Índice General

Página

PRÓLOGO. LA DOGMÁTICA PENAL (Y SUS PROBLEMAS DE INVESTIGACIÓN) ANTE EL RETO DE LA IA .....
FERNANDO MIRÓ LLINARES 37

PARTE GENERAL

CAPÍTULO 1

REFLEXIONES SOBRE INTELIGENCIA ARTIFICIAL Y DERECHO PENAL: TRANSFORMACIONES, RIESGOS Y LÍMITES
MIGUEL ÁNGEL NÚÑEZ PAZ 45

I. Introducción 45
II. Marco conceptual de la Inteligencia Artificial en el Derecho penal 46
III. Aplicaciones de la Inteligencia Artificial en el proceso penal 49
IV. Riesgos y desafíos desde una perspectiva garantista 53
V. Necesidad de regulación y enfoque interdisciplinario 57
VI. Conclusiones 61
VII. Bibliografía 63

Página

CAPÍTULO 2

¿CULPABILIDAD SIN CULPABLE? EL DÉFICIT DE RESPONSABILIDAD EN LA IA AUTÓNOMA
IGNACIO F. BENÍTEZ ORTÚZAR. 67

I. Introducción 68
II. Del instrumento al agente tecnológico 70
III. La distinción entre IA previsible e IA autónoma 73
IV. La imputación objetiva como primer filtro 74
V. La culpabilidad como límite frente a la responsabilidad objetiva 75
VI. Formas que podrían plantearse para atribuir responsabilidad penal al sujeto por el hecho cometido por la IA generativa 76
1. La autoría mediata y sus límites 76
2. Comisión por omisión y posición de garante 77
3. Inteligencia artificial, productos defectuosos y deberes de prevención 78
4. Compliance en la IA y responsabilidad penal de la persona jurídica 79
5. La «personalidad electrónica» 80
6. Otras propuestas doctrinales 81
7. Toma de posición. principio de precaución IA y culpabilidad jurídico penal 82
VII. Una nueva arquitectura de imputación subjetiva 83
VIII. Compliance y responsabilidad penal 84
IX. Justicia algorítmica y principio de culpabilidad 85
1. De la IA que actúa a la IA que decide sobre quién actúa 85
2. La llamada «justicia algorítmica» 86
3. Sesgo algorítmico e imposibilidad de automatizar la culpabilidad 86
4. Supervisión humana y sesgo de automatización 87

Página

X. Distintas formas de afrontar la regulación global de la IA que, sin duda, van a afectar a la determinación de la culpabilidad penal 88
1. El debate acerca de la autoregulación 88
2. Autorregulación y corregulación 88
3. El modelo europeo: regulación basada en el riesgo 89
4. El modelo estadounidense: estándares, sectores y gestión del riesgo 90
5. El modelo chino: intervención administrativa y gobernanza del algoritmo 90
6. Tres modelos y una misma pregunta penal 91
XI. A modo de conclusión. La doble paradoja: culpabilidad sin culpable y responsabilidad sin control 92
XII. Bibliografía 94

CAPÍTULO 3

COAUTORÍA HUMANO-MÁQUINA: ¿UN OXÍMORON JURÍDICO? LA ASINCRONÍA COMO LÍMITE DE LA IMPUTACIÓN RECÍPROCA
ALFREDO ABADÍAS SELMA 99

I. Introducción: planteamiento de una cuestión poco transitada 100
1. El estado de la cuestión: el predominio de la autoría mediata 101
2. Hipótesis, método y delimitación del objeto 103
II. Los presupuestos de la coautoría y su base antropológica. 103
1. La decisión común como vínculo subjetivo 104
2. El codominio funcional y la aportación esencial en fase ejecutiva 105
3. La imputación recíproca 106
A) Su fundamento: el otro ha de poder ser portador de injusto 106
B) El precedente de la persona jurídica y su valor limitado como analogía 106

Página

III. La máquina ante el test de la coautoría 108

1. Sujeto, objeto o «actuante»: la insuficiencia del modelo bipartito 108

2. Decisión racional autónoma: lo que la máquina sí hace 110

A) Objetivos, fines y decisiones no programadas 110

B) La opacidad sobrevenida y la caja negra causal 111

3. Lo que la máquina no puede hacer: ser destinataria de la imputación recíproca 112

IV. La asincronía como verdadero obstáculo 114

1. El acuerdo desplazado: programar como pacto anticipado y en abstracto 114

A) Tres asimetrías: tiempo, información y objeto de la decisión 115

B) El código de instrucciones como código de conducta. 115

2. La ejecución sin el otro presente: dilución del codominio 116

3. ¿Es concebible una coautoría diacrónica? 117

4. El exceso del «coautor»: aprendizaje autónomo y ruptura del plan común 118

V. Cinco escenarios de contraste 119

1. IA débil: autoría directa con instrumento sofisticado 119

2. Vehículos autónomos y situaciones de necesidad: la ponderación programada 120

A) Por qué el dilema del tranvía no es una decisión conjunta 120

B) Causas de justificación que presuponen situación y no pueden preconfigurarse 121

