



ÍNDICE

<i>Prólogo</i> , por Marcelo A. Riquert	21
<i>Presentación</i>	27
<i>Introducción</i>	31
 Capítulo I La sociedad del siglo XXI. La sociedad de la información	 35
 Capítulo II Antecedentes nacionales de la ley 26.388	 49
1. Proyecto de Leonor E. Tolomeo (1996)	49
2. Proyecto de Carlos R. Álvarez (1996)	50
3. Proyecto de José A. Romero Feris (1996)	50
4. Proyecto de Antonio T. Berhongaray (1997)	51
5. Anteproyecto de Ley de Delitos Informáticos (2001)	52
6. Proyecto de Marta L. Osorio (2005)	54
7. Proyecto de Silvia V. Martínez (2005)	55
8. Proyecto de Andrés Sotos (2005)	56
9. Proyecto de Delia B. Bisutti (2006)	59
10. Proyecto de Dante O. Canevarolo (2006)	60
11. Proyecto de Diana Conti y Agustín Rossi (2006)	62
12. Anteproyecto de Ley de Reforma y Actualización Integral del Código Penal	64
13. El proyecto de ley que da origen a la ley 26.388	74
 Capítulo III La Ley 26.388 de Reforma al Código Penal en Materia de Criminalidad Informática	 78
1. Terminología incorporada al art. 77 del C.P	78
1.1. Antecedentes	78
1.2. Análisis	79
1.3. Repercusión sobre otros tipos penales no comprendidos por la reforma de la ley 26.388	81
2. El tipo penal	83
2.1. Antecedentes	84
2.2. Bien jurídico	85
2.3. El tipo penal de ofrecimiento y distribución de imágenes relacionadas con pornografía infantil	87
2.3.1. Acciones típicas	88
2.3.2. Sujetos de la acción típica	91
2.3.3. Tipicidad subjetiva	91
2.3.4. Consumación y tentativa	91
2.3.5. Competencia	92
2.4. Tenencia de imágenes relacionadas con pornografía infantil con fines inequívocos de distribución o comercialización	92
2.4.1. Acción típica	92
2.4.2. Sujetos de la acción típica	94
2.4.3. Tipicidad subjetiva	94
2.4.4. Consumación / tentativa	94

2.5. El tipo penal de suministro de material pornográfico a menores de catorce años a través de medios informáticos	95
2.5.1. Acción típica	95
2.5.2. Sujetos de la acción típica	96
2.5.3. Tipicidad subjetiva	97
2.5.4. Consumación / tentativa	97
3. Los tipos penales de violación de secreto y privacidad (arts. 153, 153 bis, 155, 157 y 157 bis, C.P.)	97
3.1. Bien jurídico	97
3.2. Violación de correspondencia electrónica	99
3.2.1. Antecedentes	99
3.2.2. Acción típica	100
3.2.3. Sujetos de la acción típica	106
3.2.4. Tipicidad subjetiva	106
3.2.5. Consumación / tentativa	106
3.3. Acceso ilegítimo a un sistema informático	107
3.3.1. Antecedentes	107
3.3.2. Acción típica	107
3.3.3. Sujetos de la acción típica	110
3.3.4. Tipicidad subjetiva	111
3.3.5. Consumación / tentativa	111
3.3.6. Acceso ilegítimo agravado a un sistema informático	111
3.4. Publicación abusiva de correspondencia	112
3.4.1. Antecedentes	112
3.4.2. Acción típica	112
3.4.3. Sujetos de la acción típica	115
3.4.4. Tipicidad subjetiva	115
3.4.5. Consumación / tentativa	115
3.5. Revelación de secretos	115
3.5.1. Antecedentes	116
3.5.2. Acción típica	116
3.5.3. Sujetos de la acción típica	118
3.5.4. Tipicidad subjetiva	118
3.5.5. Consumación / tentativa	118
3.6. Delitos relacionados con la protección de datos personales	118
3.6.1. Antecedentes	119
3.6.2. Acción típica	119
3.6.3. Sujetos de la acción típica	124
3.6.4. Tipicidad subjetiva	125
3.6.5. Consumación/ tentativa	125
4. El tipo penal defraudación informática (art. 173, inc. 16, C.P.)	125
4.1. Antecedentes	125
4.2. Bien jurídico	127
4.3. El tipo penal de defraudación del art. 173, inc. 16 del C.P.	127
4.3.1. Acción típica	127
4.3.2. Sujeto de la acción típica	131
4.3.3. Tipicidad subjetiva	132
4.3.4. Consumación / tentativa	132
5. El tipo penal de daño de los arts. 183 y 184 del C.P.	132
5.1. Antecedentes	132
5.2. Bien jurídico	134
5.3. El tipo penal de daño de los arts. 183 y 184 del C.P.	135
5.3.1. Acción típica	135
5.3.2. Sujetos de la acción típica	140
5.3.3. Tipicidad subjetiva	140

