

Índice

Dedicatoria	XV
Prólogo	XXXV
Introducción	XXXVII
Abreviaturas	XLI

Capítulo I

LA INFORMÁTICA DESDE EL DERECHO

1. Generalidades	43
2. Las Tecnologías de la Información y Comunicación	44
2.1. La comunicación	44
2.2. La información	46
2.3. Procesamiento y mensaje de datos	46
3. Derecho informático como ciencia	47

Capítulo II

RELACIÓN DE LA INFORMÁTICA CON OTRAS CIENCIAS DEL DERECHO

1. Generalidades	51
2. Relación del Derecho Civil con el Derecho Informático	53
2.1. Obligaciones	53
2.2. Sanciones por incumplimiento de obligaciones	55
2.3. Actos o declaraciones de voluntad	56
2.4. Del error, fuerza y dolo como vicios del consentimiento	57
2.5. Capacidad Legal	59
2.6. Del Objeto lícito	60
2.7. De la causa lícita	60
2.8. Efectos de las Obligaciones	61
2.9. Del contrato o convención	62
2.10. Clasificación de los contratos	63

3. Derecho Mercantil, Informática y Comercio Electrónico en el Ecuador	65
3.1. La firma electrónica	65
3.2. Relación entre la firma digital y la firma manuscrita	65
3.3. De la falsedad documental y de alteración de los mensajes de datos	67
3.3.1. Partes del documento	67
3.3.2. De la falsedad documental	68
3.3.3. Falsedad material	68
3.3.4. Falsedad ideológica	69
3.3.5. Falsedad Ideal	69
3.3.6. La falsificación	69
3.6.7. La forjadura	69
3.6.8. Análisis de la participación desde la teoría del delito	70
3.6.9. Alteración de mensaje de datos	71
3.3. Validez de las firmas manuscritas y las firmas electrónicas	72
3.4. El consentimiento en la informática	72
3.4.1. Consentimiento para aceptar mensajes de datos	72
3.4.2. Consentimiento para el uso de los medios electrónicos	73
3.4.3. Del contrato electrónico y de su validez	74
3.4.4. Perfeccionamiento y aceptación de los contratos electrónicos	76
3.4.5. Jurisdicción consensual y legal	78

Capítulo III

EL DATO INFORMÁTICO Y LA VULNERACIÓN DE LOS SISTEMAS AUTOMATIZADOS DE INFORMACIÓN

1. El dato informático y las TIC	81
2. Vulneración de los sistemas automatizados de información	83
3. El dato como componente esencial del elemento descriptivo en el tipo objetivo del delito informático	90
4. El elemento normativo en el tipo objetivo del delito informático	96
5. Diferencia entre los delitos informáticos propios e impropios	97

*Capítulo IV***LA CONFIDENCIALIDAD INTEGRIDAD Y
DISPONIBILIDAD DE DATOS COMO BIEN JURÍDICO
EN EL DELITO INFORMÁTICO**

1. Antecedentes históricos de la teoría del bien jurídico	101
2. Definiciones	104
3. Posiciones contrapuestas	107
4. Elementos para categorizar un hecho social de interés vital como bien jurídico	110
4.1. Necesidad individual y colectiva como elemento básico del bien jurídico	112
4.2. Importancia del hecho de interés vital para el funcionamiento del sistema	113
4.3. Amenaza al interés vital mediante daño individual, colectivo o social	114
4.4. Vinculación con los derechos fundamentales	115
4.5. Valor constitucionalmente relevante	116
5. La confidencialidad, integridad y disponibilidad de datos en la informática	117
6. Teorías sobre el bien jurídico en el delito informático	120
7. Definición de la confidencialidad, integridad y disponibilidad de datos como bien jurídico	122
8. Estructura del bien jurídico confidencialidad, integridad y disponibilidad de datos informáticos	125
8.1. Primer elemento: Utilidad de la informática para las personas	125
8.2. Segundo elemento: Categorización de interés vital para la sociedad	126
8.3. Tercer elemento: Importancia para el funcionamiento de su propio sistema	129
8.4. Cuarto elemento: Afectación social por vulneración de la privacidad de la información y los datos informáticos	132
8.5. Quinto elemento: Del acceso autorizado y el derecho a la disponibilidad de los datos informáticos	136
8.6. Sexto elemento: El daño a los componentes lógicos y su afectación a la integridad de los sistemas informáticos	140

8.7. Séptimo elemento: Los datos informáticos personales como Derecho Humano	143
8.8. Octavo elemento: Valoración constitucionalmente relevante	147