3. El AI Trader y la manipulación de mercado: el caso más próximo a la coautoría 121

4. Sistemas multiagente sin humano identificable 122

5. IA fuerte: la laguna y la tentación de la responsabilidad objetiva 123

VI. Lo que el oxímoron revela 124

Página

1. La reciprocidad como último reducto del principio de culpabilidad 124
2. Programar es legislar: la privatización de la regla de conflicto 124
3. Reserva de ley, taxatividad y códigos éticos privados 125
4. El Reglamento Europeo de IA: control humano como dogma y como coartada 126
VII. Propuesta: de la coautoría a la autoría por configuración . 128
1. Autoría accesoria, comisión por omisión y posición de garante en la cadena de valor 128
2. El injusto de organización como alternativa 130
3. Límites infranqueables: prohibición de responsabilidad objetiva 131
4. ¿Sigue haciendo falta la «persona electrónica»? 133
VIII. Conclusiones: el coautor que llegó tarde 134
IX. Bibliografía 137
X. Legislación 139
XI. Jurisprudencia 140

CAPÍTULO 4

LA POSICIÓN DE GARANTE DE LA EMPRESA DE IA POR DOMINIO ALGORÍTMICO DEL RIESGO. LÍMITES DESDE LA DOGMÁTICA PENAL
LUIS CARRANZA FIGÓN 141

I. Introducción 141
II. Del riesgo tecnológico al riesgo penalmente relevante en los sistemas generativos 143
III. De la creación del riesgo al dominio sobre la fuente algorítmica 145
IV. La equivalencia entre omisión y acción en el ámbito de la organización empresarial 147
V. El deber de intervención ante la progresiva concreción del riesgo 149

Página

VI. Formulación de la posición de garante por dominio algorítmico del riesgo 154

VII. Conclusiones 159

VIII. Bibliografía 159

CAPÍTULO 5

EL TIPO SUBJETIVO EN LOS DELITOS COMETIDOS MEDIANTE IA: CONOCIMIENTO, VOLUNTAD Y ALGORITMOS

LUIS GARCÍA-PARRA POMARES 161

I. Introducción 161

II. Análisis crítico sobre la atribución de personalidad jurídica y responsabilidad penal a las IA 164

1. Concepto y límites de la IA actual: ausencia de autonomía ontológica y subordinación al ser humano 164

2. Análisis crítico sobre la viabilidad de conceder personalidad jurídica a la IA mediante una ficción legal 165

A) Exposición general de los argumentos dogmáticos existentes para la superación de los obstáculos a la concesión de personalidad jurídica a la IA y conclusión sobre su inviabilidad 165

B) Crítica a la asimilación entre empresa e IA: inaplicabilidad a la IA de la misma teoría para la atribución de personalidad jurídica y responsabilidad penal a la empresa 167

C) Resoluciones de la Unión Europea sobre la inaplicabilidad ontológica y moral de personalidad jurídica a la IA 168

III. Atribución de responsabilidad penal individual por actos cometidos por o mediante IA: aplicación de las instituciones clásicas de la dogmática penal 169

IV. Dolo eventual, error de tipo e ignorancia deliberada: delegación de funciones en la IA 175

V. Conclusiones 178

VI. Bibliografía 180

Página

CAPÍTULO 6

LA CRISIS DEL PARADIGMA ANTROPOCÉNTRICO DE LA ACCIÓN EN EL SISTEMA PENAL: ¿HACIA UNA ACCIÓN ROBÓTICA?
MIGUEL BUSTOS RUBIO 185

I. Introducción 185

II. Algo de historia: el concepto clásico de acción y su fundamento antropocéntrico 187

III. La primera ruptura del paradigma: la responsabilidad penal de las personas jurídicas 193

IV. Inteligencia artificial y crisis de las categorías tradicionales de imputación penal 195

V. *¿Machina delinquere et puniri potest?* El debate sobre la atribución de una personalidad robótica y sobre la responsabilidad penal de la IA 198

VI. Volviendo a la acción penalmente relevante: toma de postura 209

VII. Bibliografía 210

PARTE ESPECIAL

CAPÍTULO 7

LA SUPLANTACIÓN DE IDENTIDAD MEDIANTE INTELIGENCIA ARTIFICIAL GENERATIVA: REGULACIÓN PENAL VIGENTE Y PROPUESTA DE REFORMA
ESTEBAN MESTRE DELGADO 215

I. La resistible ascensión de la inteligencia artificial generativa como instrumento para la suplantación de identidad 216

II. Previsiones penales vigentes frente a la suplantación o la manipulación de la identidad (propia o ajena) 222

1. Delitos en cuyo reproche se integra la asunción de una identidad ajena 223

A) La usurpación del estado civil 223

Página

B) La utilización de la imagen u otros datos ajenos con finalidad coactiva 224

C) La manipulación de rasgos o datos concretos de la identidad del sujeto activo para engañar a un tercero 225

D) La simulación de autoridad o función pública en la ejecución de los delitos de detención ilegal y secuestro 227

