ 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 debe ser 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 *habeas data* ____ 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 Rerserve 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. *Big Data*, inteligencia artificial y los posibles ilícitos contra la libre competencia ____ 227
— Inteligencia artificial y el CADE ____ 229
§ 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) *Compliance* 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
— *Skimming* ____ 255
§ 4. Fraude o estafa informático *(Computerbetrug)* ____ 259
a) *Phishing* ____ 269
— El intermediario financiero, "mulero informático" *(Finanzagent)* ____ 272
b) *Pharming* ____ 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 *online (online extortion)* ____ 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 ODIO 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