



ÍNDICE GENERAL

PRESENTACIÓN	9
ABREVIATURAS	21

A. DOCTRINA

1. DERECHO PENAL. PARTE GENERAL

1	
LA TUTELA DE LA INTEGRIDAD Y DISPONIBILIDAD DE DATOS Y SISTEMAS INFORMÁTICOS: EL MODELO TRADICIONAL VINCULADO A UNA PROTECCIÓN Estrictamente Patrimonial, un mal Referente	
NORBERTO J. DE LA MATA BARRANCO	
§ 1. Introducción	29
§ 2. Referentes legales internacionales y de derecho comparado	30
§ 3. Los ataques a datos y sistemas en el contexto de los delitos de daños	34
§ 4. Los ataques a datos y sistemas como delitos contra su integridad y disponibilidad	36
§ 5. Los datos y sistemas: el objeto de ataque de las conductas punibles	38
§ 6. El interés a tutelar	40
§ 7. El denominado delito de interferencia ilegal en datos	43
§ 8. El delito de interferencia ilegal en sistemas de información	48
§ 9. Reflexión final	49

2

«FAKE NEWS»: CIBERCRIMINALIDAD Y LIBERTAD DE EXPRESIÓN EN INTERNET

JAVIER AUGUSTO DE LUCA - YAMILA YAEL LUZZA

§ 1. Introducción	51
§ 2. Noticias falsas a través de los servidores de Internet	52
a) ¿Qué son las «fake news» y cómo detectarlas?	52
b) Noticias falsas. Guerrilla comunicacional y democracia	53
§ 3. Control estatal: sobre la necesidad o no de intervención del derecho penal. Algunos estándares en el derecho internacional	55
§ 4. Responsabilidad de los intermediarios por los contenidos	63
§ 5. Conclusiones	70

3

RESPONSABILIDAD PENAL DE LOS PROVEEDORES DEL SERVICIO EN INTERNET

GUSTAVO EDUARDO ABOSO

§ 1. Introducción	73
§ 2. La autodeterminación informativa y el derecho «al olvido» en Internet	74
§ 3. La responsabilidad de los proveedores de servicio en la sociedad de la información a través de la jurisprudencia	78
a) «CubbyInc.v.CompuServeInc.»(1991)	80
b) «Zeranv.AmericaOnlineInc.»(1997)	80
c) Caso «CompuServer Deutschland» (1998)	83
d) Críticas al fallo del AG München en el caso «CompuServer Deutschland»	86
e) «United States v.Thomas»	88

§ 4. Creación de un «link» o enlace para la comisión de delitos	89
§ 5. Las leyes 25.690,26.032 y 27.078	90
§ 6. La responsabilidad de los proveedores intermediarios de servicios en la jurisprudencia argentina	91
§ 7. La responsabilidad de los proveedores intermediarios de servicios en la jurisprudencia comunitaria: Google Spain, S.L. y Google Inc./Agencia Española de Protección de Datos (AEPD) y Mario Costeja González (2014)	93
§ 8. Aplicación de las reglas de participación criminal a los proveedores de servicio de Internet	96
§ 9. El conocimiento de la actividad como presupuesto normativo de responsabilidad	106
§ 10. Responsabilidad de los establecimientos comerciales que brindan servicio de Internet	108
§ 11. Valoración final	109

4

UNA VISIÓN DESDE LOS DERECHOS HUMANOS SOBRE LAS TECNOLOGÍAS DE VIGILANCIA E INVESTIGACIÓN

EDUARDO FERREYRA

§ 1. Introducción	113
§ 2. Sistema universal de derechos humanos	115
§ 3. Sistema interamericano de derechos humanos	116
§ 4. El hackeo estatal	121
§ 5. Acceso transfronterizo de datos	124
§ 6. Conclusión	126