E) La consideración de la falsa identidad como falsedad documental 227

2. La ambivalencia funcional del camuflaje de la propia identidad en la agravante de disfraz 229

III. Insuficiencias de la regulación penal vigente frente a las nuevas formas de suplantación o manipulación de la identidad (propia o ajena) 230

IV. Elementos para la configuración del nuevo delito de suplantación de identidad 233

V. Redacción que se propone 235

VI. Bibliografía 235

CAPÍTULO 8

VEHÍCULOS AUTÓNOMOS Y DELITOS CONTRA LA VIDA Y LA INTEGRIDAD FÍSICA: EL FABRICANTE ANTE LA IMPUTACIÓN DE RESULTADOS LESIVOS

ISIDORO BLANCO CORDERO 237

I. Introducción 237

II. Niveles de automatización y marco teórico 238

III. Responsabilidad penal en el nivel 3 (intervención humana subsidiaria) 240

1. Los deberes de cuidado del fabricante 240

2. Los deberes de cuidado del conductor 241

3. Previsibilidad, omisión y posición de garante del conductor .. 242

4. La concurrencia de imprudencias entre conductor y fabricante 243

Página

IV. La automatización plena: la responsabilidad penal por el producto 244
1. La relación de causalidad y la inteligencia artificial 244
V. Las fuentes del deber de cuidado y el riesgo permitido . . . 245
1. La determinación escalonada y los criterios de ponderación . . 248
2. El principio de confianza 250
VI. La previsibilidad del resultado y la opacidad tecnológica . 250
VII. La realización del riesgo en el resultado y el nexo de antijuridicidad 251
VIII. Deberes tras la puesta en circulación y comisión por omisión 253
IX. El sujeto responsable y el problema de las muchas manos 254
X. Perspectivas *de lege ferenda* y conclusiones 255
XI. Bibliografía 256

CAPÍTULO 9

INTELIGENCIA ARTIFICIAL GENERATIVA COMO MULTIPLICADOR DEL RIESGO DEFRAUDATORIO: SUFICIENCIA Y PRUEBA DEL ENGAÑO EN EL DELITO DE ESTAFA
MARTA CARRERA TORNER 259

I. Introducción: la estafa en la era de la inteligencia artificial generativa 259
II. La inteligencia artificial generativa como herramienta de intensificación del riesgo defraudatorio 264
1. De la estafa tradicional a la estafa tecnológicamente asistida . 265
2. Delimitación respecto de la estafa informática 267
3. Nuevas formas de construcción del engaño: phishing hiperpersonalizado, clonación de voz, deepfakes, chatbots, fraude sentimental y suplantación de identidad 269
III. El engaño bastante ante la inteligencia artificial generativa 273
1. Suficiencia e idoneidad: criterios objetivo-subjetivos 275

Página

IV. La prueba del engaño generado mediante inteligencia artificial 278
1. La paradoja probatoria de la IA 278
2. Pericial informática, trazabilidad y cadena de custodia 280
V. Consideraciones finales 283
VI. Bibliografía 284

CAPÍTULO 10

ESTAFAS Y *FRAUD AS-A-SERVICE*: DE LA IA GENERATIVA COMO HERRAMIENTA A LA IA GENERATIVA COMO AGENTE DEFRAUDATORIO E INDUSTRIALIZADOR
ANA MARÍA PRIETO DEL PINO 287

I. Contexto estructural: IA generativa unimodal, multimodal con *Transformer* e IA agente como herramientas en los delitos de estafa 288
II. Contra el sesgo holístico en el análisis de la IA generativa: de la especulación teórica al estudio fragmentado de la estafa 290
III. La evolución de la IA generativa y su incidencia en las estafas basadas en códigos maliciosos (*malware*) 292
1. ¿Qué aportan la IA multimodal y la IA agente al malware o código malicioso? 292
2. El papel de la IA generativa en las estafas informáticas con empleo de malware (art. 249 CP) 295
A) La evolución de los troyanos bancarios y el *malware-as-a-service* 295
B) La optimización de *webskimmers* 296
C) Los drenadores de carteras de criptomonedas (*crypto drainers*) 296
D) La redirección fraudulenta (*malicious adware*) 297
3. El papel de la IA generativa en la estafa con engaño bastante mediante empleo de malware (art. 248): scareware y estafa de falso soporte técnico 297

Página

IV. Las estafas mediante contenidos de simulación sintética hiperrealista (*deepfakes*) 298

1. La evolución de la simulación sintética hiperrealista 298

2. El denominado deepfake as-a-service: los contenidos sintéticos de simulación hiperrealistas como producto asequible en la dark web 300

3. Estafas con engaño bastante mediante contenidos sintéticos de simulación hiperrealistas (art. 248 CP) 301

A) Estafas con suplantación de una persona mediante clonación de voz (*voice spoofing*) 301

B) Estafas mediante suplantación *ad hoc* de personas en medios audiovisuales 302

C) La actualización de estafas con engaño bastante 303

4. Estafas informáticas mediante contenidos sintéticos de simulación hiperrealistas (art. 249 CP) 304

A) El fraude de arbitraje de devoluciones en comercio electrónico (*refund scams*) 304

