

# Índice

---

<b>Prólogo</b> .....	13
<b>Capítulo 1. Las TIC y la seguridad internacional. Infraestructuras críticas, soberanía y responsabilidad diligente</b> .....	17
<i>Francisco Jiménez García</i>	
I. INTRODUCCIÓN: INFRAESTRUCTURAS CRÍTICAS Y CADENAS DE SUMINISTROS ANTE LOS CIBERATAQUES. LA DESINFORMACIÓN COMO AMENAZA A LOS SISTEMAS DEMOCRÁTICOS Y LA PROTECCIÓN DE LOS DERECHOS Y LIBERTADES FUNDAMENTALES .....	17
II. EL GRUPO DE TRABAJO DE COMPOSICIÓN ABIERTA SOBRE LA SEGURIDAD Y EL USO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES (2021-2025) .....	28
1. <i>El Ciberespacio como el quinto elemento «meta-espacial» de actuación de los Estados y otros actores internacionales.</i> .....	28
2. <i>La dinámica de creación y actuación de los Grupos de Expertos sobre las TIC en materia de seguridad internacional. El alcance de la soberanía: ¿principio o regla de Derecho internacional?</i> .....	31
III. LOS ATAQUES CIBERNÉTICOS A LAS INFRAESTRUCTURAS CRÍTICAS (INCLUIDA SU FUNCIONALIDAD) COMO AMENAZAS EXISTENTES Y EMERGENTES. LA NECESIDAD DE UNA CLÁUSULA DE SOLIDARIDAD CIBERNÉTICA .....	40
IV. FORTALECIMIENTO DE LA RESPONSABILIDAD: DILIGENCIA DEBIDA COMO NORMA COMÚN PERO DIFERENCIADA EN FUNCIÓN DE LAS CAPACIDADES DE LOS ESTADOS .....	47
V. CAPACIDADES Y MEDIDAS DE FOMENTO DE LA CONFIANZA. HACIA UN FONDO DE CONTRIBUCIONES VOLUNTARIAS .....	56
VI. CONCLUSIONES. ANTE LA ASIMETRÍA CIBERNÉTICA SOLO CABE RESPONSABILIDAD DIFERENCIADA HASTA QUE SE ALCANCE UN DESARROLLO CIBERNÉTICO SOSTENIBLE Y SOLIDARIO .....	61
<b>Capítulo 2. Soberanía y ciberespacio: ¿deben cambiar las reglas del juego?</b> .....	63
<i>María José Cervell Hortal</i>	
I. INTRODUCCIÓN. ....	63

II. LA VIOLACIÓN MÁS GRAVE DE LA SOBERANÍA: EL (CIBER)USO DE LA FUERZA Y LA (CIBER)AGRESIÓN . . . . .	64
III. CIBEROPERACIONES E INTERVENCIONES EN OTROS ESTADOS . . . . .	68
IV. EL PRINCIPIO DE SOBERANÍA COMO GARANTÍA ÚLTIMA. . . . .	71
1. <i>El vínculo territorial</i> . . . . .	72
2. <i>La opinión de los Estados</i> . . . . .	75
V. CONCLUSIONES . . . . .	77
<b>Capítulo 3. Inteligencia artificial, ciberdelincuencia y desinformación en el derecho de la revolución digital</b> . . . . .	79
<i>Felipe Debasa</i>	
I. INTRODUCCIÓN: LA ADECUACIÓN DEL DELITO A LA ERA DIGITAL . . . . .	79
II. CLASIFICACIÓN Y ALCANCE DE LAS CONDUCTAS ILÍCITAS EN LOS ENTORNOS DIGITALES . . . . .	82
III. DESINFORMACIÓN, MANIPULACIÓN COGNITIVA Y RIESGOS PARA LAS DEMOCRACIAS. . . . .	90
IV. CONCLUSIONES . . . . .	93
<b>Capítulo 4. La inteligencia artificial al servicio de la desinformación: un nuevo reto para el derecho penal</b> . . . . .	95
<i>José León Alapont</i>	
I. INTRODUCCIÓN. . . . .	95
II. EL FENÓMENO DE LA DESINFORMACIÓN Y SU INTERÉS PARA EL <i>IUS PUNIENDI</i> . . . . .	96
1. <i>Contexto</i> . . . . .	96
2. <i>Confusión terminológica: algunas precisiones.</i> . . . . .	101
3. <i>¿Qué supone la desinformación?</i> . . . . .	104
III. ACCIONES REGULATORIAS DE LA UNIÓN EUROPEA EN MATERIA DE INTELIGENCIA ARTIFICIAL Y DESINFORMACIÓN . . . . .	105
1. <i>Algún estudio inicial</i> . . . . .	105
2. <i>La incidencia del Reglamento de la Unión Europea sobre inteligencia artificial en la lucha contra la desinformación</i> . . . . .	108
IV. ¿DEBE ACTUAR EL DERECHO PENAL CONTRA LA DESINFORMACIÓN? ¿CÓMO?. . . . .	111
1. <i>¿Contiene ya el Código Penal una respuesta a este fenómeno?</i> . . . . .	111
2. <i>Cómo materializar dicha intervención: propuestas de lege ferenda</i> . . . . .	114
2.1. Las opciones . . . . .	114
2.2. Mi propuesta . . . . .	117
2.2.1. Especial referencia a la comisión del delito (propuesto) mediante el recurso a inteligencia artificial. . . . .	122
V. REFLEXIONES FINALES . . . . .	125

