

**DANIELA S. DUPUY** dirección  
**FEDERICO BAUDINO** coordinación

# Innovación en investigaciones digitales

## TÉCNICAS Y TECNOLOGÍAS APLICADAS A LA INVESTIGACIÓN DE HECHOS DELICTIVOS

ANONIMATO DIGITAL PARA COMETER DELITOS. VIOLENCIAS SEXUALES A NIÑOS, NIÑAS Y ADOLESCENTES POR MEDIOS DIGITALES. «SEXTING». HOSTIGAMIENTOS DIGITALES. CIBERFRAUDES. REGULACIÓN DE «BLOCKCHAIN» Y CRIPTOMONEDAS. PRUEBA DIGITAL. PROTECCIÓN DE LOS DATOS PERSONALES. AGENTE ENCUBIERTO EN EL CIBERESPACIO. ALLANAMIENTOS REMOTOS Y EL USO DE DRONES. VIDEOVIGILANCIA Y USO DE VANT. RECONOCIMIENTO FACIAL. IA Y NEUROCIENCIAS. «HACKEO» MENTAL

autores **YAMILA V. ARRIAGA GONZÁLEZ - ANTONELLA MARÍA BENTIN - AGUSTINA. CHALHUB  
PAOLA V. CHARAJA COATA - MARÍA SOL CINOSI - VÍCTOR HUGO J. DÍAZ PÉREZ  
JAZMÍN GALLEGOS AMAYA - MARTÍN GOVETTO - DENISE GROSS - CECILIA LABANCA  
GABRIELA M. LAPADULA - JORGE LUIS LITVIN - CARLOS A. LÓPEZ MENDOZA - NATALIA M. MOLINA  
MACARENA ORTEGA - DIANA LIZETH PROAÑO AYALA - ROMINA A. QUEVEDO  
FERNANDO L. RIVAROLA - AGUSTINA MARÍA ROMAIN - JUAN MANUEL SARRABAYROUSE  
SAMUEL A. SILVA VILLAGÓMEZ - DIEGO STRATIOTIS - NIEVES PAPA TELLO  
ALEJANDRO A. TEMPORETTI OLIVERA - AMPARO ZAVALÍA - MARÍA AGUSTINA ZELIS LINARES**

**1ª EDICIÓN**



**hammurabi**  
JOSE LUIS DEPALMA EDITOR



© Copyright by  
**editorial hammurabi s.r.l.**

Talcahuano 438 - 1° piso "A"  
C1013AAI - Buenos Aires - Argentina  
Tel.: (54-11) 4371-8179 — líneas rotativas —  
E-mail: info@hammurabi.com.ar - www.hammurabi.com.ar

- [twitter.com/hammurabi\\_srl](https://twitter.com/hammurabi_srl)
- [facebook.com/libreriahammurabi](https://facebook.com/libreriahammurabi)
- [Instagram.com/libreriahammurabi](https://instagram.com/libreriahammurabi)
- [youtube.com/libreriahammurabi](https://youtube.com/libreriahammurabi)

Producción integral



concept design

de **FERNANDO LUCAS DEPALMA**

**EDICIÓN DIGITAL**

Marzo de 2022

**EDICIÓN PAPEL**

Marzo de 2022

Impreso por «**La Imprenta Ya S.R.L.**»  
A. Hipólito Bouchard 4381, Buenos Aires - Argentina

Hecho el depósito de ley 11.723

Derechos reservados

Prohibida su reproducción total o parcial

Impreso en Argentina / Printed in Argentina

ISBN: 978-987-805-229-8

1215307

DANIELA S. DUPUY dirección - FEDERICO BAUDINO coordinación

**INNOVACIÓN EN INVESTIGACIONES DIGITALES**

1ª edición, Buenos Aires, **Hammurabi**, 2022

680 ps., 23 x 16 cm.