B) Estafas mediante identidades sintéticas 304

C) Estafas informáticas de suplantación de otra persona eludiendo sistemas de verificación biométrica mediante inyección de vídeo. 306

V. La automatización de estafas «tradicionales» mediante IA multimodal con tecnología *Transformer* 307

1. La automatización de las estafas con engaño bastante 307

A) La aportación de la IA multimodal con *Transformer* al engaño bastante 307

B) Fraude BEC evolucionado (*Business Email Compromise*) 307

C) Estafas de falsas ofertas de empleo (*Employment Scams*). 308

D) Estafas sentimentales (*dating/love scams*) y otras semejantes 308

2. La automatización de la estafas informáticas (art. 249 CP): especial consideración del phishing y el phishing as-a-service 309

Página

VI. El avance más reciente: la automatización dinámica de las estafas mediante IA agente 310

1. Los agentes de IA defraudatorios basados en IA agente o autónoma 310

2. La IA agente en las estafas con engaño bastante: ciberestafas sentimentales y otras similares 311

3. La IA agente en las estafas informáticas: phishing totalmente automatizado 312

VII. Una reflexión final sobre el *phishing* bancario optimizado con IA: de la sofisticación tecnológica al ilícito mercantil *de facto* 312

VIII. Bibliografía 313

CAPÍTULO 11

LA DESINFORMACIÓN EN EL MERCADO DE VALORES DEL SIGLO XXI: REDES SOCIALES, *FINFLUENCERS* E INTELIGENCIA ARTIFICIAL

DANIEL TEJADA PLANA 321

I. (Des)información y mercado de valores: consideraciones iniciales 321

II. De las Guerras Napoleónicas a los *deepfakes*: las nuevas manipulaciones informativas en los mercados de valores de hoy en día 327

III. Los efectos de las noticias falsas en los mercados. Externalidades negativas y dinámicas de difusión de la información falsa 330

IV. Redes sociales, *finfluencers* y mercados de valores: nuevos riesgos para la integridad del mercado 333

1. Los influencers financieros (finfluencers) y su impacto en el mercado de valores 337

2. Mercados de valores y conflictos de interés: los supuestos de scalping 342

3. Ejemplos de manipulaciones de mercado y redes sociales 347

A) Elon Musk y las manipulaciones en Twitter y Tesla 347

B) El caso Grifols en España 348

Página

V. Inteligencia artificial y desinformación: la afectación a la integridad financiera a través de los *deepfakes* 350

VI. Bibliografía 358

CAPÍTULO 12

LA INTERVENCIÓN DEL DERECHO PENAL FRENTE AL DESMEDIDO CONTROL ALGORÍTMICO DE LA ACTIVIDAD LABORAL

CARLOS EMILIO DEL CACHO ESTIL-LES 365

I. Introducción 365

II. Algoritmos de gestión laboral 367

1. La dignidad del trabajador como límite 368

2. El látigo digital 374

III. La relevancia penal de la hostilidad algorítmica 376

1. El análisis del tipo del art. 173.1 del CP 376

2. Hostilidad algorítmica como acoso 378

3. Atribución del hecho al empresario 381

IV. Bibliografía 386

CAPÍTULO 13

DESINFORMACIÓN, MANIPULACIÓN DEMOCRÁTICA Y DELITOS ELECTORALES POTENCIADOS POR IA

DANIEL GONZÁLEZ URIEL. 389

I. Introducción 389

II. Campañas de desinformación automatizada, *microtargeting* electoral y *deepfakes* políticos: su incidencia penal . . 391

1. El concepto de desinformación 391

2. Los riesgos y las amenazas de la desinformación para los sistemas democráticos 393

3. El impacto de la IA en los derechos fundamentales 396

4. La desinformación desde la vertiente penal 399

Página

5. Los procesos electorales y la influencia de la desinformación y de las herramientas de IA 405

III. A modo de reflexiones finales 411

IV. Bibliografía 414

CAPÍTULO 14

IA Y DELITOS CONTRA LA LIBERTAD SEXUAL: NUEVAS MODALIDADES COMISIVAS

DIEGO ALBERTO GUTIÉRREZ AZANZA 419

I. Introducción 419

II. *Grooming* mediante *chatbots* e identidades sintéticas 422

1. Breve referencia a los elementos del tipo de child grooming 422

2. Grooming mediante chatbots e identidades sintéticas 426

III. La persistencia en el ataque a la libertad: el acoso automatizado 431

1. La afectación persistente a la libertad con el uso de chatbots 431

2. Breve referencia a los elementos de los delitos de acoso 432

3. Acoso mediante chatbots o identidades sintéticas 435

IV. Bibliografía 437

CAPÍTULO 15

MENORES E INTELIGENCIA ARTIFICIAL (IA): RESPONSABILIDAD PENAL JUVENIL EN EL ENTORNO DIGITAL

JUAN JOSÉ PERIAGO MORANT 441

I. Introducción: la intersección entre inteligencia artificial, menores y Derecho penal 441

1. Delimitación conceptual: los deepfakes como técnica de síntesis de imagen y sonido mediante IA generativa 443

2. El fenómeno del «porno de venganza» y el hostigamiento digital entre menores: un reto para la LORPM 446

A) De los deepfakes al *revenge porn* 446

B) El uso de las nuevas tecnologías: un reto para la LORPM 450

Página

II. La tipicidad de los *deepfakes* sexuales 451
III. La actual respuesta que proporciona la Ley Orgánica 5/2000 reguladora de la responsabilidad penal de los menores 457
IV. *Deepfakes*: la propuesta del proyecto de Ley Orgánica para la protección de las personas menores de edad en los entornos digitales 460
V. El delito de ultrafalsificaciones del art. 173 bis del Código penal 461
VI. Bibliografía 464

