



Palazzi, Pablo Andrés
 Delitos informáticos / Pablo Andrés Palazzi. - 3a ed. - Ciudad Autónoma de Buenos Aires: Abeledo Perrot, 2016. 400 p.; 24 x 17 cm.

ISBN 978-950-20-2768-5

1. Cibercrimitos. 2. Delitos Informáticos. 3. Derecho Penal. I. Título.

CDD 345

© Pablo A. Palazzi, 2016
 © De esta edición, AbeledoPerrot S.A., 2016
 Tucumán 1471 (C1050AAC) Buenos Aires
 Queda hecho el depósito que previene la ley 11.723

Impreso en la Argentina

Todos los derechos reservados.
 Ninguna parte de esta obra puede ser reproducida o transmitida en cualquier forma o por cualquier medio electrónico o mecánico, incluyendo fotocopiado, grabación o cualquier otro sistema de archivo y recuperación de información, sin el previo permiso por escrito del Editor y el autor.

Printed in Argentina

All rights reserved.
 No part of this work may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording or by any information storage or retrieval system, without permission in writing from the Publisher and the author.

Tirada: 600 ejemplares
 ISBN: 978-950-20-2768-5
 SAP: 41976827

ARGENTINA

ÍNDICE GENERAL

Introducción a la tercera edición	I
Introducción a la segunda edición	V
Introducción a la primera edición.....	VII

PRIMERA PARTE

ANTECEDENTES DE LA REFORMA

CAPÍTULO I

I. Introducción	3
1. Fundamentación de la necesidad de reformas en el Código Penal..	3
2. Las falencias del Código Penal en materia de tecnologías de la información: reformas parciales con soluciones insuficientes.....	3
3. El problema de la criminalidad informática.....	6
II. Antecedentes de la reforma	10
1. Primeros antecedentes	10
2. Anteproyecto de reforma y actualización integral del Código Penal.....	12
III. La reforma de la ley 26.388	19

SEGUNDA PARTE

ANÁLISIS DE LA REFORMA

CAPÍTULO I

INTRODUCCIÓN

I. Panorama general de la reforma de la ley 26.388.....	25
II. Los nuevos conceptos y bienes jurídicos que introduce la reforma	26
III. Lo que faltó en la reforma del año 2008	29

CAPÍTULO II

**EL DELITO DE OFRECIMIENTO Y DISTRIBUCIÓN DE IMÁGENES
RELACIONADAS CON LA PORNOGRAFÍA INFANTIL, Y DE TENENCIA
CON FINES DE DISTRIBUCIÓN**

I. Antecedentes	31
1. Convenciones internacionales	32
2. Antecedentes nacionales	36
II. Iter legislativo del proyecto	36
III. Acciones punibles	38
1. Producción, ofrecimiento y distribución de pornografía infantil	38
2. Tenencia con fines de distribución	42
3. Otras modalidades relacionadas con la pornografía infantil	45
IV. Objeto material del delito	48
V. Elemento subjetivo	53
1. Dolo y dolo eventual	53
2. Servicios de hosting, motores de búsqueda y foros de intercambio en internet	53
3. Almacenamiento en memoria caché de un ordenador y distribución en redes p2p	57
VI. Concurso de figuras	58
VII. Competencia, jurisdicción internacional y otras cuestiones procesales	58

CAPÍTULO III

**VIOLACIÓN DE SECRETOS Y DE LA PRIVACIDAD –
ACCESO ILEGÍTIMO A SISTEMAS O DATOS INFORMÁTICOS –
PUBLICACIÓN INDEBIDA DE COMUNICACIONES ELECTRÓNICAS –
PROTECCIÓN PENAL DE LOS DATOS PERSONALES**

I. La reconfiguración del bien jurídico	67
II. Violación de correspondencia electrónica	71
1. El texto legal luego de la reforma	71
2. Antecedentes	71
3. Concepto de comunicación electrónica	74
4. Acciones punibles	76
4.1. Apertura o acceso a correspondencia	76
4.2. Apoderamiento de una comunicación electrónica y de papeles privados	78

4.3. Desvío o supresión de comunicaciones electrónicas	79
4.4. Interceptación indebida de comunicaciones electrónicas	80
4.5. Comunicación o publicación ilegítima	82
5. Elemento subjetivo	83
6. Situación del filtrado automático de comunicaciones	84
7. Quid del empleador que revisa las comunicaciones del empleado	89
8. Naturaleza de la acción	96
9. Competencia	96
III. Acceso ilegítimo a un sistema o dato informático	97
1. La reforma	97
2. Antecedentes y nociones generales	97
3. Bien jurídico protegido	101
4. Acción típica	101
5. Supuestos especiales	103
5.1. Spyware	103
5.2. Cookies	105
6. Acceso ilegítimo y ethical hacking	106
7. Supuesto del empleador que accede a su sistema informático propio	108
8. Ingeniería inversa y medidas de protección tecnológicas (DRM)	109
9. Cloud computing y acceso ilegítimo a la "nube"	113
10. Agravantes	114
IV. Publicación indebida de comunicaciones electrónicas	115
1. La reforma	115
2. Acción punible	116
3. Objeto del delito	117
4. Concepto de ilegitimidad	118
5. Consentimiento para la publicación de correspondencia	119
6. Supuesto de exención de responsabilidad penal	120
7. Delito de acción privada	122
V. Revelación de secretos	122
1. La reforma	122
2. Sujeto activo	123
3. Acción típica	123
4. Culpabilidad	124
5. Concurso con otras figuras	125
VI. Delitos relacionados con la protección de datos personales	125