ISBN: 978-987-805-229-8

1. Derecho penal I. Título

CDD 345

Fecha de catalogación: 10/3/2022

Archivo Digital: *Online*

ISBN: 978-987-805-230-4

Fecha de publicación: 10/3/2022

## ÍNDICE GENERAL

<b>ABREVIATURAS</b> .....	23
---------------------------	----

### PRIMERA PARTE DERECHO PENAL

#### Capítulo I

#### **CAPAS DE INVISIBILIDAD Y MÁSCARAS DIGITALES PARA OCULTAR LA IDENTIDAD**

LAS CARAS DEL ANONIMATO: DERECHO Y HERRAMIENTA CRIMINAL

JORGE LUIS LITVIN

§ 1. Magia y tecnología .....	33
§ 2. Históricamente anonimizados .....	35
§ 3. La sociedad basada en datos .....	37
§ 4. El anonimato 2.0 .....	40
§ 5. ¿Permitido, prohibido o garantizado? .....	44
§ 6. En búsqueda de un balance. Propuesta y consideraciones finales .....	48

#### Capítulo II

#### **¿EXISTE UN DERECHO AL PROPIO ENTORNO VIRTUAL?**

ANÁLISIS DESDE LA JURISPRUDENCIA ESPAÑOLA

PAOLA VANESSA CHARAJA COATA

§ 1. Introducción .....	51
§ 2. Origen jurisprudencial del derecho al propio entorno virtual .....	53
§ 3. Sobre los derechos implícitos o no enumerados .....	56
§ 4. El derecho a la intimidad .....	57

§ 5. Características del derecho al propio entorno virtual .....	59
§ 6. El derecho al propio entorno virtual como derecho implícito al derecho a la intimidad .....	61
§ 7. El derecho al propio entorno virtual y otros derechos fundamentales .....	62
a) El derecho a la protección de datos de carácter personal .....	62
b) Derecho al secreto de las comunicaciones .....	65
§ 8. Sentencias del Tribunal Europeo de Derechos Humanos sobre la intimidad en el ámbito laboral .....	65
§ 9. Conclusiones .....	68

## Capítulo III

**EL TRÁFICO DE MATERIAL DE ABUSO SEXUAL INFANTIL.  
EL ABUSO SEXUAL QUE SURGE DE LAS IMÁGENES  
O VIDEOS. ACCIÓN PENAL**

APLICACIÓN DE LAS CONVENCIONES INTERNACIONALES

NATALIA MARCELA MOLINA

69

## Capítulo IV

**VIOLENCIAS SEXUALES EN NIÑOS,  
NIÑAS Y ADOLESCENTES  
POR MEDIOS DIGITALES**

MARTÍN GOVETTO - NIEVES PAPA TELLO

§ 1. Introducción .....	83
§ 2. Conceptos generales y violencias digitales .....	84
§ 3. Investigación .....	85
a) Desarrollo. Encuesta .....	85
b) Resultado de la encuesta .....	86
§ 4. Examen de los delitos de violencia sexual por medios digitales .....	91
§ 5. Las víctimas .....	92
§ 6. El interés superior del niño .....	94
a) Marco legal y principios de protección .....	94
b) La identidad digital y su afectación .....	95
§ 7. El perfil del pederasta digital .....	97
§ 8. Lineamientos para determinar las penas en delitos digitales .....	101
§ 9. Medidas cautelares y accesorias a la pena .....	103
§ 10. Examen de sentencias de la Argentina .....	103
a) «Carignano, Franco Daniel p.s.a. producción de imágenes pornográficas de menores de 18 años» .....	103
b) «Russo, Ricardo A. G. s/Art. 128 CP» .....	104
c) «Luna, Yésica c. Griffith, Daniel Alejandro s/Coacción» .....	105
§ 11. Conclusiones .....	106

**ÍNDICE GENERAL**

11

## Capítulo V

**LOS DATOS COMO INSUMO PARA EL ANÁLISIS DEL ABUSO SEXUAL INFANTIL EN EL CIBERESPACIO**

JAZMÍN GALLEGOS AMAYA

§ 1. Introducción .....	107
§ 2. El inicio de la problemática .....	109
a) Panorama del abuso sexual infantil .....	112
b) El abuso sexual infantil en el ciberespacio .....	114
c) Las estadísticas y los bancos de información como herramientas para la identificación del abuso sexual infantil .....	115
§ 3. Conclusiones .....	116