CAPÍTULO 16

EL CONFLICTO ENTRE EL DERECHO A LA PRIVACIDAD E INTIMIDAD DE LOS MENORES DE EDAD EN EL ENTORNO DIGITAL Y EL CONTROL PARENTAL. REPERCUSIONES EN EL DERECHO PENAL
CARLOS VÁZQUEZ GONZÁLEZ 467

I. Introducción 468
II. Protección de los menores en internet. Entornos digitales seguros para los menores de edad. El control parental 470
III. Derecho a la privacidad e intimidad de los menores de edad 472
IV. Conflictos entre el control de los padres sobre sus hijos en internet y su derecho a la intimidad y privacidad. El principio del interés superior del menor 474
V. Intervención del Código Penal. Los delitos de descubrimiento y revelación de secretos 476
VI. Cuando se exceden los límites del control parental y se vulnera el derecho a la intimidad del menor. Delitos de descubrimiento y revelación de secretos en el ámbito familiar 478
1. Resoluciones a favor del derecho a la intimidad del menor 478
2. Resoluciones a favor del deber de protección de los padres 480
3. Resoluciones controvertidas 481

Página

VII. Conclusiones 483

VIII. Bibliografía 487

CAPÍTULO 17

EL PROYECTO DE LEY ESPAÑOL DE PROTECCIÓN DE MENORES EN EL ENTORNO DIGITAL: ANÁLISIS CRÍTICO DE LA REFORMA PENAL

DEBORAH GARCÍA MAGNA 489

I. Introducción 489

II. Una regulación transversal para abordar una cuestión multifacética 493

III. Análisis de los aspectos más relevantes de la reforma penal 496

1. Modificaciones de la parte general del Código penal: alejamiento de entornos digitales e inhabilitación especial para actividades en espacios virtuales 499

2. Modificaciones de la parte especial del Código penal: ultrafalsificaciones, ampliación del delito de exhibición de pornografía y agravante específica de enmascaramiento de identidad . 503

A) El nuevo delito contra la integridad moral del art. 173 bis 503

B) La ampliación del delito de exhibición de material pornográfico 506

C) La agravación de enmascaramiento de identidad en entornos digitales 508

IV. Conclusiones 510

V. Bibliografía 511

CAPÍTULO 18

FRAUDE PATRIMONIAL Y SUPLANTACIÓN DE IDENTIDAD MEDIANTE INTELIGENCIA ARTIFICIAL EN BRASIL

IZABEL RIGO PORTOCARRERO 513

I. Introducción 513

Página

II. El fenómeno y su relevancia penal 515
1. Manifestaciones consideradas en la investigación 515
2. Elementos comunes con relevancia jurídica 516
III. La respuesta penal vigente 517
1. El fraude patrimonial mediante contenido sintético 517
A) El tipo básico y el fraude electrónico 517
B) El deslinde con el hurto mediante fraude electrónico 518
2. La suplantación de identidad y los límites de los tipos vigentes 520
3. El empleo de inteligencia artificial como circunstancia 523
IV. Gobernanza digital y prevención del fraude 523
1. La protección de los datos personales 523
2. La prevención en el sistema financiero 524
3. La responsabilidad de las plataformas 525
4. La regulación del contenido sintético 527
V. Prueba y proceso 528
1. La autenticidad y la cadena de custodia 528
2. La pericia y la valoración del contenido 530
3. La atribución de autoría y el acceso a los registros 531
4. La competencia territorial 532
VI. Valoración crítica y propuestas de reforma 532
1. Los límites de una agravación basada en la inteligencia artificial 532
2. La protección penal de la identidad personal 533
3. La prioridad de la prevención y la trazabilidad 534
VII. Conclusiones 535
VIII. Bibliografía 536
1. Doctrina 536
2. Legislación y documentos oficiales 538
3. Jurisprudencia 539

Página

CONSECUENCIAS JURÍDICAS, COMPLIANCE, PROCESO PENAL Y PROPUESTAS DE REFORMA

CAPÍTULO 19

PENAS APLICABLES A LAS PERSONAS JURÍDICAS POR DELITOS DE SUS SISTEMAS DE IA. FUNDAMENTOS DOGMÁTICOS Y LEGISLATIVOS
JUAN ANTONIO MARTOS NÚÑEZ 543