2. DERECHO PENAL. PARTE ESPECIAL

1

A DIEZ AÑOS DE LA LEY DE DELITOS INFORMÁTICOS. BALANCE Y PROPUESTAS

NORA A. CHERÑAVSKY - PABLO H. GRIS MUNIAGURRIA DIÓGENES A. MOREIRA

§ 1. Introducción	129
§ 2. La ley 26.388. Definiciones. Generalidades. Nuevos bienes tutelados	132
§ 3. La ley 26.388 y la adaptación de los tipos tradicionales. Evolución legislativa y jurisprudencial en diez años de su vigencia	135
a) Art. 128, CP: pornografía infantil por Internet	135
b) Art. 153, CP: violación de correspondencia digital. Secreto y privacidad de las comunicaciones	136
c) Art. 153 «bis», CP: acceso ilegítimo a datos o a un sistema informático	140
d) Art. 155, CP: difusión del contenido de una comunicación electrónica	141
e) Art. 157, CP: revelación de datos	144
f) Art. 157 «bis», CP: acceso ilegítimo, difusión o alteración de bases de datos personales	145
g) Art. 173, inc. 16, CP: estafa o fraude informático	146
h) Arts. 183 y 184, CP: daño informático	148
i) Art. 197, CP: interrupción o entorpecimiento de comunicaciones privadas o públicas	149
j) Art. 255, CP: sustracción/destrucción de medios de prueba	150
§ 4. Otros delitos informáticos previstos en leyes especiales	151
§ 5. Incriminación posterior a la sanción de la ley 26.388: el «grooming»	151
§ 6. Delitos tradicionales cometidos por medios informáticos	152
§ 7. Nuevos fenómenos delictivos y necesidad de nuevas incriminaciones	153
a) El robo de identidad digital	153
b) El «sexting»	154

c) «Revenge porn» o pornovenganza	154
§ 8. Reflexiones finales sobre el entorno virtual y la cooperación internacional.	
Conclusiones	156

2

ALGUNAS CONSIDERACIONES SOBRE EL «SEXTING» EN EL DERECHO PENAL ARGENTINO

VÍCTOR HUGO PORTILLO

§ 1. Introducción	161
§ 2. Concepto y magnitud del «sexting»	162
a) Concepto	162
b) Magnitud del fenómeno	163
§ 3. Marco regulatorio del «sexting» en el derecho penal argentino y el derecho comparado	164
a) El «sexting» en el derecho penal argentino	164
b) El «sexting» en el derecho penal español	167
§ 4. Análisis de casos judicializados sobre «sexting»	168
a) Caso «H.A. v. State of Florida», 2007	168
b) «Miller v. Skumanick»	169
§ 5. Análisis final	170
§ 6. Conclusión	171

3

EL CIBERATAQUE «WANNACRY» COMO MODALIDAD DE DELINCUCENCIA INFORMÁTICA

FRANCISCO ALMENAR PINEDA

§ 1. Introducción	173
§ 2. Breve referencia a la evolución histórica de los delitos de «hacking»	175
a) Introducción	175
b) Concepto y rasgos de la delincuencia informática	176
c) Evolución normativa supranacional	177
§ 3. Concepto del delito de «hacking» y del denominado «WannaCry»	179
a) Concepto del delito de «hacking»	179
b) Concepto de «WannaCry»	180
§ 4. El tratamiento del «hacking» en el ordenamiento penal español	181
a) La situación antes de la reforma de 2010	181
b) La reforma de 2010	183
c) La reforma de 2015	184
§ 5. «WannaCry» en relación con el bien jurídico protegido y objeto material en el delito de «hacking»	185
a) Introducción	185
b) «WannaCry» como delito contra la intimidad	186
c) El objeto material afectado por «WannaCry»	189
§ 6. Naturaleza jurídica de «WannaCry»	191
§ 7. «WannaCry» en el art. 197 «bis», 1 del CP	194
a) Sujeto activo y pasivo	194
b) La conducta típica	195
c) La relevancia penal de las conductas de facilitar «WannaCry»	198
d) La conducta de mantenimiento en el sistema	199
e) Aspecto subjetivo	200
f) Formas de aparición	200
§ 8. Las relaciones concúrtales derivadas de «WannaCry»	205
§ 9. «WannaCry» como conducta cometida en el seno de organización o grupo criminal	208
§ 10. Conclusiones	211

3. DERECHO PROCESAL PENAL

1

LA NUEVA LEY «CLOUD ACT». SU IMPACTO EN INVESTIGACIONES EN ENTORNOS DIGITALES

DANIELA DUPUY - MARIANA KIEFER

§ 1. Planteamiento del problema	219
§ 2. Acuerdos de Asistencia Legal Mutua «MLAT»	222
§ 3. Contexto legal en Estados Unidos: Ley de Privacidad de Comunicaciones Electrónicas y Ley de Comunicaciones Almacenadas	224
§ 4. El caso «Microsoft/Ireland» como precedente de la «Cloud Act»	226
§ 5. Una respuesta legislativa: la «Cloud Act»	231
§ 6. Críticas versus respaldos a la «Cloud Act»	235
§ 7. Conclusión	236