## Capítulo VI

**EL ABUSO SEXUAL POR MEDIOS TELEMÁTICOS**

MACARENA ORTEGA

§ 1. Introducción .....	119
§ 2. El abuso sexual .....	120
a) Naturaleza jurídica .....	120
b) Acción típica .....	121
c) Cambio de paradigma .....	121
§ 3. El abuso sexual informático .....	122
a) Argumentos en contra .....	122
b) Argumentos a favor .....	123
c) Consideraciones personales .....	125
§ 4. El principio de legalidad .....	126
§ 5. Autoría mediata .....	128
§ 6. Jurisprudencia .....	128
§ 7. Conclusión .....	134

## Capítulo VII

**LA EFICACIA DEL HOSTIGAMIENTO DIGITAL EN EL PROCESO DE CONSTRUCCION DE VERDAD**

ROMINA ADRIANA QUEVEDO

§ 1. Introducción y estructura del trabajo .....	137
§ 2. ¿A qué llamamos verdad y qué valor le damos? .....	138
§ 3. La verdad en Foucault y la construcción del discurso .....	140
§ 4. La opinión pública: de la espiral del silencio al hostigamiento digital .....	142
a) La opinión pública .....	142
b) La espiral del silencio .....	143
§ 5. El hostigamiento digital .....	145
— ¿Por qué hay hostigamiento digital? .....	145

§ 6. El hostigamiento digital y el ciberodio .....	147
§ 7. El hostigamiento digital y la cultura de la cancelación .....	150
§ 8. Conclusión .....	152

## Capítulo VIII

**DIFUSIÓN NO CONSENTIDA DE MATERIAL SEXUAL PRIVADO  
CON FINES DIFAMATORIOS**

AGUSTÍN ARIEL CHALHUB

§ 1. Antecedentes: «sexting», «sextorsión» y la mal llamada «pornovenganza» .....	155
a) «Sexting» .....	155
b) «Sextorsión» .....	156
c) Difusión no consentida de material sexual privado con fines difamatorios .....	157
§ 2. Normativa vigente .....	161
§ 3. El antecedente del Código Penal español .....	161
§ 4. El Proyecto de Reforma al Código Penal. Modificación de los arts. 155 y 169 del Código Penal .....	162
a) El nuevo art. 155 .....	163
b) El nuevo art. 169 .....	164
§ 5. Cuestiones a analizar para la tipificación de las conductas .....	164
§ 6. Un supuesto que traerá aún más controversias .....	167
§ 7. Perspectiva de género en los tribunales .....	169
§ 8. Conclusión .....	172

## Capítulo IX

**ANÁLISIS POLÍTICO-CRIMINAL DEL CIBERFRAUDE BANCARIO  
Y PROPUESTA PARA UNA RESPUESTA PENAL ADECUADA  
EN LA REPÚBLICA ARGENTINA**

JUAN MANUEL SARRABAYROUSE

§ 1. La cuestión de los delitos informáticos en la actualidad .....	176
§ 2. El tratamiento de la ciberdelincuencia en el ordenamiento jurídico penal argentino .....	180
§ 3. Bases fundamentales para un análisis político-criminal de la ciberdelincuencia: el rol de las teorías de la pena y de la criminología .....	183
a) Las teorías de la pena como punto de partida de un análisis político-criminal .....	183
b) El principio de razonabilidad como herramienta de análisis de adecuación de la medida político-criminal .....	187
c) El análisis económico del Derecho y la necesidad de una base criminológica .....	190
d) Primera conclusión parcial: la estructura necesaria para un análisis político-criminal suficiente en torno al ciberfraude .....	193
§ 4. Las particularidades del ciberfraude bancario, su mayor gravedad y una necesaria referencia a su casuística .....	193
a) Características generales de los ciberdelitos y la mayor gravedad relativa del injusto .....	193

b) Características particulares del ciberfraude bancario y la necesidad de una mayor respuesta penal .....	197
c) Necesaria referencia a la fenomenología y casuística del ciberfraude bancario ..	199
1. Primer grupo de casos .....	199
2. Segundo grupo de casos .....	200
3. Tercer grupo de casos .....	201
4. Cuarto grupo de casos .....	202
5. Quinto grupo de casos .....	203
6. Patrones comunes en la técnica del ciberfraude bancario .....	203
d) Segunda conclusión parcial: la mayor gravedad relativa del ciberfraude bancario	204
§ 5. Análisis político-criminal del ciberfraude bancario .....	205
§ 6. Conclusión final: una concreta propuesta de adecuación político-criminal .....	205

