

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 Hamurabi	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