<b>Capítulo 5. IA y responsabilidad penal en el marco de la delincuencia organizada digital: ¿la única jugada ganadora es no jugar? . . . .</b>	<b>129</b>
<i>Inês Fernandes Godinho</i>	
I. INTRODUCCIÓN. . . . .	129
II. IA RESPONSABLE Y PROCESO DE REGULACIÓN. . . . .	130
III. ORGANIZACIÓN CRIMINAL, DELINCUENCIA ORGANIZADA E IA. . . . .	132
IV. JUSTICIA PREDICTIVA Y DELINCUENCIA ORGANIZADA. . . . .	136
V. REFLEXIONES FINALES . . . . .	138
<b>Capítulo 6. La digitalización en Europa e Iberoamérica. Perspectivas desde el Derecho Internacional y la Agenda 2030 . . . . .</b>	<b>139</b>
<i>Elena C. Díaz Galán</i>	
I. INTRODUCCIÓN. . . . .	139
II. LA RELACIÓN DE LA DECLARACIÓN EUROPEA Y LA CARTA IBEROAMERICANA SOBRE DIGITALIZACIÓN CON LA PRIMERA ESFERA CRÍTICA DE LA AGENDA 2030, ES DECIR, LAS PERSONAS. . . . .	142
III. ANTECEDENTES, PRINCIPIOS Y ÁMBITOS ESENCIALES DE LA DECLARACIÓN EUROPEA Y LA CARTA IBEROAMERICANA SOBRE DIGITALIZACIÓN, Y SU IMPACTO EN LA COOPERACIÓN INTERNACIONAL. . . . .	148
IV. LA NATURALEZA POLÍTICO-JURÍDICA DE LA DECLARACIÓN EUROPEA Y DE LA CARTA IBEROAMERICANA EN MATERIA DIGITAL . . . . .	153
V. CONCLUSIONES . . . . .	157
<b>Capítulo 7. La ciberdelincuencia en el Derecho español contemporáneo a la luz de la normativa internacional y europea . . . . .</b>	<b>161</b>
<i>Carlos González León</i>	
I. INTRODUCCIÓN. . . . .	161
II. NORMATIVA INTERNACIONAL Y EUROPEA SOBRE CIBERDELINCUENCIA . . . . .	163
1. <i>Convenios internacionales</i> . . . . .	163
1.1. El Convenio de Budapest sobre ciberdelincuencia (2001) . . . . .	163
1.2. El Proyecto de Convención de las Naciones Unidas (2024) . . . . .	165
2. <i>Directivas europeas y reglamento sobre protección de datos</i> . . . . .	168
2.1. Directiva sobre los ataques contra los sistemas de información (2013) . . . . .	168
2.2. Reglamento General de Protección de Datos (2016) . . . . .	170
2.3. Directiva relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión (2022) . . . . .	173
III. LA CIBERDELINCUENCIA EN EL DERECHO ESPAÑOL: LEYES, ESTRATEGIAS, DIRECTIVAS Y PLAN NACIONAL DE CIBERSEGURIDAD . . . . .	176
1. <i>Ley Orgánica de Defensa Nacional (2005)</i> . . . . .	176
2. <i>Ley de Seguridad Nacional (2015)</i> . . . . .	177
3. <i>Estrategia Nacional de Ciberseguridad (2019)</i> . . . . .	180