## Capítulo X

**CIBERESTAFAS. ARGENTINA, UN ESTADO QUE FACILITA EL CIBERFRAUDE**

## DÉFICIT EN LOS SISTEMAS DE COMERCIALIZACIÓN DE ABONADOS DE TELEFONÍA CELULAR Y BILLETAS VIRTUALES

FERNANDO LUIS RIVAROLA

§ 1. Introducción .....	209
§ 2. La realidad digital. El ciberespacio .....	211
§ 3. Un caso: una matriz .....	214
— Flujo de dinero .....	216
§ 4. Responsabilidad del Estado. Obligaciones asumidas .....	218
a) Los abonados celulares como instrumentos de las ciberestafas .....	224
b) Regulación de la nominatividad de abonados celulares en Perú .....	231
c) La cuestión en la legislación española .....	233
d) Algunos cuestionamientos a la obligación de la nominatividad .....	236
§ 5. Las billeteras virtuales: La otra nueva herramienta que favorece la ciberdefraudación .....	238
§ 6. ¿Qué juez/a resulta competente? .....	244
§ 7. Conclusión .....	246

## Capítulo XI

**NUEVAS TECNOLOGÍAS Y EL CRIMEN ORGANIZADO: REGULACIÓN DE «BLOCKCHAIN» Y «CRIPTOMONEDAS»**

CARLOSA. LÓPEZ MENDOZA

§ 1. Introducción .....	249
§ 2. La tecnología de las criptomonedas .....	251

§ 3. «Blockchain» .....	253
a) Almacenamiento de datos en la cadena de bloques: estructura de datos de la cadena de bloques .....	254
b) Actualización de datos en la cadena de bloques: algoritmo de resonancia de nodo distribuido .....	255
c) Protección de datos en «blockchain»: criptografía .....	255
d) Manipulación de datos en «blockchain»: contratos inteligentes .....	255
§ 4. Regulaciones penales sobre delitos con criptomonedas .....	256
§ 5. La esencia de la moneda digital privada: moneda emitida sin autorización .....	257
a) Teoría de la mercancía virtual .....	258
b) Teoría de los valores .....	258
c) Teoría de los activos digitales .....	258
§ 6. La naturaleza monetaria de la moneda digital privada .....	259
§ 7. La necesidad de regulaciones penales para las criptomonedas .....	260
a) La moneda digital privada viola la soberanía de la moneda nacional .....	261
b) La moneda digital privada pone en peligro la seguridad nacional .....	262
c) El dilema real del sistema judicial penal para los delitos de moneda digital privada .....	263
§ 8. Supuestos legislativos sobre delitos donde se relacionan las criptomonedas .....	265
a) Eliminación de las restricciones al delito de falsificación de moneda mediante interpretaciones judiciales y reglamentos administrativos .....	266
b) Modificaciones al delito de tenencia y uso de moneda falsa .....	267
§ 9. Conclusión .....	267

## SEGUNDA PARTE

**DERECHO PROCESAL PENAL**

## Capítulo I

**LA DISPUTA DE LA PROTECCIÓN DE LOS DATOS PERSONALES EN LAS INVESTIGACIONES PENALES A LA LUZ DE UNA REDEFINICIÓN DE LA PRIVACIDAD**

## AMPARO ZAVALÍA

§ 1. Introducción .....	271
§ 2. Marco histórico y normativo desde sus orígenes hasta la actualidad .....	273
a) Contexto global y el modelo de sociedad .....	273
b) Europa: el derecho y los datos personales .....	274
c) Caso «Schrems» y la recomendación del Consejo .....	276
d) Estados Unidos .....	279
e) Argentina .....	283
§ 3. Alcances de los datos personales: ¿A qué llamamos datos personales? ¿qué estamos protegiendo? .....	285
a) Información: elementos y tipos de datos .....	285
b) Denominación de datos en una investigación .....	287