Capítulo V

DERECHO PENAL INFORMÁTICO

1. Definición de derecho penal informático	149
1.1. Criminalidad científica	150
1.1.1. Anonimato	152
1.1.2. Bajo costo	152
1.1.3. La vulnerabilidad de los sistemas informáticos	152
1.1.4. La confidencialidad, integridad y disponibilidad como nuevos bienes jurídicos	153
1.2. Características del delincuente informático	153
1.3. La delincuencia informática en el contexto social	156
2. Clasificación de los delitos informáticos desde el iter críminis	158
3. Nuevo paradigma del Derecho Penal Informático, con base al bien jurídico confidencialidad, integridad y disponibilidad de datos	162
3.1. La informática y el derecho	162
3.2. La seguridad de la información	163
3.3. La sociedad de la información	164
3.3.1. Elementos que conforman la sociedad de la información	167
3.3.2. La Sociedad de la Información y su función en las TIC	168
4. Esquema doctrinario del derecho penal informático desde la confidencialidad, integridad y disponibilidad de datos	171
5. Principios del Derecho penal informático	173
5.1. Principio de autodeterminación informática	175
5.2. Principio de seguridad de la información	175
5.3. Principio de seguridad informática	175
5.4. Principio de confidencialidad	176
5.5. Principio de integridad	176
5.6. Principio de disponibilidad	176
5.7. Principio de privacidad informática	176
5.8. Principio de intimidad	176

6. El tipo penal informático construido desde la confidencialidad, integridad y disponibilidad de datos	176
6.1. La acción en el delito informático	177
6.2. Tipo objetivo	178
6.2.1. El tipo objetivo informático	178
6.2.2. Elementos descriptivos	179
6.2.3. Elemento normativo	179
6.2.4. Imputación al tipo objetivo	179
6.2.4.a. Teoría de la causalidad	181
6.2.4.b. Teoría del nexo causal	182
6.2.4.c. Teoría de la equivalencia de las condiciones	182
6.2.4.d. Teoría de la adecuación	182
6.2.5. Del riesgo permitido	183
6.2.6. Normas de cuidado en el riesgo permitido	183
6.2.7. La conducta imprudente en los delitos informáticos	184
6.2.8. Bien jurídico	187
6.2.9. Verbos núcleos del tipo	187
6.3. Tipo subjetivo	190
6.3.1. El dolo	191
6.3.2. Sujeto activo de la infracción	193
6.4. Antijuridicidad	195
6.5. Culpabilidad	197
6.6. Punibilidad	200
6.6.1. Teoría de la retribución de la pena	200
6.6.2. Teoría de la prevención especial	201
6.6.3. Teoría de la prevención general	202
7. Política criminal	202
7.1. Origen de la conducta delictiva	203
7.2. La prevención del delito informático	205
7.3. La encriptación cuántica como forma de prevención del delito informático	205
7.4. Políticas informativas acerca de los riesgos del delito informático y de su prevención	208

*Capítulo VI***DERECHO PENAL INFORMÁTICO
EN EL ECUADOR**

1. Principios en los que se fundamenta el Derecho penal ecuatoriano	216
1.1. Principios constitucionales de Derecho penal	217
1.1.a. Principio de legalidad	217
1.1.b. Principio in dubio pro-reo	218
1.1.c. Principio de favorabilidad	219
1.1.d. Principio de inocencia	220
1.1.e. Principio de no autoincriminación	221
1.1.f. Principio de igualdad	222
1.1.g. Principio de proporcionalidad de la pena	223
1.1.h. Principio de mínima intervención penal	223
1.1.i. Principio non bis in ídem	225
1.1.j. Principio de seguridad jurídica	226
1.1.k. Principio de motivación	227
1.1.2. Principios del Derecho penal	228
1.1.2.a. Principio dispositivo	228
1.1.2.b. Principio de oralidad	228
1.1.2.c. Principio de concentración	229
1.1.2.d. Principio de inmediación	230
1.1.2.e. Principio de contradicción	231
1.1.2.f. Principio de la verdad procesal	231
1.1.2.g. Principio de simplificación	232
1.1.2.h. Principio de celeridad	235
1.1.2.i. Reformatio in peius	236
1.1.2.j. Principio de objetividad	236
2. Principios del Derecho penal informático en la República del Ecuador	237
2.1. Principio de autodeterminación informática	240
2.2. Principio de seguridad de la información	241
2.3. Principio de seguridad informática	241
2.4. Principio de confidencialidad	242
2.5. Principio de integridad	242

