

# Índice General

Página

ABREVIATURAS .....	17
INTRODUCCIÓN – CIBERSEGURIDAD Y DERECHO PENAL: CONCEPTUALIZACIÓN .....	21
CAPÍTULO I	
LA CIBERSEGURIDAD EN EL DERECHO PENAL INTERNACIONAL Y DE LA UNIÓN EUROPEA .....	35
1.1. Génesis del Derecho penal de la ciberseguridad: antes de los grandes acuerdos internacionales .....	35
1.1.1. Ataques históricos contra la ciberseguridad .....	39
1.1.2. Los instrumentos jurídicos no vinculantes: las recomendaciones del Consejo de Europa .....	40
1.1.3. La necesidad de avanzar hacia la armonización legislativa internacional .....	42
1.2. Derecho penal internacional .....	43
1.2.1. El Convenio sobre la Ciberdelincuencia de Budapest de 23 de noviembre de 2001 .....	43
1.2.1.1. Derecho penal sustantivo .....	45
1.2.1.1.1. Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos .....	45
1.2.1.1.1.1. Acceso ilícito .....	45
1.2.1.1.1.2. Interceptación ilícita .....	46
1.2.1.1.1.3. Interferencia en los datos .....	46
1.2.1.1.1.4. Interferencia en el sistema .....	46
1.2.1.1.1.5. Abuso de los dispositivos .....	47
1.2.1.1.2. Delitos informáticos .....	47
1.2.1.1.2.1. Falsificación informática .....	47
1.2.1.1.2.2. Fraude informático .....	48

1.2.1.1.3.	Reflexiones doctrinales en materia de Derecho penal internacional sustantivo ....	48
1.2.1.2.	Derecho procesal penal internacional y otros elementos de cooperación internacional .....	53
1.2.1.2.1.	Competencia judicial .....	53
1.2.1.2.2.	La Red 24/7 .....	55
1.2.1.2.3.	Reflexiones doctrinales en materia de Derecho procesal penal internacional .....	56
<b>1.3.</b>	<b>Derecho penal de la Unión Europea .....</b>	<b>58</b>
1.3.1.	<i>La inexistencia de un Corpus Iuris Poenalis europeo .....</i>	58
1.3.2.	<i>Análisis de los principales actos legislativos para la creación de un Derecho penal sobre ciberdelincuencia de la Unión Europea .....</i>	61
1.3.2.1.	La Directiva (UE) 2016/1148 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información de la Unión (Directiva NIS) .....	61
1.3.2.2.	El Reglamento (UE) 2019/881 relativo a ENISA y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación .....	67
1.3.3.	<i>Influencia del Derecho penal de la Unión Europea en la legislación de los Estados miembros .....</i>	68
1.3.3.1.	Francia .....	68
1.3.3.2.	Alemania .....	69
<b>1.4.</b>	<b>Límites del Derecho penal internacional y comunitario en relación con la ciberseguridad .....</b>	<b>71</b>

## CAPÍTULO II

	<b>LA CIBERSEGURIDAD EN EL DERECHO PENAL COMPARADO DE PAÍSES FUERA DEL ÁMBITO DE LA UNIÓN EUROPEA .....</b>	<b>75</b>
<b>2.1.</b>	<b>La diversidad de estrategias nacionales en materia de ciberseguridad a nivel mundial .....</b>	<b>75</b>
2.1.1.	<i>Convergencias .....</i>	76
2.1.2.	<i>Divergencias .....</i>	77
<b>2.2.</b>	<b>Interpretación de los datos contenidos en los cinco pilares del Global Cybersecurity Index .....</b>	<b>77</b>
2.2.1.	<i>Legal .....</i>	78
2.2.2.	<i>Técnico .....</i>	79