**ÍNDICE GENERAL**

15

c) El sentido de los datos personales en el siglo XXI. Protección y privacidad. Sociedad de consumo .....	289
§ 4. Tríada en datos personales: Empresas, Estado y Titulares de datos. Interrelación entre sus roles y responsabilidades .....	296
a) Empresas privadas y titulares de datos personales .....	296
1. Políticas de privacidad y consentimiento .....	297
2. Los alcances de los efectos adversos del almacenamiento y uso de datos y el desconocimiento generalizado de sus titulares .....	300
3. Opciones de los titulares .....	303
4. Concientización .....	305
b) Empresas privadas y Estado: privacidad «versus» persecución penal .....	307
1. Apple. Caso «San Bernardino», de 2016 .....	310
2. Whatsapp y su política de privacidad .....	310
3. Google .....	311
4. Twitter, Facebook y Trump .....	312
§ 5. Nuevo concepto de privacidad .....	314
§ 6. Reflexiones .....	316

## Capítulo II

**CONTRIBUCIÓN AL ESTUDIO  
DE PARAÍSO DIGITALES**

## EL «DETRÁS DE ESCENA» DE LAS REDES CIBERCRIMINALES

DENISE GROSS

§ 1. Introducción .....	320
§ 2. La búsqueda de una definición. Causas y variables .....	321
a) Desarrollo del concepto y determinación de sus límites .....	321
1. Definición de paraíso digital. ¿Un espacio físico y/o virtual? .....	321
2. Paraíso digital «versus» Paraíso fiscal .....	322
b) Variables susceptibles de afectar la prevención y represión del cibercrimen .....	323
1. Factores económicos .....	324
2. Factores jurídicos, ideológicos, geopolíticos y culturales .....	325
3. Un cúmulo de factores técnicos .....	327
§ 3. Fundamentos de la definición propuesta y su impacto .....	327
a) Paraíso digital como facilitador del cibercrimen .....	328
1. Durante la preparación del ciberataque y de su infraestructura .....	328
I. Servicios de comunicación .....	328
II. Infraestructura y herramientas de anonimización .....	330
2. Durante la monetización del ciberataque ejecutado .....	336
b) Paraíso digital como obstáculo en la lucha contra el cibercrimen .....	341
1. Ante la falta de armonización legislativa .....	341
2. Ante las dificultades en la cooperación internacional .....	347
§ 4. Conclusiones .....	351
§ 5. Anexos .....	352

## Capítulo III

**DESAPARICIÓN DE MUJERES Y FEMICIDIOS. ESTRATEGIAS DE INVESTIGACIÓN BASADAS EN LA EVIDENCIA DIGITAL**

AGUSTINA MARÍA ROMAIN

§ 1. Introducción .....	357
§ 2. Estándares Internacionales en materia de femicidios .....	359
§ 3. Ley 26.791: la figura del femicidio en el Código Penal .....	361
a) Elementos del tipo .....	363
1. Elementos subjetivos .....	363
I. Sujeto pasivo .....	363
II. Sujeto activo .....	363
2. Elemento objetivo: la existencia de violencia de género .....	363
b) El contexto violento: ¿qué buscamos para probar la violencia de género? .....	364
§ 4. Desapariciones de mujeres .....	365
§ 5. Directrices de la investigación .....	367
a) Protocolos y guías de actuación .....	367
b) Hipótesis delictivas .....	369
c) Trabajo interdisciplinario y comunicación .....	370
d) Selección de evidencia .....	370
1. Evidencia digital .....	370
2. Principio de libertad probatoria .....	371
3. Evidencia digital útil en femicidios y desaparición de mujeres .....	373
I. Investigación en fuentes abiertas (OSINT) .....	375
II. Cámaras de seguridad .....	377
III. Teléfonos celulares .....	378
III.1. Datos de titularidad .....	378
III.2. Datos de tráfico .....	379
a. Listados de llamadas .....	379
b. Celdas de activación y entrecruzamiento de llamadas .....	380
c. Historial de IMEI .....	380
d. Tráfico de datos .....	381
III.3. Datos de contenido .....	382
IV. Plataformas digitales .....	384
IV.1. Información de carácter público .....	385
IV.2. Información básica del suscriptor .....	387
IV.3. Información transaccional .....	388
IV.4. Información de contenido .....	388
IV.5. Preservación de la información .....	389
IV.6. Pedido emergencial .....	389
V. Correos electrónicos .....	390
V.1. Información de registración y logueo .....	390
V.2. Información de contenido .....	391
V.3. «E-mail header» .....	391
4. Cadena de custodia y cálculo «hash» .....	392
§ 6. Conclusiones .....	393

