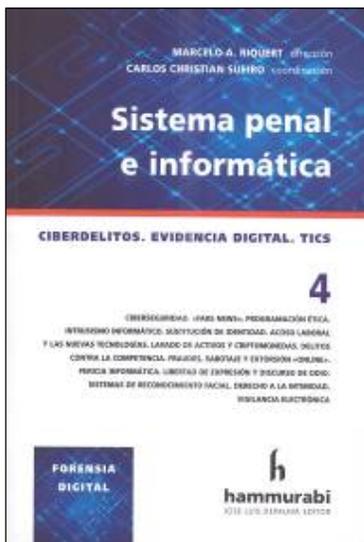


ÍNDICE GENERAL



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 ciberdelictos 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) <i>The Silk Road</i>	208
b) <i>Liberty Reserve SA</i>	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	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) <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 TECNOLOGIA

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 donadores	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 de fraudación 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
BIBLIOGRAFIA GENERAL	505
PAUTAS EDITORIALES	525