I. Introducción 543

II. Fundamento de la responsabilidad penal de las personas jurídicas 544

1. Autorresponsabilidad 544

2. Heterorresponsabilidad o vicarial 545

III. El artículo 31 bis del Código penal 546

IV. Inteligencia artificial generativa de delitos ambientales 549

V. Penas aplicables a las personas jurídicas por delitos de sus sistemas de IA 556

VI. Bibliografía 561

CAPÍTULO 20

LA SEGURIDAD DEL FUTURO: DE LA POLICÍA PREDICTIVA A LA PUNTUACIÓN SOCIAL
MOISÉS BARRIO ANDRÉS 563

I. Introducción 563

II. Inteligencia artificial y control social 566

III. Principales problemas e interrogantes 568

1. Identificación de riesgos 568

2. Evaluación de riesgos 570

3. Gestión de riesgos 571

IV. La seguridad del futuro 572

1. Nuevas amenazas para la seguridad del futuro 573

Página

2. Cómo abordar las perturbaciones de la seguridad en el futuro 574

V. Conclusiones 575

VI. Bibliografía 577

CAPÍTULO 21

DE LA DELEGACIÓN ALGORÍTMICA AL DEFECTO DE ORGANIZACIÓN: GOBERNANZA DE LA INTELIGENCIA ARTIFICIAL EN EL ÓRGANO DE ADMINISTRACIÓN Y RESPONSABILIDAD PENAL POR DELITOS CONTRA EL MEDIO AMBIENTE

GEMA MARTÍNEZ GALINDO 579

I. Introducción 580

II. La implementación de la inteligencia artificial para la toma de decisiones en el órgano de administración 583

III. El fallo de la delegación algorítmica: defecto de organización y responsabilidad penal por delitos contra el medio ambiente 587

1. El modelo del art. 31 bis CP ante la decisión algorítmica 587

2. Los delitos contra el medio ambiente: el greenwashing algorítmico y el «escudo algorítmico» frente a la imputación penal . . 591

IV. La gobernanza algorítmica como estándar de diligencia debida 595

1. La creación de una debida diligencia algorítmica 595

2. El marco europeo como parámetro de idoneidad del modelo: Reglamento de IA, Directiva (UE) 2024/1203 y diligencia debida en sostenibilidad 600

V. Bibliografía 602

CAPÍTULO 22

***NON BIS IN IDEM* E INTELIGENCIA ARTIFICIAL EN LOS DELITOS CORPORATIVOS**

CARLOS MANUEL CUEVAS OLTRA 607

I. Introducción 607

II. El principio de *non bis in idem* 608

Página

III. El régimen sancionador del RIAUE en concurrencia con la responsabilidad penal corporativa en España 612

1. La responsabilidad penal de las personas jurídicas y el bis in idem 612

2. El régimen sancionador en el reglamento 617

3. Posibilidades de bis in idem 624

A) Delito de estafa 626

B) Aprovechamiento de la vulnerabilidad de la víctima como elemento típico o como agravante 627

C) Delito de odio 628

D) Delito contra la intimidad 629

E) Pornografía infantil 630

IV. Conclusiones 632

V. Bibliografía 633

CAPÍTULO 23

PROGRAMAS DE CUMPLIMIENTO NORMATIVO PARA SISTEMAS DE INTELIGENCIA ARTIFICIAL Y PREVENCIÓN DEL RIESGO PENAL EN LA SOCIEDAD ALGORÍTMICA

MARIO EDUARDO MALDONADO SMITH 637

I. Introducción 637

II. La sociedad algorítmica y sus implicaciones en el ámbito penal 640

III. Algunos casos ejemplificativos asociados a sistemas algorítmicos 644

IV. Marco normativo europeo aplicable a los sistemas de inteligencia artificial 647

V. Eventual responsabilidad de los integrantes de la empresa y de la persona jurídica 649

VI. Programas de cumplimiento para sistemas de IA 652

VII. Bibliografía 657

Página

CAPÍTULO 24

IA APLICADA AL COMPLIANCE PENAL EN EL ECOSISTEMA *BLOCKCHAIN* (TRANSACCIONES CON CRIPTOACTIVOS)
JAVIER LÓPEZ ANDREO, MANUEL MARÍN MARTÍNEZ 661

I. El marco regulatorio penal del compliance cripto y la necesidad de herramientas de IA 662

1. La insuficiencia de los mecanismos tradicionales de detección del fraude en el ecosistema blockchain 662

2. El Reglamento MiCA y la configuración de un marco regulatorio europeo para los criptoactivos 664

3. Divergencia regulatoria global: modelos de supervisión de la IA en el ámbito financiero 665

4. La necesidad de herramientas de IA como instrumento del compliance penal 666

II. Metodologías de IA para la detección de fraude cripto: *Machine Learning, Deep Learning*, NLP e IA generativa como instrumentos del compliance penal 667