## Capítulo IV

**PRUEBA DIGITAL Y DELITOS EN CONTRA DE LA MUJER.  
DESAFÍOS EN LA PRÁCTICA PROCESAL**

VÍCTOR HUGO J. DÍAZ PÉREZ

§ 1. Introducción .....	395
§ 2. Materiales y métodos .....	397
§ 3. Estadísticas y carga procesal de los delitos en contra de la mujer .....	398
§ 4. Desafíos en la práctica procesal peruana .....	400
§ 5. ¿Prueba digital en juicio? .....	408
§ 6. Conclusiones .....	413

## Capítulo V

**EL AGENTE ENCUBIERTO EN EL CIBERESPACIO: LA AUSENCIA  
DE REGULACIÓN EN LA ARGENTINA Y SU IMPACTO  
EN LAS GARANTÍAS CONSTITUCIONALES**

ANTONELLA MARÍA BENTIN

§ 1. Introducción .....	415
§ 2. La figura del agente encubierto convencional en el ordenamiento jurídico argentino .....	416
— Regulación de la figura del agente encubierto en la ley 27.319 y el Código Procesal Penal Federal .....	417
§ 3. Infiltración del agente policial en el ciberespacio: grados de afectación en las garantías constitucionales .....	420
a) Nivel I: Ciberpatrullaje .....	420
b) Nivel II: Utilización de pseudónimos. Contactos previos. Expectativa razonable de privacidad .....	423
c) Nivel III: Agente encubierto Informático. Canales de comunicación cerrados. Autorización judicial. Autoincriminación .....	427
§ 4. Problemas de la aplicación analógica de la figura del agente encubierto convencional en el espacio cibernético .....	428
a) El requisito «organización criminal» o «asociación delictiva» .....	428
b) Intercambio de archivos ilícitos. Uso de inteligencia artificial. Agente provocador .....	434
c) Derecho de la defensa a interrogar al testigo de cargo - agente encubierto .....	439
§ 5. Conclusión .....	440

## Capítulo VI

**LOS ALLANAMIENTOS REMOTOS  
Y EL USO DE DRONES**

DIEGO STRATIOTIS

§ 1. Introducción .....	443
-------------------------	-----

§ 2. Algunos conceptos informáticos previos .....	444
a) Evidencia digital .....	444
b) Cadena de custodia .....	447
c) Copia forense «hash» .....	449
d) «Phishing» y programas espías o maliciosos («malware») .....	449
§ 3. Planteo del tema: investigaciones remotas y drones .....	450
§ 4. España: incorporación de medidas de investigación tecnológica .....	452
a) Principios generales de procedencia .....	452
b) Incorporación de los registros remotos .....	455
c) Acerca de la instalación de un «software». Programas maliciosos («malware») ..	457
§ 5. El registro remoto a través de drones .....	460
— Fases de acceso a la información .....	461
1. Crozono Explorer .....	461
2. Crozono Auditor .....	461
3. Crozono Forensic .....	462
§ 6. La autorización judicial de un registro remoto ¿cuáles son sus límites? .....	464
§ 7. Correo electrónico: ¿Datos de almacenado o comunicación? .....	466
§ 8. Los accesos remotos en la Argentina .....	469
a) Su incorporación .....	469
b) La libertad probatoria y los límites a la aplicación de institutos no previstos .....	472
§ 9. Conclusión .....	475

## Capítulo VII

### **VIDEOVIGILANCIA Y USO DE VANT EN EL MARCO DE INVESTIGACIONES PENALES EN LA ARGENTINA**

CECILIA LABANCA

§ 1. Introducción .....	477
§ 2. Preliminar. ¿De qué hablamos cuando hablamos de VANT? .....	478
§ 3. Contexto legal .....	479
§ 4. Videovigilancia y uso de VANT .....	481
§ 5. Utilización de VANT por las fuerzas de seguridad .....	483
§ 6. Necesidad de regulación procesal .....	486
§ 7. Sobre la posibilidad de utilización de VANT en el estado actual del arte .....	489
§ 8. Final. Ensayando una conclusión .....	490

## Capítulo VIII

### **TROYANO JUDICIAL**

¿VIOLACIÓN A LA PRIVACIDAD O ADECUACIÓN A LA MENSAJERÍA «INTELIGENTE»?