4. <i>Directiva de Defensa Nacional (2020)</i> . . . . .	183
5. <i>Directiva de Política de Defensa (2020)</i> . . . . .	184
6. <i>Estrategia de Seguridad Nacional (2021)</i> . . . . .	185
7. <i>Plan Nacional de Ciberseguridad (2022)</i> . . . . .	187
IV. LA CIBERCRIMINALIDAD EN EL DERECHO PENAL CONTEMPORÁNEO . . . . .	188
1. <i>Contexto y definición</i> . . . . .	188
2. <i>El Fiscal de Sala de Criminalidad Informática y las secciones de criminalidad informática de las Fiscalías (2011)</i> . . . . .	190
3. <i>La clasificación de la cibercriminalidad según sus tipos</i> . . . . .	192
V. CONCLUSIONES . . . . .	195
<b>Capítulo 8. El uso de las TIC como normalización de la violencia física, sexual, odio y discriminación hacia los menores: ¿hacia un nuevo escenario para la violencia en el ciberespacio?</b> . . . . .	197
<i>Mercedes Yela Uceda</i>	
I. INTRODUCCIÓN. . . . .	197
II. EL USO DE LAS TIC Y LA VIOLENCIA HACIA LOS MENORES . . . . .	202
1. <i>La ciberviolencia como manifestación de la violencia género hacia mujeres y niñas: hacia la Directiva (UE) 2024/1385 del Parlamento Europeo y del Consejo, de 14 de mayo de 2024, sobre la lucha contra la violencia contra las mujeres y la violencia doméstica</i> . . . . .	204
2. <i>Odio y discriminación mediante el uso de las TIC</i> . . . . .	216
III. CONCLUSIONES Y PROPUESTA DE SOLUCIONES FUTURAS . . . . .	222
<b>Capítulo 9. A vueltas con el delito de enaltecimiento y humillación a las víctimas: ¿exigencia político criminal en un contexto dominado por las TIC o criminalización del discurso?</b> . . . . .	225
<i>Carlos Fernández Abad</i>	
I. INTRODUCCIÓN. . . . .	225
II. LOS DELITOS DE ENALTECIMIENTO Y HUMILLACIÓN A LAS VÍCTIMAS DEL TERRORISMO . . . . .	229
1. <i>El delito de enaltecimiento del terrorismo</i> . . . . .	230
2. <i>El delito de humillación a las víctimas</i> . . . . .	245
III. ¿EXIGENCIA POLÍTICO-CRIMINAL EN UNA SOCIEDAD DOMINADA POR LAS TIC O CRIMINALIZACIÓN DEL DISCURSO? . . . . .	252
<b>Capítulo 10. Cibercriminalidad: análisis de tipo penal con enfoque en los delitos de auto doctrinamiento o autodiestramiento a través de redes e internet</b> . . . . .	255
<i>Alicja M. Skokowska Nowak</i>	
I. INTRODUCCIÓN. . . . .	255

II. CIBERCRIMINALIDAD Y DELITO INFORMÁTICO . . . . .	257
1. <i>Regulación de delito informático y ciberdelincuencias en la normativa internacional europea</i> . . . . .	260
1.1. Marco legislativo internacional: el Proyecto convención de la ONU . . . . .	261
1.2. La Unión Europea . . . . .	264
III. ADOCTRINAMIENTO, ADIESTRAMIENTO TERRORISTA A TRAVÉS DE LAS TIC . . . . .	270
1. <i>Consideraciones generales</i> . . . . .	270
2. <i>Análisis de la conducta típica, imputación objetiva y elementos subjetivos del tipo penal del artículo 575.2 CP</i> . . . . .	273
IV. CONCLUSIONES . . . . .	276
<b>Capítulo 11. ¿Es posible coordinar/combinar la seguridad con la IA?</b>	
<b>La biometría como ejemplo</b> . . . . .	279
<i>Roberto Cuesta Calvo</i>	
I. INTRODUCCIÓN. . . . .	279
II. VERIFICACIÓN DE IDENTIDAD . . . . .	280
III. BIOMETRÍA. . . . .	281
IV. BIOMETRÍA EN LAS TIC. . . . .	282
1. <i>Características</i> . . . . .	282
V. CUMPLIMIENTO NORMATIVO . . . . .	283
VI. BIOMETRÍA FACIAL. . . . .	287
1. <i>Implementaciones sistemas biométricos</i> . . . . .	287
2. <i>Implementación sistemas biométricos basados en inteligencia artificial</i> . . . . .	288
VII. UTILIDADES DE LA BIOMETRÍA EN LA SEGURIDAD. . . . .	290
VIII. CONCLUSIONES . . . . .	291
<b>Capítulo 12. La influencia de la inteligencia artificial en las organizaciones criminales, en especial en la trata sexual</b> . . . . .	293
<i>María Cristina Aranda López</i>	
I. INTRODUCCIÓN. . . . .	293
II. LA INTELIGENCIA ARTIFICIAL Y SU PRINCIPAL CLASIFICACIÓN . . . . .	294
III. LA SIMBIOSIS ENTRE LA IA Y EL CRIMEN ORGANIZADO . . . . .	298
IV. LOS USOS DE LA IA POR LAS ORGANIZACIONES CRIMINALES, EN ESPECIAL LA TRATA SEXUAL. . . . .	299
V. LA NUEVA LEGISLACIÓN EUROPEA CONOCIDA COMO LEY IA. . . . .	304
VI. CONCLUSIONES . . . . .	310