2.6. Principio de disponibilidad	243
2.7. Principio de privacidad informática	243
2.8. Principio de intimidad	243
3. El Código Orgánico Integral Penal y los delitos informáticos	244
3.1. De la revelación de información y atentado a la intimidad y privacidad	244
3.2. De la interceptación ilegal	245
3.3. Del engaño informático	251
3.4. De la comercialización ilegal	258
3.5. Del auxilio y participación en el ilícito informático	261
3.6. Del lucro ilegal y de las transferencias electrónicas	262
3.7. Ataque a los sistemas automatizados de información	264
3.7.a. El Virus informático	269
3.7.b. Gusanos de internet	269
3.7.c. Bomba lógica o cronológica	270
3.8. De la destrucción de la información clasificada	272
3.9. Del hackeo o acceso no autorizado	274
3.10. De la falsificación informática como nuevo tipo penal en la legislación ecuatoriana	277
3.11. Delitos informáticos contra el derecho a la propiedad	280
3.12. De la comercialización ilegal y del uso indebido de equipos terminales móviles (celulares)	281
3.13. Del delito sexual y los sistemas de información	286
4. Bienes jurídicos en los delitos informáticos tipificados en el Código Orgánico Integral Penal	287
5. La ciberdelincuencia y la Política Criminal en el Ecuador	288

Capítulo VII

ESTUDIO COMPARADO

1. Punto de partida en el estudio comparado	295
2. ARGENTINA	296
2.1. Principios en los que se desarrolla el derecho penal argentino	296
2.1.1. Principio de legalidad	296
2.1.2. Principio de retroactividad y ultraactividad de la ley penal	298

2.1.3. Principio de proporcionalidad	299
2.1.4. Principio de subsidiariedad y fragmentariedad	300
2.1.5. Principio de reserva y lesividad	301
2.1.6. Principio de exterioridad de la acción	301
2.1.7. Principio de culpabilidad	302
2.1.8. Principio de personalidad de la pena y resocialización	303
2.1.9. Principio de judicialidad	304
2.2. Principios del Derecho penal informático	304
2.2.1. Principio de autodeterminación informática	305
2.2.2. Principio de seguridad de la información	305
2.2.3. Principio de seguridad informática	306
2.2.4. Principio de confidencialidad	306
2.2.5. Principio de integridad	307
2.2.6. Principio de disponibilidad	308
2.2.7. Principio de privacidad informática	308
2.2.8. Principio de intimidad	309
2.3. Resoluciones que sirvieron de detonante en la República Argentina para la tipificación de los delitos informáticos	309
2.4. Análisis estructural de la ley 26.388 desde la teoría del delito	310
2.4.1. El delito contra la integridad sexual mediante medios informáticos	310
2.4.2. Los delitos contra la violación de secretos y de la privacidad por medios informáticos	313
2.4.2.a. Del delito de acceso indebido a comunicación electrónica	313
2.4.2.b. El delito de acceso no autorizado a sistemas automatizados de información (hacking)	316
2.4.2.c. El delito de publicación indebida de comunicación electrónica	319
2.4.2.d. El delito de revelación de hechos, actuaciones, documentos o datos	322
2.4.2.e. El delito de protección de datos personales	323
2.4.3. Los delitos contra la propiedad en la ley 26.388	325
2.4.3.a. Estafas y otras defraudaciones	326

2.4.3.b. Del daño informático	327
2.4.4. El delito de interrupción informática	329
2.4.5. Del delito de abuso de autoridad y violación de los deberes de los funcionarios públicos desde la informática	330
2.4.5.a. La falsedad documental y la alteración de datos en el documento electrónico	330
2.4.5.b. El objeto material y la alteración de datos en el documento digital	333
2.5. Los bienes jurídicos que protegen los delitos informáticos en la República Argentina	335
2.5.1. El bien jurídico en el delito contra la integridad sexual mediante medios informáticos	336
2.5.2. El bien jurídico en los delitos contra la violación de secretos y de la privacidad por medios informáticos	337
2.5.3. El bien jurídico en el delito de hackeo o acceso no autorizado a sistemas de información	338
2.5.4. La publicación indebida de comunicación electrónica y el bien jurídico	339
2.5.5. El bien jurídico en el delito de revelación de hechos, actuaciones, documentos o datos	339
2.5.6. El bien jurídico en el delito de protección de datos personales	340
2.5.7. El bien jurídico en los delitos contra la propiedad de la ley 26.388	340
2.5.8. El bien jurídico en el delito de interrupción informática	342
2.5.9. El bien jurídico en el delito de abuso de autoridad y violación de los deberes de los funcionarios públicos desde la informática	343
2.6. Estrategia Nacional de Ciberseguridad y la ciberdelincuencia en la República Argentina	344
2.7. Análisis General del Derecho Penal Informático en la República Argentina	349
4. CHILE	355
4.1. La información en la Constitución de la República de Chile	355