1. Bancos de datos personales y derecho a la privacidad: evolución en el derecho comparado.....	125
2. Antecedentes y bien jurídico protegido.....	135
3. El texto reformado. Sus fundamentos.....	137
4. Las acciones punibles.....	138
4.1. Acceso no autorizado a un banco de datos personales.....	139
4.2. Proporcionar o revelar información registrada en un banco de datos.....	141
4.3. Inserción de datos en un banco de datos.....	145
5. Delito de acción privada.....	149
VII. El delito de captación ilegal de datos, imágenes y sonidos.....	150
1. El texto propuesto por la Cámara de Diputados.....	150
2. Eliminación del art. 153 ter por el Senado.....	151
3. Nuestra opinión.....	152

CAPÍTULO IV

LA ESTAFA INFORMÁTICA

I. Antecedentes.....	157
II. El nuevo texto legal.....	158
III. Modalidades de estafas informáticas.....	160
1. Alteración de registros informáticos.....	160
2. Uso no autorizado de tarjetas y claves falsas o sustraídas o de sus datos.....	160
3. Mise en scène en cajeros automáticos.....	163
4. Estafa de telecomunicaciones.....	163
5. Phising y robo de identidad.....	165
6. Estafas en mercados virtuales o con medios de pago virtuales.....	169
IV. Acción típica.....	171
V. El ardid informático.....	172
VI. Perjuicio patrimonial.....	175
VII. Competencia judicial.....	175

CAPÍTULO V

DAÑO A BIENES INTANGIBLES Y DISTRIBUCIÓN DE VIRUS INFORMÁTICOS

I. El nuevo texto legal.....	177
II. Antecedentes.....	177

III. Acción típica.....	178
IV. Objeto del delito.....	180
V. Elemento subjetivo.....	181
VI. Distribución de programas destinados a causar daños.....	182
VII. Situación legal de las medidas anticopia luego de la reforma.....	188
VIII. Daño informático agravado.....	190
IX. Competencia judicial.....	191
X. Derecho comparado.....	192

CAPÍTULO VI

INTERRUPCIÓN DE COMUNICACIONES ELECTRÓNICAS

I. Antecedentes.....	195
II. Análisis del texto legal.....	195
III. Elemento subjetivo.....	197
IV. Supuestos especiales relacionados con internet.....	198
1. Deep packet inspection.....	198
2. Tecnología antipiratería.....	199
3. Clausura de cuenta de usuarios.....	199

CAPÍTULO VII

ALTERACIÓN DE PRUEBAS

I. Texto sancionado.....	201
II. Antecedentes.....	201
III. Objeto.....	202
IV. Acciones atípicas.....	203
V. Elemento subjetivo.....	203

TERCERA PARTE

DIMENSIÓN INTERNACIONAL DEL DELITO INFORMÁTICO

I. Introducción.....	205
1. El contexto internacional de los delitos informáticos.....	205
2. El Convenio del Cibercrimen del Consejo de Europa. Sus antecedentes.....	208

3. Estado actual del Convenio del Cibercrimen	210
4. Incorporación de terceros países al Convenio	211
5. Intervención de otros organismos internacionales en el cibercrimen	212
II. Aspectos sustantivos del convenio del cibercrimen	214
1. Definiciones	214
2. Medidas que deben ser adoptadas a nivel nacional	216
3. Infracciones contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos	217
3.1. Acceso ilegítimo	217
3.2. Interceptación ilícita	218
3.3. Atentados contra la integridad de los datos y del sistema	219
3.4. Abuso de equipos e instrumentos técnicos	220
4. Infracciones informáticas	221
4.1. Falsedad informática	221
4.2. Estafa informática	221
5. Infracciones relativas al contenido	222
5.1. Infracciones relativas a la pornografía infantil	222
5.2. Infracciones vinculadas a los atentados a la propiedad intelectual	223
III. Aspectos procesales del convenio	224
1. Ámbito de aplicación de las medidas de derecho procesal	225
2. Derechos y garantías constitucionales involucrados en la ejecución de medidas procesales	225
3. Medidas a adoptar relativas a pruebas informáticas	230
3.1. Conservación de datos informáticos almacenados	230
3.2. Conservación y divulgación inmediata de los datos de tráfico	231
3.3. Mandato de comunicación	232
3.4. Secuestro y decomiso de datos informáticos almacenados	233
3.5. Recolección en tiempo real de datos informáticos	234
3.6. Interceptación de datos relativos al contenido	234
3.7. Jurisdicción	235
IV. Cooperación internacional	236
1. Principios generales relativos a la cooperación internacional	236
2. Principios relativos a la extradición	237
3. Principios generales relativos a la colaboración	237
3.1. Información espontánea	239
3.2. Procedimiento relativo a las demandas de colaboración en ausencia de acuerdo internacional aplicable	240
4. Cooperación en materia de medidas cautelares	240

4.1. Medidas que se pueden solicitar	240
4.2. Acceso transfronterizo a los datos informáticos almacenados, con consentimiento o de libre acceso	241
V. Otros instrumentos internacionales	243
1. Protocolo adicional al Convenio sobre actos racistas o xenófobos cometidos a través de medios informáticos	243
2. Convenio del Consejo de Europa para la protección de los menores contra la explotación y el abuso sexual	245
3. Acuerdo comercial anti-falsificación (Anti Counterfeiting Trade Agreement)	247

ANEXO LEGISLATIVO

CUADRO COMPARATIVO DE LA LEY 26.388
Y EL CÓDIGO PENAL

Acuerdo de confidencialidad y acceso a servidores para testeado de fallas de seguridad	303
Anexo I	305
Políticas internas de seguridad de XYZ	305