	<u>Página</u>
2.2.3. Organización .....	79
2.2.4. Construcción de capacidades .....	79
2.2.5. Cooperación .....	80
<b>2.3. Regulación en el Derecho penal comparado del delito de acceso ilícito a un sistema informático .....</b>	<b>80</b>
2.3.1. Primera categoría: regulación del delito en normas penales especiales .....	81
2.3.2. Segunda categoría: regulación del delito en un título o capítulo propio y diferenciado .....	82
2.3.3. Tercera categoría: regulación del delito junto a otros delitos ya existentes .....	82
<b>2.4. Análisis de la regulación de los delitos que afectan a la ciberseguridad en el Derecho penal comparado .....</b>	<b>85</b>
2.4.1. Reino Unido .....	85
2.4.2. Estados Unidos de América .....	87
2.4.2.1. Conclusiones del Internet Crime Report 2019 del FBI ...	89
2.4.2.1.1. Resultados generales relativos a los ciberdelitos .....	90
2.4.2.1.2. Resultados específicos relativos a los delitos que afectan a la ciberseguridad .....	91
2.4.2.2. La importancia de la protección de los datos sanitarios en la jurisprudencia estadounidense .....	92
2.4.2.2.1. Sorrell v. IMS Health Inc. ....	92
2.4.2.2.2. CareFirst, Inc. v. Chantal Attias .....	93
2.4.2.2.3. LabMD, Inc. v. Federal Trade Commission ...	93
2.4.2.3. Particularidades de la legislación de Washington D.C. ...	94
2.4.3. Canadá .....	94
2.4.4. Australia .....	96
2.4.5. Nueva Zelanda .....	98
2.4.6. Suiza .....	99
2.4.7. Federación de Rusia .....	100
<b>2.5. Aspectos del Derecho penal comparado susceptibles de ser tenidos en cuenta en el Derecho penal español .....</b>	<b>102</b>

## CAPÍTULO III

<b>LA CIBERSEGURIDAD EN EL DERECHO PENAL ESPAÑOL</b> .....	105
<b>3.1. El principio de <i>ultima ratio</i> como límite entre el Derecho administrativo y el Derecho penal</b> .....	105
<b>3.2. La importancia del principio de precaución en el desarrollo de los delitos contra la ciberseguridad</b> .....	109
<b>3.3. Derecho penal sustantivo</b> .....	114
3.3.1. <i>Construcción de los perfiles de los delitos que afectan a la ciberseguridad</i> .....	114
3.3.2. <i>Los delitos que afectan a la ciberseguridad en el Código Penal</i> .....	118
3.3.2.1. Ciberseguridad en los delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio .....	118
3.3.2.1.1. Apoderamiento de secretos documentales ...	118
3.3.2.1.2. Interceptación de comunicaciones .....	120
3.3.2.1.3. Descubrimiento del secreto recogido en archivos o registros .....	121
3.3.2.1.4. Actual configuración del delito de intrusión en un sistema de información .....	122
3.3.2.1.4.1. Inadecuada ubicación entre los delitos de descubrimiento y revelación de secretos .....	122
3.3.2.1.4.2. Más allá de la intimidad y de los datos reservados de carácter personal como bienes jurídicos protegidos .....	125
3.3.2.1.4.3. La actual redacción del tipo delictivo del artículo 197 bis 1 del Código Penal .....	133
3.3.2.1.5. Interceptación de transmisiones no públicas de datos informáticos .....	136
3.3.2.2. Ciberseguridad en los delitos contra el patrimonio y contra el orden socioeconómico .....	137
3.3.2.2.1. Robo con fuerza en las cosas .....	137
3.3.2.2.1.1. Descubrimiento de claves para la sustracción del contenido .....	138
3.3.2.2.1.2. Uso de llaves falsas .....	138

	<u>Página</u>
3.3.2.2.1.3. Inutilización de sistemas espe- cíficos de alarma o guarda .....	141
3.3.2.2.2. Estafa informática .....	142
3.3.2.2.3. Utilización ilícita de energías, sustancias u otros servicios ajenos .....	147
3.3.2.2.4. Daños informáticos .....	148
3.3.2.2.5. Conductas relacionadas con la superación de dispositivos de protección en los delitos relativos a la propiedad intelectual .....	154
3.3.2.2.6. Descubrimiento y revelación de secretos de empresa .....	156
3.3.2.3. Ciberseguridad en los delitos contra la seguridad colectiva .....	160
3.3.2.3.1. Estragos .....	160
3.3.2.4. Ciberseguridad en los delitos de falsedades .....	161
3.3.2.4.1. Fabricación o tenencia de programas infor- máticos destinados a la comisión de estos delitos .....	161
3.3.2.5. Ciberseguridad en los delitos contra la Administra- ción pública .....	162
3.3.2.5.1. Infidelidad en la custodia de documentos y violación de secretos .....	162
3.3.2.6. Ciberseguridad en los delitos contra la Constitución ...	165
3.3.2.6.1. Delitos cometidos por los funcionarios públicos contra la inviolabilidad domici- liaria y demás garantías de la intimidad ...	165
3.3.2.7. Ciberseguridad en los delitos contra el orden público ...	167
3.3.2.7.1. Daños a instalaciones de telecomunica- ciones .....	167
3.3.2.7.2. Terrorismo .....	168
3.3.2.8. Ciberseguridad en los delitos de traición y contra la paz o la independencia del Estado y relativos a la Defensa Nacional .....	170
3.3.2.8.1. Descubrimiento y revelación de secre- tos e informaciones relativas a la Defensa Nacional .....	170
3.3.3. <i>La responsabilidad penal de las personas jurídicas en los delitos que afectan a la ciberseguridad</i> .....	173