4.2. El bien jurídico protegido en los delitos informáticos en Chile	356
4.3. Análisis de la ley 19.223 que tipifica los delitos informáticos	359
4.4. Principios aplicables al Derecho penal chileno	362
4.4.1. Principio de legalidad Constitucional	362
4.4.2. Principio de legalidad en el Código Penal	363
4.4.3. Principio de culpabilidad	364
4.4.4. Principio non bis in ídem	365
4.4.5. Principio de proporcionalidad	366
4.4.6. Principio de igualdad	366
4.4.7. Principio de inocencia	367
4.5. Principios aplicables al derecho penal informático en la República de Chile	368
4.5.1. Principio de libertad en el tratamiento de datos personales	368
4.5.2. Principios de información y consentimiento del titular	368
4.5.3. Principio de finalidad	369
4.5.4. Principio de calidad de datos	370
4.5.5. Principio de protección especial de los datos sensibles	370
4.5.6. Principio de seguridad de datos	371
4.5.7. Principio del deber de secreto	371
4.6. Política criminal en la República de Chile	372
4.7. Bien jurídico, delitos informáticos y políticas públicas entre Argentina y Chile	374
5. BOLIVIA	378
5.1. Antecedentes en cuanto los delitos informáticos en la República de Bolivia	378
5.2. La Constitución Boliviana y las Tecnologías de la Información y Comunicación	380
5.3. Los delitos informáticos en la República de Bolivia y su bien jurídico	381
5.3.1. De la manipulación informática	381
5.3.2. Del hackeo, la alteración y el uso indebido de datos	382
5.4. La protección de datos	383

5.5. Principios de la Ley de Telecomunicaciones aplicables a los delitos informáticos en Bolivia	385
5.6. La Seguridad Informática y las Políticas Públicas en el Estado Plurinacional de Bolivia	386
5.7. Cibercrimitos, seguridad informática y ciberpolticas en Bolivia y Argentina	390
6. PERÚ	394
6.1. Los cibercrimitos y sus reformas	394
6.2. Bienes jurídicos informáticos en la legislación peruana	396
6.3. Los delitos informáticos en la República del Perú	396
6.3.1. Acceso ilícito	396
6.3.2. Delito contra la integridad de los datos informáticos	398
6.3.3. Delitos informáticos contra la indemnidad y libertad sexual	398
6.3.4. Delitos contra la intimidad y el secreto de las comunicaciones	400
6.3.5. Delitos informáticos contra el patrimonio	404
6.3.6. Delitos informáticos contra la fe pública	405
6.4. La protección de datos en la República del Perú	407
6.5. Los principios aplicables en la legislación penal informática	408
6.5.1. De la confidencialidad y seguridad de datos personales informatizados	408
6.5.2. De la integridad de los datos	409
6.5.3. Derecho a la disponibilidad y acceso del titular a los datos personales	409
6.6. Política criminal en la República del Perú	410
6.7. Argentina y Perú frente a los delitos informáticos y políticas públicas para enfrentarlos	412
7. VENEZUELA	414
7.1. Los bienes jurídicos protegidos en la legislación penal venezolana	414
7.2. Los delitos informáticos en la legislación venezolana	417
7.2.1. Delitos informáticos propios e improprios	417
7.2.2. Diferencia entre las tecnologías de la información y las tecnologías de la comunicación	418