YAMILA VANESA ARRIAGA GONZÁLEZ

§ 1. Introducción .....	493
§ 2. Derechos en juego. Intimidación. Privacidad. Confidencialidad .....	494
§ 3. Troyano judicial. Nueva medida investigativa .....	498

**ÍNDICE GENERAL**

19

§ 4. Actualidad. Uso. Obstáculo .....	498
§ 5. Derechocomparado .....	500
a) España .....	500
b) Francia .....	502
c) Estados Unidos de América .....	503
d) Alemania .....	504
e) República Oriental del Uruguay .....	504
f) República Argentina .....	505
§ 6. Conclusiones finales .....	508

## Capítulo IX

**EL ESTUDIO AUTOMÁTICO DE LAS MICROEXPRESIONES FACIALES  
MEDIANTE EL USO DE TÉCNICAS DE INTELIGENCIA ARTIFICIAL  
APLICADO EN INVESTIGACIONES Y SEGURIDAD**

GABRIELA M. LAPADULA

§ 1. Introducción .....	511
§ 2. La inteligencia artificial (IA) .....	512
§ 3. Las microexpresiones faciales .....	513
§ 4. Paul Ekman y el estudio de las ME faciales .....	514
a) Sistema de codificación de acciones faciales («Facial Action Coding System - FACS») .....	515
b) ME, mentiras y detección del engaño .....	516
§ 5. La IA aplicada al estudio de las ME faciales .....	518
§ 6. Análisis automático de ME faciales .....	518
a) Bases de datos («Datasets») .....	519
b) Metodología .....	520
1. Detección .....	521
I. Pre-procesamiento .....	521
I.1. Detección y seguimiento de los puntos de referencia faciales .....	521
I.2. Registro de la cara .....	522
I.3. Enmascaramiento .....	523
I.4. Recuperación de la región de la cara .....	523
II. Detección de ME faciales .....	523
2. Reconocimiento .....	523
I. Pre-procesamiento .....	524
II. Representaciones .....	525
II.1. Basados en LBP .....	525
II.2. Basados en el flujo óptico .....	526
III. Clasificación .....	528
§ 7. Variantes en el análisis automático de ME .....	529
a) Características locales espaciotemporales .....	529
b) Aprendizaje del diccionario y codificación dispersa .....	529
c) Agrupación de características espaciotemporales .....	530
§ 8. Aplicación del análisis automático de ME en el ámbito de la seguridad de investigaciones .....	530
a) BioObserver .....	530

b) Vaakeye .....	531
c) Detección del engaño en videos .....	531
§ 9. Conclusiones. Consideraciones futuras .....	533

## Capítulo X

## ¿QUEREMOS A LA TECNOLOGÍA DE RECONOCIMIENTO FACIAL AL SERVICIO DE LA INVESTIGACIÓN PENAL?

MARÍA SOL CINOSI

§ 1. Introducción .....	535
§ 2. Los riesgos .....	536
§ 3. Los beneficios .....	538
§ 4. La situación en los Estados Unidos de América .....	539
§ 5. La situación en Europa .....	543
— El caso de España .....	544
§ 6. Doble revisión científica: Un juicio «ex ante» y un juicio «ex post» .....	561
§ 7. Ahora veremos el caso de la Argentina. ¿Se respeta este doble estándar? .....	563
§ 8. Desafíos procesales en la Argentina: ¿Medio de investigación o de prueba? .....	570
§ 9. Conclusión .....	573