1. Panorama general: la redefinición de las estrategias de compliance mediante la inteligencia artificial 667

2. Machine Learning: monitorización de transacciones y detección de anomalías 668

3. Deep Learning y redes neuronales basadas en grafos: reconocimiento de patrones complejos de fraude 669

4. Procesamiento del Lenguaje Natural (NLP): análisis de comunicaciones y due diligence reforzada 671

5. IA generativa: simulación de escenarios y datos sintéticos como herramienta proactiva del compliance 672

6. Retos transversales y perspectivas de futuro 673

III. Desafíos jurídico-penales: opacidad algorítmica, fragmentación regulatoria y validez probatoria de la IA en la detección de fraude cripto 674

1. La opacidad algorítmica como obstáculo para el compliance penal: el problema de la caja negra 674

Página

2. La fragmentación regulatoria global: un mosaico normativo para los sistemas de compliance basados en IA 676
3. La calidad y accesibilidad de los datos: una barrera para la eficacia probatoria de los sistemas de IA 677
4. La insuficiencia de la evidencia empírica sobre la eficacia real de los sistemas de IA en el compliance 678
5. Desafíos éticos y asimetría de recursos: la brecha digital en el compliance penal 679
6. La evolución de las tácticas delictivas y la necesidad de adaptación continua de los sistemas de IA 680
IV. Conclusiones 681
V. Bibliografía 682

CAPÍTULO 25

HERRAMIENTAS ALGORÍTMICAS DE EVALUACIÓN DEL RIESGO EN JUSTICIA PENAL: ANÁLISIS COMPARADO DE LOS PRINCIPALES SISTEMAS Y APLICABILIDAD EN EL CONTEXTO EUROPEO
ALBERTO DE NOVA LABIÁN 685

I. Introducción 685
II. Principales herramientas algorítmicas 688
1. Sistema LSI-R 688
2. Sistema compas 691
3. Sistema PSA 695
III. Aplicabilidad de herramientas algorítmicas en el ámbito europeo 699
1. Implementación de los principales sistemas norteamericanos 699
2. Sistemas europeos 701
3. Pronunciamientos judiciales 705
IV. Bibliografía 708

Página

CAPÍTULO 26

INTELIGENCIA ARTIFICIAL Y RESPONSABILIDAD PENAL: CATEGORÍAS Y GARANTÍAS EN LA SOCIEDAD ALGORÍTMICA
DANIEL MONTESDEOCA RODRÍGUEZ 715

I. Introducción: la sociedad algorítmica como nuevo marco de la política criminal 716

II. Delimitación conceptual de la inteligencia artificial, autonomía y opacidad algorítmica 717

1. Delimitación conceptual de la inteligencia artificial 717

2. Niveles de autonomía y supervisión humana 718

3. Opacidad y explicabilidad 719

4. Modalidades de aprendizaje y relevancia jurídico-penal 720

5. Modelos de IA de uso general 721

III. Cuestiones dogmáticas ante la intervención de sistemas de IA 721

1. Causalidad e imputación objetiva 721

2. Deber objetivo de cuidado y principio de confianza 722

3. Dolo eventual e imprudencia consciente 722

4. Autoría y participación ante la intervención de sistemas de IA 723

A) La intervención del desarrollador y del proveedor del sistema 724

B) La intervención del proveedor 724

C) La intervención del responsable del despliegue y del usuario 725

IV. Responsabilidad penal de las personas jurídicas y sistemas de inteligencia artificial 726

1. Integración de los riesgos asociados a la IA en los modelos de cumplimiento normativo 726

2. La supervisión humana en los modelos de cumplimiento normativo 727

Página

3. Organización de las funciones de supervisión y cumplimiento en materia de IA 727

V. La inteligencia artificial como posible sujeto de responsabilidad penal 728

VI. Inteligencia artificial y nuevas formas de criminalidad ... 729

1. Deepfakes y contenidos sintéticos 729

2. Sesgos algorítmicos y límites de la respuesta penal frente a la discriminación 731

3. Criminalidad patrimonial y ciberdelincuencia facilitadas por IA 731

4. Utilización de sistemas de IA en la manipulación de mercados 732

5. Tratamiento de datos mediante IA y tutela penal de la intimidad 732

6. Identificación biométrica y reconocimiento de emociones 732

VII. La construcción de un marco jurídico europeo para la inteligencia artificial 733

1. El Reglamento (UE) 2024/1689 y la evaluación del riesgo delictivo 733

2. El Convenio Marco del Consejo de Europa 733

3. Régimen sancionador y Derecho penal 733

VIII. Conclusión 734

IX. Bibliografía 735

CAPÍTULO 27

LA PRUEBA DEL *DEEPFAKE* GENERADO O MANIPULADO POR IA EN EL PROCESO PENAL
MIGUEL ÁNGEL LÓPEZ MARCHENA 737

I. Introducción 737

II. Normativa sobre *deepfake* 741

1. Normativa comunitaria y del Consejo de Europa 741

2. Normativa interna 743

III. Supuestos de *deepfakes* 744

Página

1. Deepfakes encuadrados en actividades legales 744
2. Deepfakes y criminalidad 746
A) Difamación de inocentes con la finalidad de desacreditarlos o incluso preparar pruebas falsas 746
B) Recopilación, intercambio y difusión de datos personales 747
C) Infracciones contra la propiedad intelectual y artística 747
D) Propagación de información errónea en procesos electorales 748
E) Fraude financiero, bancario y suplantaciones de personalidad 748
F) *Deepfakes* de contenido sexual y ciberviolencia 749
IV. La prueba del *deepfake* en el proceso penal 749
1. Introducción 749
2. Incautación de la evidencia digital y su incorporación al proceso como prueba. Carga probatoria 751
A) Incautación de la evidencia digital en un registro domiciliario autorizado por la autoridad judicial 752
B) Aportación a la causa mediante archivos de impresión de las evidencias digitales por el denunciante o tercero 753
C) Régimen de los *deepfakes* 754
V. Conclusiones 755
VI. Bibliografía 756