7.2.3. Del delito de hacking o acceso no autorizado	419
7.2.4. Del Sabotaje o daño a un sistema automatizado de información, sus datos y componentes físicos	421
7.2.5. La culpa en los delitos informáticos	423
7.2.5.1. Imputación al tipo objetivo en los delitos informáticos en Venezuela	424
7.2.5.2. Imprudencia, negligencia e impericia en los delitos informáticos venezolanos	425
7.2.5.3. El Hardening y la infracción al deber objetivo de cuidado en el delito informático culposo	428
7.2.6. Posesión o uso de dispositivos y programas para sabotaje informático	430
7.2.7. Del delito de espionaje informático en Venezuela	431
7.2.8. De la falsedad y falsificación de documentos electrónicos	433
7.2.8.1. La falsedad documental	433
7.2.8.2. El tipo penal de falsificación de documentos y TIC	435
7.2.9. Delitos contra la propiedad	436
7.2.9.1. Del hurto y del fraude electrónico	436
7.2.9.2. Las tarjetas inteligentes y los tipos penales informáticos	437
7.2.10. De los delitos contra la privacidad de las personas y las comunicaciones	441
7.2.11. De la pornografía infantil y las TIC	443
7.2.12. Delitos contra la propiedad intelectual en internet	444
7.3. Principios del Derecho penal informático en la República de Venezuela	445
7.4. Política criminal en la República Bolivariana de Venezuela respecto a los delitos informáticos	447
7.5. Enunciados comparativos entre Venezuela y Argentina y el delito informático culposo en estas legislaciones	452
8. URUGUAY	455
8.1. La Constitución y la informática en la República Oriental del Uruguay	455
8.2. Principios generales sobre la protección de datos en la República del Uruguay	457

8.2.1. Principio de legalidad	458
8.2.2. Principio de veracidad	459
8.2.3. Principio de finalidad	459
8.2.4. Principio de previo consentimiento informado	460
8.2.5. Principio de seguridad de datos	460
8.2.6. Principio de reserva	461
8.3. La legislación uruguaya en el contexto del delito informático	462
8.4. Los bienes jurídicos en el contexto informático en la legislación uruguaya	466
8.5. Políticas de seguridad cibernéticas en la República Oriental del Uruguay	468
8.6. Datos personales y principios informáticos en Uruguay y Argentina	472
9. PARAGUAY	474
9.1. Bosquejo constitucional y legal de la ruta seguida por las Tecnologías de la Información y Comunicación en la República del Paraguay	474
9.2. Delitos informáticos en la República del Paraguay	476
9.2.1. Hacking. Acceso indebido a sistemas informáticos	476
9.2.2. Del Sabotaje informático	477
9.2.3. Pornografía infantil	477
9.2.4. Acceso indebido a datos	477
9.2.5. De la interceptación de datos	478
9.2.6. Del acceso indebido e interpretación de datos	478
9.2.7. El patrimonio y el injusto penal informático	479
9.2.8. De la destrucción o daño	480
9.2.9. Falsificación de tarjetas de crédito, débito y otros medios electrónicos	481
9.2.10. De la equiparación en el procesamiento de datos	482
9.3. El bien jurídico en los delitos informáticos en Paraguay	483
9.4. Política de Estado sobre ciberseguridad y delitos informáticos en Paraguay	484
9.5. Similitud en cuanto a ciberdelitos en Paraguay y Argentina	489

10. ESTADOS UNIDOS DE AMÉRICA	491
10.1. Antecedentes	491
10.2. Delitos informáticos en la legislación federal estadounidense	495
10.2.1. De la obtención de información protegida contra la seguridad nacional	495
10.2.2. Del acceso a una computadora y obtención de información	496
10.2.3. De la invasión de una computadora del Gobierno	499
10.2.4. Del acceso, fraude y obtención de valores	500
10.2.5. Del daño de computadora o información	501
10.2.6. Del tráfico de contraseñas	504
10.2.7. De la amenaza de causar daño a una computadora protegida	506
10.2.8. De la interceptación de comunicaciones	509
10.2.9. De la divulgación de una comunicación interceptada	512
10.2.10. Del uso de una comunicación interceptada	513
10.2.11. Del acceso ilegal a comunicaciones almacenadas	515
10.2.12. Del robo de identidad	518
10.2.13. Del fraude del dispositivo de acceso	520
10.2.14. Ley CAN-SPAM. Del Correo no deseado	520
10.2.15. Del fraude electrónico	522
10.2.16. De la interferencia de las comunicaciones	524
10.3. El principio de daño o Harm Principle	525
10.4. Política criminal en cuanto a los delitos informáticos en los Estados Unidos de Norteamérica	529
10.5. El principio de daño y el bien jurídico entre EE. UU. y la Argentina	531
11. INGLATERRA	533
11.1. Antecedentes	533
11.2. Delitos informáticos en Inglaterra	535
11.2.1. (1.) Acceso no autorizado a un material de computadora	535
11.2.2. (2.) Acceso no autorizado con intención de cometer o facilitar la comisión de futuras infracciones	537