B. FORENSIA DIGITAL

1

EL TRATAMIENTO DE LA EVIDENCIA DIGITAL EN LOS PROCESOS PENALES

BRUNO CONSTANZO - SABRINA LAMPERTI ANA HAYDÉE DI IORIO

§ 1. Introducción	239
§ 2. La evidencia digital en la legislación argentina	240
a) Contexto general	240
b) Evolución normativa	242
1. Provincia de Neuquén	243
2. Provincia de Río Negro	244
3. Provincia de Buenos Aires	246
4. Procuración General de la Nación. Ministerio Público Fiscal	254
5. Provincia de Corrientes	255
6. Provincia de Salta	255
7. Ministerio de Seguridad de la Nación	256
8. Ministerio de Justicia y DDHH de la Nación. Consejo de procuradores, fiscales, defensores y asesores generales de la República Argentina. Consejo Federal de Política Criminal	257
§ 3. Aspectos a considerar desde la perspectiva técnica informática	258
a) Evidencia digital en Internet	258
b) Evidencia digital en memoria principal o memoria volátil	260
c) Evidencia digital en memoria persistente o disco	261
d) Evidencia digital en dispositivos móviles	262
§ 4. Conclusiones	263

C. DERECHO INFORMÁTICO COMPARADO

1

LOS DELITOS INFORMÁTICOS EN LA LEGISLACIÓN PENAL PERUANA

FELIPE VILLAVICENCIO TERREROS

§ 1. Alcances generales	267
a) Introducción	267
b) Concepto y modalidades	269
c) Bien jurídico tutelado	270
d) El perfil del ciberdelincuente	271
e) Las personas jurídicas como sujeto activo y sujeto pasivo	273

§ 2. La Ley de Delitos Informáticos en la legislación penal peruana	274
a) Antecedente de los delitos Informáticos	274
b) La ley 30.096	275
1. Objetivo y finalidad de la ley	275
2. Modalidades típicas previstas en la ley	276
3. Circunstancias modificativas de responsabilidad	282
4. Exención de responsabilidad	283

2

EL IMPACTO DE LA INFORMÁTICA EN EL SISTEMA JURÍDICO PENAL BRASILEÑO

SPENCER TOTH SYDOW

§ 1. Introducción	285
§ 2. Derecho y tecnología	285
§ 3. «Malum prohibitum» y «malum in se»	286
§ 4. El sistema jurídico brasileño en la era de la virtualidad	287
§ 5. Dificultades modernas	294
§ 6. Conclusiones	295

D. SELECCIÓN DE JURISPRUDENCIA

I. «Grooming» (art. 131, CP)	299
1. Acción típica de «Grooming». Contacto telemático o a través de sistemas de transmisión de información	299
2. Competencia de la Justicia en lo Penal Contravencional y de Faltas de la Ciudad de Buenos Aires	299
II. Pornografía infantil (art. 128, CP)	299
1. Rechazo de la suspensión de proceso a prueba en casos de difusión o comercialización de pornografía infantil	299
2. Competencia de la Justicia en lo Penal, Contravencional y de Faltas de la Ciudad de Buenos Aires, respecto de distribución de pornografía infantil	300
3. Jurisdicción y competencia provincial si la conexión a Internet para distribuir pornografía infantil se realizó desde el territorio de una provincia	300
III. Delitos cometidos contra base de datos personales (art. 157 «bis», CP)	300
— Competencia del fuero federal en caso de violación de base de datos personales	300
IV. Defraudación informática (art. 173, inc. 16, CP)	300
— Adecuación típica de la conducta a la figura de defraudación informática. Técnicas de manipulación del sistema	300
V. Daño informático (art. 183, CP)	301
— Competencia de la Justicia Nacional en el supuesto de códigos maliciosos o accesos remotos que causen daño en sitios de una empresa extranjera	301
VI. Daño informático agravado (art. 184, CP)	301
— Prueba digital. Peritaje en un daño informático agravado	301

E. COMENTARIOS BIBLIOGRÁFICOS

1

NUEVOS DESAFÍOS DE LA EVIDENCIA DIGITAL: ACCESO TRANSFRONTERIZO Y TÉCNICAS DE ACCESO REMOTO A DATOS INFORMÁTICOS

MARCOS SALT

	305
BIBLIOGRAFÍA GENERAL	309
PAUTAS EDITORIALES	319