## TERCERA PARTE

## INTELIGENCIA ARTIFICIAL Y NEUROCIENCIAS APLICADAS AL DERECHO PENAL Y PROCESAL PENAL

## Capítulo I

### INTELIGENCIA ARTIFICIAL AL SERVICIO DE LA HUMANIDAD

MARÍA AGUSTINA ZELIS LINARES

§ 1. Las máquinas comenzaron a pensar ... solo de manera diferente .....	577
§ 2. La nueva Humanidad habitando el ciberespacio .....	581
§ 3. Tarot del siglo XXI: «Data Science» .....	582
§ 4. Derecho a acceder al Ciberespacio de forma segura (DAFS). Nuestros derechos en la matrix .....	585
§ 5. La inteligencia artificial sesgada de humanidad .....	589
§ 6. Conclusiones .....	594

## Capítulo II

### INTELIGENCIA ARTIFICIAL. SU APLICACIÓN PRÁCTICA EN CASOS DE VIOLENCIA DE GÉNERO

ALEJANDRO A. TEMPORETTI OLIVERA

§ 1. Introducción .....	597
§ 2. Definiciones necesarias .....	599
§ 3. Antecedentes: la experiencia IA y género de IALAB .....	601

**ÍNDICE GENERAL**

21

§ 4. Análisis del caso testigo: femicidio de Úrsula Bahillo (pertinencias). Cuestiones previas al femicidio .....	602
§ 5. Medidas judiciales .....	603
§ 6. 18 Denuncias... o más .....	603
§ 7. El eterno tintinear de las víctimas .....	604
§ 8. Gestión de riesgos .....	605
§ 9. La IA como alternativa a la colaboración de la resolución de casos de violencia de género .....	605
§ 10. Problemática .....	605
a) Víctimas y sistema de denuncias .....	605
b) ¿Cuál es la causa por la que se reconocen víctimas de violencia? .....	606
§ 11. Revictimización institucional «versus» sesgos discriminatorios .....	607
§ 12. Problemática: multiplicidad de puertas de ingreso de denuncias .....	609
§ 13. Solución propuesta. IA predictiva y empática .....	610
§ 14. Solución propuesta. Hipótesis: Registro Único e Inteligente de denuncias por casos o situaciones de violencia de género .....	611
§ 15. Prueba anticipada .....	612
§ 16. Redes sociales: registros de manifestaciones de venganza, ciberacoso, «stalking», preexistentes en casos de violencia física o femicidio .....	613
§ 17. Auditoria del algoritmo .....	614
§ 18. Entrenamiento del sistema: cajas negras .....	614
§ 19. Reconocimiento de patrones. IA predictiva .....	615
§ 20. Detección precoz de violencia de género .....	615
§ 21. Conclusión .....	616

## Capítulo III

**«HACKEO» MENTAL**

## LOS «NEURODERECHOS» COMO MEDIO DE PROTECCIÓN FRENTE A LA MANIPULACIÓN CEREBRAL

DIANALIZETH PROAÑO AYALA

§ 1. Introducción .....	619
§ 2. Movimientos filosóficos .....	621
a) Consideraciones sobre el movimiento transhumanista .....	621
b) El movimiento posthumanista .....	622
§ 3. «The Internet of the Bodies» (IOB) .....	622
§ 4. El «hackeo» mental .....	624
§ 5. Los neuroderechos .....	629
§ 6. Conclusión .....	631

## Capítulo IV

**TECNOLOGÍAS APLICADAS A LA CIBERSEGURIDAD PARA EVITAR LA POSIBLE MANIPULACIÓN CEREBRAL**

SAMUEL ALBERTO SILVA VILLAGÓMEZ

§ 1. Introducción .....	636
-------------------------	-----

§ 2. Método .....	637
§ 3. Desarrollo .....	637
§ 4. El transhumanismo .....	643
§ 5. La manipulación psicológica .....	645
§ 6. El blindaje para la ciberseguridad .....	646
§ 7. «Blockchain» .....	647
§ 8. Seguridad del «blockchain» .....	647
§ 9. Privacidad diferencial .....	649
§ 10. Seguridad de la privacidad diferencial .....	649
§ 11. Conclusiones .....	650
<b>BIBLIOGRAFÍA GENERAL .....</b>	<b>653</b>