<b>3.4.</b>	<b>Derecho procesal penal</b> .....	174
3.4.1.	<i>La determinación de la ley penal aplicable en el espacio y de la jurisdicción competente</i> .....	174
3.4.2.	<i>Líneas de evolución futuras</i> .....	178
<b>3.5.</b>	<b>Cuestiones de <i>lege ferenda</i></b> .....	180
3.5.1.	<i>La ciberseguridad como bien jurídico protegido autónomo</i> .....	180
3.5.1.1.	El avance de la tecnología hace inevitable la aparición de nuevos bienes jurídicos protegidos .....	180
3.5.1.2.	La ciberseguridad en la Declaración Universal de los Derechos Humanos .....	181
3.5.1.3.	La ciberseguridad en la Constitución española de 1978 .....	182
3.5.1.4.	La ciberseguridad en la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales .....	182
3.5.1.5.	Conceptualización de la ciberseguridad como bien jurídico protegido autónomo en el Derecho penal .....	183
3.5.2.	<i>El delito de intrusión en un sistema de información, o delito de cracking</i> .....	185
3.5.2.1.	Propuesta político-criminal sobre la represión penal autónoma de esta conducta .....	185
3.5.2.2.	Sistema de criminalización .....	189
3.5.2.3.	Consideración del <i>hacking</i> como conducta lícita .....	194
3.5.3.	<i>La creación de un nuevo título en el CP para los delitos contra la ciberseguridad</i> .....	196

## CAPÍTULO IV

	<b>CIBERSEGURIDAD Y DERECHO PENAL EN TECNOLOGÍAS EMERGENTES SANITARIAS</b> .....	199
<b>4.1.</b>	<b>Las nuevas tecnologías como elemento instrumental para la ciberseguridad en el ámbito sanitario</b> .....	199
<b>4.2.</b>	<b>Inteligencia Artificial</b> .....	201
4.2.1.	<i>Desafíos para la IA en relación con los delitos que afectan a la ciberseguridad</i> .....	201
4.2.2.	<i>Aplicaciones para la IA como herramienta de ciberseguridad en el ámbito sanitario</i> .....	206
4.2.2.1.	La IA como protección frente al correo no deseado en hospitales y centros sanitarios .....	207

	<u>Página</u>
4.2.2.2. La IA como protección frente a los accesos indebidos para descubrir secretos .....	209
4.2.2.3. La IA como protección más eficiente frente a los daños informáticos .....	210
4.2.2.4. La IA como protección de las propias medidas de ciberseguridad .....	213
4.2.2.5. La IA y su uso en cirugía como ejemplo de su adaptación a un esquema jurídico-penal clásico .....	215
4.2.3. <i>Los peligros de la utilización de la IA en el ámbito sanitario y su influencia sobre el Derecho penal</i> .....	220
<b>4.3. Robótica y drones</b> .....	225
4.3.1. <i>Robótica</i> .....	225
4.3.1.1. Cuestiones de Derecho penal relativas a la ciberseguridad de la robótica actual .....	225
4.3.1.2. Desafíos jurídico-penales para la ciberseguridad de los sistemas autónomos inteligentes .....	228
4.3.2. <i>Drones</i> .....	229
4.3.2.1. Ciberseguridad como protección de los drones médicos y sanitarios frente a delitos .....	229
<b>4.4. Hospitales inteligentes</b> .....	231
<b>4.5. Internet de las Cosas Médicas (IdCM)</b> .....	233
<b>4.6. La nube sanitaria</b> .....	236
<b>4.7. Salud electrónica</b> .....	237
<b>4.8. Los avances tecnológicos obligan a ir más allá de las clásicas cuestiones de <i>lege lata</i> y <i>lege ferenda</i></b> .....	238
<b>4.9. El futuro jurídico-penal de la ciberseguridad en el ámbito sanitario</b> ...	241
 EPILOGO – LA LEALTAD A LA LEY DIVINA COMO FUNDAMENTO PARA LA SUPERVIVENCIA DE NUESTRO PUEBLO .....	 249
BIBLIOGRAFÍA .....	251