5.3.4. Consumación / tentativa	141
5.3.5. Competencia judicial	141
5.4. El delito de daño agravado a través de medios informáticos	141
6. El tipo penal del art. 197 del C.P	143
6.1. Antecedentes	143
6.2. Bien jurídico	144
6.3. El tipo penal de interrupción o entorpecimiento de las comunicaciones	145
6.3.1. Acción típica	145
6.4. Resistencia violenta al restablecimiento de la comunicación interrumpida	147
6.4.1. Acción típica	147
6.4.2. Sujetos de la acción típica	147
6.4.3. Tipicidad subjetiva	148
7. El tipo penal del art. 255 del C.P	148
7.1. Antecedentes	149
7.2. Bien jurídico	149
7.3. El tipo penal de alteración, sustracción, ocultación, destrucción e inutilización de medios de prueba doloso	150
7.3.1. Acción típica	150
7.3.2. Sujetos de la acción típica	152
7.3.3. Resultado	153
7.3.4. Tipicidad subjetiva	153
7.3.5. Tentativa	153
7.4. El tipo penal de alteración, sustracción, ocultación, destrucción e inutilización de medios de prueba agravado	153
7.5. El tipo penal de alteración, sustracción, ocultación, destrucción e inutilización de medios de prueba culposo	154

Capítulo IV

Los tipos penales no abarcados por la ley 26.388 y la ausencia de una reforma procesal penal en materia de criminalidad informática

1. Introducción	157
1.1. El tipo penal de hurto (art. 162, C.P.)	159
1.2. El tipo penal de revelación de secretos de Estado y ultraje a símbolos patrios (art. 222, C.P.)	163
1.2.1. Delitos contra la seguridad de la Nación. Delitos que comprometen la paz y la dignidad de la Nación	163
1.3. Régimen Penal Cambiario (art. 1º, ley 19.359 complementaria del C.P.)	167
1.4. Régimen Penal Tributario (arts. 1º, 2º, 7º y 8º, leyes 24.769 y 26.735 complementaria del C.P.)	171
1.4.1. Debitos relativos a los recursos de la seguridad social	172
1.5. Derecho penal aduanero (arts. 864, 865, 866 y 867, Cód. Aduanero. Ley 22.415)	175
1.6. El tipo penal de estrago (art. 186, C.P.)	181
1.7. Los tipos penales de falsificación de documento público y documento privado y uso de documento falso o adulterado (arts. 292 y 296, C.P.)	184
2. La ausencia de una reforma procesal penal en materia de criminalidad informática	187

Capítulo V

La infraestructura tecnológica disponible por la administración de justicia.

¿El advenimiento de nuevas conductas

como consecuencia de una nueva tecnología?

1. La infraestructura tecnológica disponible por la administración de justicia	200
1.1. La ley 26.685 y el expediente digital	204
1.2. La computación de la nube o “cloud computing”	208
1.2.1. Concepto	208
1.2.2. Tipos de nube	211
1.2.3. Ventajas de la computación de la nube	212
1.2.4. Desventajas o riesgos de la computación de la nube	213
1.3. La implementación del expediente digital y su compatibilidad con el empleo de la computación de la nube	215
2. ¿El advenimiento de nuevas conductas como consecuencia de una nueva tecnología?	217
2.1. El derecho a las nuevas tecnologías y el acceso a Internet como derechos humanos emergentes	227

Capítulo VI

Ventajas y limitaciones de la ley 26.388 de reforma

al Código Penal de la Nación en materia de criminalidad informática

1. Ventajas de la reforma de la ley 26.388	233
2. Limitaciones de la reforma de la ley 26.388	239

Capítulo VII

Posibles actualizaciones en materia de criminalidad informática

1. Introducción: los antecedentes nacionales y las leyes de de reforma en materia de criminalidad informática al Código Penal de la Nación (leyes 26.388, 26.685 y 26.904)	247
2. La criminalidad informática en el Proyecto de Ley de Re- forma, Actualización e Integración al Código Penal de la Nación (dec. PEN 678)	251
2.1. Parte General. Terminología y definiciones	253
2.2. Parte Especial. El tipo penal de ofrecimiento y distribución de imágenes relacionadas con pornografía infantil (art. 128, C.P.)	254
2.3. Los tipos penales de violación de secreto y privacidad	256
2.3.1. Violación de correspondencia electrónica	257
2.3.2. Acceso ilegítimo a un sistema informático	259
2.3.3. Publicación abusiva de correspondencia	261
2.3.4. Revelación de secretos	263
2.3.5. Delitos relacionados con la protección de datos personales	264
2.3.6. Violación de privacidad o captación de imágenes y sonidos	265
2.4. El tipo penal de defraudación informática (art. 173, inc. 16, C.P.)	266
2.5. El tipo penal de daño	266
2.6. El tipo penal de interrupción o entorpecimiento de las comunicaciones.	268
2.7. El tipo penal de alteración, sustracción, ocultación, destrucción e inutilización de medios de prueba	270
3. Recomendaciones y sugerencias en torno a la actualización de la ley penal y procesal penal en materia de criminalidad informática	271
3.1. Tipos penales propuestos por otros proyectos de ley previos y no incorporados por las leyes 26.388, 26.904, ni por el Proyecto de Ley de Reforma, Actualización e Integración del Código Penal de la Nación (dec. 678)	273
3.2. Tipos penales previstos en leyes complementarias y no incorporados por las leyes 26.388, 26.904, ni por el Proyecto de Ley de Reforma, Actualización e Integración del Código Penal de la Nación (dec. 678)	274
3.3. La incorporación de nuevos tipos penales	275

4. Recomendaciones y sugerencias para la actualización de la infraestructura tecnológica y capacitación del personal de la administración de justicia	276
5. Recomendaciones y sugerencias para la actualización en materia de cooperación internacional	278
Anexos	
I. Convenio sobre Cibercriminalidad, Budapest, 2001	279
II. Estados miembros del Convenio sobre Cibercriminalidad actualizado al año 2014	307
III. Derecho comparado. Catálogo de delitos transnacionales que pueden perpetrarse a través de medios informáticos	309
Bibliografía	313