

ÍNDICE

Prólogo	11
Introducción	17

Capítulo I

EXPANSIÓN TECNOLÓGICA Y CAMBIO SOCIAL

1. Los cambios sociales producidos por la expansión de la tecnología informática	19
2. Breve reseña histórica	24
3. El ciberespacio	28

Capítulo II

DELITOS INFORMÁTICOS

1. La cuestión terminológica	31
2. Definición y concepto	34
2.1. Concepción amplia	36
2.2. Concepción intermedia	38
2.3. Concepción restringida	38
3. El delito informático como categoría independiente	41
4. Bienes jurídicos vinculados al delito informático	44
4.1. Seguridad informática	44
4.2. Integridad y disponibilidad de los datos informáticos	46
4.3. Libertad informática	49

Capítulo III

EL HACKING

1. <i>Hacking</i> y <i>hackers</i>	53
1.1. <i>White hat</i> y <i>Black hat hackers</i>	55
1.2. Ética <i>hackero</i> “ <i>nética</i> ”	56
1.3. El caso Aaron Swartz	57

2. El <i>hacktivismo</i>	58
2.1. Operaciones <i>Anonymous</i>	59
3. El intrusismo informático o <i>hacking</i> puro.....	61
4. ¿Debe el intrusismo informático ser considerado un delito autónomo?	63

Capítulo IV

HACKING Y DERECHO PENAL

1. El tratamiento del <i>hacking</i> en derecho penal	67
1.1. El <i>hacking</i> en el Convenio de Budapest.....	67
1.2. El intrusismo informático simple (o <i>hacking</i>) en el Código Penal Argentino.....	68
1.2.1. Bien Jurídico Protegido.....	69
1.2.2. Acción Típica	71
1.2.3. Otros elementos que componen el tipo objetivo	71
1.2.4. Elementos normativos del tipo.....	74
1.2.5. El tipo subjetivo	76
1.2.6. Situaciones que podrían excluir la tipicidad	77
1.2.6.1. ¿Qué sucede cuando las motivaciones del intruso, están guiadas por el mero afán de encontrar fallas en el sistema para sugerir correcciones?	77
1.2.6.2. ¿Es posible ingresar a un sistema o dato informático de acceso restringido en el marco de un proceso judicial?	79
1.2.6.3. ¿Qué sucede si el Juez que emite la orden judicial que franquea el acceso a un sistema informático no tiene jurisdicción para tomar contacto con los datos por estar estos situados en otro lugar?	80
1.2.6.4. ¿Pueden los empleadores ingresar a los datos o sistemas informáticos proporcionados a sus empleados?.....	80
1.2.7. Sujeto Activo	81
1.2.8. Sujeto Pasivo	81
1.2.9. Consumación y Tentativa	81
1.2.10. Carácter de la figura	83
1.2.11. Figura Agravada	83
1.2.12. Carácter de la acción.....	84
1.2.13. Competencia Judicial	85

1.2.14. Producción, venta y posesión de elementos destinados a <i>hackear</i>	86
1.2.15. Condena por <i>hacking</i> puro en Argentina	87
1.3. El <i>hacking</i> como delito en el Derecho Penal Regional del Mercosur	88
1.4. El <i>hacking</i> como delito en el Derecho Penal europeo	96
1.5. El <i>hacking</i> como delito en el Derecho Penal de Estados Unidos de Norteamérica	92

Capítulo V

EL HACKING COMO MEDIO DE COMISIÓN DE OTRAS CONDUCTAS

1. Acceso ilegítimo a banco de datos personales, revelación ilegítima de su información e inserción ilegítima de datos	93
2. Acceso y apoderamiento de comunicaciones electrónicas	94
3. Sabotaje informático (infecciones de <i>malware</i> , <i>defacing</i> , y otras conductas)	95
3.1. <i>Malware</i>	95
3.2. <i>Defacement</i>	95
3.3. <i>Botnets</i>	95
3.4. <i>Ransomware</i>	96
3.5. <i>Kompromat</i>	96
4. Fraudes informáticos (<i>phishing</i>)	96
5. Robo de identidad	97
6. Alteración dolosa de registros fiscales	97
7. Porno Venganza (<i>revange porn</i>)	97

Capítulo VII

PROPUESTA LEGISLATIVA

.....	99
-------	----

Capítulo VIII

ANEXO NORMATIVO

1. Disposición ONTI N° 02/2013 que crea el ICIC-CERT en la República Argentina	105
---	-----

2. Resolución N° 234/2016 dictada por el Ministerio de Seguridad de la República Argentina, que aprueba el protocolo general de actuación para las fuerzas policiales y de seguridad en la investigación y proceso de recolección de pruebas en ciberdelitos	110
3. Decreto 577/2017 que crea el Comité de Ciberseguridad en el ámbito del Ministerio de Modernización de la República Argentina	122
Bibliografía	127