11.2.3. (3.) Actos no autorizados con la intención de perjudicar, o con imprudencia en cuanto al deterioro o funcionamiento de una computadora, etc.	538
11.2.4. (3ZA) Actos no autorizados que causan o crean riesgos o daños graves	541
11.2.5. (3A) Fabricación, suministro u obtención de artículos para comisión de delitos de la sección 1, 3 o 3ZA	544
11.3. Política Criminal en el Reino Unido	547
11.4. El Common Law y el principio de legalidad entre Inglaterra y Argentina	553
12. Sistemas legales con fundamento en la confidencialidad, integridad y disponibilidad de datos informáticos como bien jurídico en los ciberdelitos	555
12.1. ESPAÑA	555
12.1.1. Antecedentes históricos de los delitos informáticos en España	555
12.1.2. Los delitos informáticos en España según el bien jurídico que protegen	558
12.1.3. Delitos informáticos con finalidad económica	559
12.1.3.a. De la estafa informática	559
12.1.3.b. De la Defraudación utilizando un equipo terminal de telecomunicaciones	560
12.1.3.c. Del hurto con uso de equipo terminal de telecomunicaciones	562
12.1.3.d. Del daño informático	563
12.1.3.e. De la denegación de servicio	564
12.1.3.f. Del virus informático como medio para el delito de daño	564
12.1.3.g. Del delito contra la propiedad intelectual	565
12.1.3.h. Del espionaje informático en los delitos relativos al mercado y a los consumidores	567
12.1.3.i. Difusión de datos económicos engañosos por internet	569
12.1.4. Delitos informáticos propios en España	569
12.1.5. Las Tecnologías de la Información y Comunicación como medios para cometer otros ilícitos	572

12.1.5.a. Delitos informáticos y las conductas contra la indemnidad sexual	572
12.1.5.b. Delitos contra la Constitución y las TIC	574
12.1.5.c. Delitos informáticos con finalidad terrorista	575
12.1.6. La protección de datos personales en el Reino de España	575
12.1.6.a. Los derechos digitales en la legislación española	576
12.1.6.b. Principios de protección de datos	578
12.1.7. Estrategia Nacional de Ciberseguridad como política pública contra la ciberdelincuencia	579
12.1.8. La protección de datos personales en España y Argentina	585
12.2. COLOMBIA	587
12.2.1. La información en la Constitución de la República de Colombia	587
12.2.2. El bien jurídico en los delitos informáticos en Colombia	588
12.2.3. Análisis estructural de los delitos informáticos en Colombia	591
12.2.3.a. Del acceso abusivo a un sistema informático	592
12.2.3.b. De la obstaculización ilegítima del sistema informático o red de telecomunicación	594
12.2.3.c. De la interceptación de datos informáticos	597
12.2.3.d. Del daño informático	601
12.2.3.e. Del uso de software malicioso	604
12.2.3.f. De la violación de datos personales	605
12.2.3.g. De la suplantación de sitios web para capturar datos personales	608
12.2.3.i. Del hurto por medios informáticos y semejantes	612
12.2.3.j. De la transferencia no consentida de activos	618
12.2.4. Principios del Derecho penal en Colombia	628
1.2.4.a. Principio de legalidad	628
1.2.4.b. Principio de igualdad	629
1.2.4.c. Principio de prohibición de doble incriminación	630

1.2.4.d. Principio de tipicidad penal	631
1.2.4.e. Principio de la antijuridicidad	632
1.2.4.f. Principio de culpabilidad	633
1.2.4.g. Principio de legalidad de la pena	633
1.2.4.h. Principio de integración	634
1.2.4.i. Principio de dignidad humana	635
12.2.5. Principios aplicables al derecho penal informático en Colombia	635
12.2.5.a. Principio de autodeterminación informática	635
12.2.5.b. Principio de seguridad de la información	636
12.2.5.c. Principio de seguridad informática	637
12.2.5.d. Principio de confidencialidad	638
12.2.5.h. Principio de integridad	639
12.2.5.i. Principio de disponibilidad	639
12.2.5.j. Principio de privacidad informática	640
12.2.5.k. Principio de intimidad	640
12.2.6. Política Criminal en la República de Colombia	641
12.2.7. La confidencialidad, integridad y disponibilidad de datos en Colombia y Argentina	643
13. Instituciones jurídicas paralelas a la Teoría del Bien Jurídico	646
Referencias bibliográficas	649