CAPÍTULO 28

¿DEBE CASTIGARSE LA CREACIÓN DE ULTRAFALSIFICACIONES (*DEEPFAKES*) CON FINES LESIVOS? FUNDAMENTO Y LÍMITES DE UNA TUTELA PENAL ANTICIPADA
JAVIER CUAIRÁN GARCÍA 763

I. Introducción 764
1. El potencial lesivo de las ultrafalsificaciones 764

Página

2. El concepto normativo de ultrafalsificación 765

II. Ausencia en nuestro código penal de un delito que tipifique la creación de ultrafalsificaciones con fines lesivos... 766

1. Los delitos vigentes en nuestro Código penal..... 766

A) Delito de apoderamiento y revelación de secretos personales (arts. 197.1 y 197.7 CP) o empresariales (art. 278.1 CP) 766

B) Delito de injurias (arts. 208 y 209 CP) 767

C) Delitos de falsedad documental (arts. 390, 392, 395 y 396 CP)..... 767

D) Delito de usurpación de estado civil (art. 401 CP)... 768

E) Delitos contra la integridad moral y pornografía de menores (arts. 173 y 189 CP) 768

2. Iniciativas legislativas en España..... 770

3. La creación de ultrafalsificaciones en el Derecho Europeo ... 772

III. Fundamento y límites de una eventual tutela de la creación de ultrafalsificaciones 773

1. Bienes jurídicos comprometidos en las tres modalidades examinadas..... 774

A) La creación de ultrafalsificaciones sexuales no consentidas (modalidad a) 774

B) La creación de ultrafalsificaciones destinadas a provocar disposiciones patrimoniales bajo engaño (modalidad b)..... 775

C) La creación de ultrafalsificaciones destinadas a ser utilizadas como pruebas falsas ante los Juzgados y Tribunales (modalidad c) 776

2. La peligrosidad criminal como fundamento del adelantamiento de las barreras de protección 778

3. Respuesta a las objeciones oponibles a la tipificación autónoma de la creación..... 781

A) Expansión ilegítima de los delitos de preparación y de posesión..... 781

B) Vulneración del derecho a la libertad de expresión y a la creación artística 783

Página

C) Vulneración del principio de *última ratio* del Derecho penal 783

IV. La creación y posterior difusión de las ultrafalsificaciones en el derecho comparado 785

1. Ordenamientos jurídicos que tipifican la puesta en conocimiento de terceros, pero no la mera creación privada de ultrafalsificaciones 785

2. Ordenamientos jurídicos que tipifican la creación de ultrafalsificaciones 788

V. Bibliografía 789

CAPÍTULO 29

PROPUESTAS DE *LEGE FERENDA*: HACIA UN DERECHO PENAL DE LA INTELIGENCIA ARTIFICIAL. UNA MIRADA DESDE LA PRÁCTICA DE LA DEFENSA PENAL TECNOLÓGICA

FRANCISCO JOSÉ PELÁEZ ORTIZ 793

I. Introducción: de la casuística a la política criminal 793

II. Nuevos tipos penales específicos 795

1. El contenido sintético lesivo: la laguna de la víctima adulta 795

2. La suplantación de identidad: colmar la insuficiencia del artículo 401 796

3. El uso indebido de los sistemas de inteligencia artificial 797

4. Una cautela transversal: contra la agravante genérica «por uso de IA» 798

5. El fraude automatizado por agentes autónomos: por qué (casi) nunca hará falta un tipo nuevo 798

III. Reformas en la parte general del Código penal 799

1. La pluralidad de sujetos y el problema de la autoría 799

2. Dolo, imprudencia y el problema de la «caja negra» 800

3. La persona jurídica y el compliance específico de inteligencia artificial 801

4. Consecuencias jurídicas: decomiso e inhabilitación 802

Página

5. El sello de la defensa: una regla de garantía probatoria frente a la prueba sintética 802
6. Un límite al horizonte: no legislar para la superinteligencia . 803
IV. Propuestas de armonización internacional 803
1. Del Convenio de Budapest a la prueba electrónica transnacional 803
2. El AI Act como estándar administrativo y el riesgo de administrativización 804
3. Hacia una armonización penal mínima en la Unión 804
V. Principios rectores para la legislación penal sobre inteligencia artificial 805
VI. Conclusión..... 807

EPÍLOGO .....
MIGUEL ABEL SOUTO 809