
Índice

Abreviaturas	15
Presentación de la segunda edición	19
Presentación de la primera edición	21
Capítulo I. Las nuevas tecnologías y la protección penal de la intimidad	23
1. El derecho a la vida privada	25
2. Privacidad <i>versus</i> nuevas tecnologías	25
3. Breve reseña del derecho a la privacidad en la Argentina	30
3.1. La privacidad en la Constitución Nacional	30
3.2. La privacidad en el Código Penal argentino de 1921	32
3.3. El derecho a la privacidad en el Derecho Procesal Penal	33
3.4. La privacidad en las leyes de correos y comunicaciones	37
3.5. El derecho a la intimidad en las normas del Derecho privado	39
3.6. La privacidad en la Ley de Protección de Datos Personales	41
3.7. La privacidad en la Ley de Delitos Informáticos	44
3.8. Privacidad en la Convención del Ciberdelito	46
3.9. Privacidad en la Convención 108	48
3.10. Ley de Teletrabajo	50
3.11. Otras normas que hacen referencia a la privacidad	51
4. Evolución legislativa	54
4.1. El caso de Estados Unidos	54
4.2. El caso de la Unión Europea	63
5. Desafíos de la protección penal de la privacidad	68
6. La intimidad informática como nueva esfera de protección	73

Capítulo II. Violación de correspondencia electrónica	77
1. Antecedentes	79
2. Bien jurídico protegido	82
3. Alcance del término comunicación electrónica	84
3.1. Concepto de correspondencia en el Código Penal	84
3.2. Concepto de comunicación electrónica	85
3.3. Datos de contenido y datos de tráfico (metadatos)	88
3.4. Comunicaciones en tránsito y almacenadas	94
4. Acciones punibles	97
4.1. Apertura y acceso a correspondencia electrónica	97
4.2. Apoderamiento de una comunicación electrónica y de papeles privados contenidos en soportes digitales	99
4.3. Desvío o supresión de comunicaciones electrónicas	103
4.4. Interceptación indebida de comunicaciones electrónicas	106
4.5. Comunicación o publicación ilegítima	112
4.6. Agravante del hecho cometido por funcionario público	113
4.7. Concurso y relaciones con otras figuras	113
5. Culpabilidad	115
6. Ilegitimidad	117
7. Acciones no punibles. Casos especiales	118
7.1. Revisión y filtrado automático de comunicaciones	118
7.2. Correo electrónico empresarial	124
a) Doctrina	126
b) Jurisprudencia	128
c) Acceso al correo electrónico en relaciones de empleo público	135
d) Consentimiento del empleado. Validez	139
e) El argumento propiedad <i>versus</i> privacidad	141
f) Nulidad de la prueba ilegal <i>versus</i> delito penal	141
g) Reglamento de uso del correo electrónico laboral del empleado	144
h) La Ley de Teletrabajo y uso de "software de vigilancia" dentro de la empresa	145
i) Conclusiones	147
7.3. Patria potestad y comunicaciones electrónicas de menores	148
7.4. Requisas privadas y hallazgos casuales	153
7.5. Acceso con orden judicial	157

8. Aspectos procesales	158
8.1. Naturaleza de la acción	158
8.2. Competencia federal	160
8.3. Persona legitimada para querellar	163
Capítulo III. Espionaje y vigilancia estatal	165
1. Introducción	167
2. Derecho Comparado	169
3. Marco legal de los organismos de inteligencia en la Argentina	170
3.1. Antecedentes	170
3.2. Evolución legislativa	177
3.3. Límites legales a las actividades de inteligencia	177
3.4. El caso Nisman y la reforma de la Ley de Inteligencia	185
3.5. Marco legal de las “escuchas telefónicas”	186
3.6. Marco legal del uso estatal de datos de fuentes públicas (OSINT)	188
3.6.1. Concepto	188
3.6.2. Normas para la investigación OSINT en Argentina	191
Resolución 31/2018	191
Resolución 144/2020	193
Texto completo de la Resolución 144/2020	195
Resolución 720/2022	204
Resolución 428/2024 del Ministerio de Seguridad (BO 28/5/2024)	205
Texto completo de la Resolución 428/2024	206
Estatuto de la PFA	214
4. Estructura de la Ley de Inteligencia	215
4.1. Prohibiciones en la Ley de Inteligencia	215
4.2. Figuras penales previstas en la Ley de Inteligencia	216
4.3. Omisiones de la Ley de Inteligencia	217
4.4. Cuadro comparativo de la reforma	218
5. Interceptación indebida de comunicaciones (escuchas ilegales)	219
5.1. Bien jurídico protegido	219
5.2. Sujeto activo	221
5.3. Acción punible	221
5.4. Elemento subjetivo	222
6. Omisión de destrucción de escuchas telefónicas	222

6.1. Bien jurídico protegido	222
6.2. Sujeto activo	223
6.3. Omisión punible	223
6.4. Elemento subjetivo	225
7. Acciones ilegales de inteligencia	226
7.1. Bien jurídico protegido	226
7.2. Acción punible	226
7.3. Sujeto activo	228
Capítulo IV. Acceso no autorizado a sistemas informáticos	229
1. Antecedentes y nociones generales	231
2. Introducción de la figura en el Derecho argentino	236
3. Críticas y reparos. Los abusos del acceso no autorizado	238
4. Bien jurídico protegido. Distintas teorías	241
5. Acción típica	246
6. ¿Cuándo el acceso es no autorizado? Indiferencia de la finalidad del sujeto activo	253
7. Casos especiales	256
7.1. Acceso a teléfonos móviles	256
7.2. Herramientas y programas para acceso no autorizado (<i>spyware</i> con fines de inteligencia)	259
7.3. Acceso no autorizado para defensas activas contra accesos no autorizados (<i>hackbacks</i>)	264
7.4. Acceso no autorizado a sistemas SCADA	266
7.5. Acceso no autorizado a redes wi-fi	269
7.6. Acceso no autorizado a la Internet de las cosas y asistentes personales virtuales	270
7.7. Acceso ilegítimo a datos en la "nube"	272
7.8. <i>Hacking</i> de automotores	274
7.9. Software <i>spyware</i> comercial y para amparar derecho de autor	277
7.10. Archivos para identificar sesiones (<i>cookies</i>)	280
7.11. Acceso con cuentas bloqueadas o canceladas	283
7.12. Acceso por ex empleados o ex proveedores	285
7.13. Testeo de fallas de seguridad (<i>ethical hacking</i> o <i>good faith hacking</i>)	287

7.14. Programas de recompensa (<i>bug bounty</i>) por informar vulnerabilidad de datos o sistemas informáticos	294
7.15. Investigaciones en seguridad y publicación de vulnerabilidades de sistemas informáticos	298
7.16. <i>Hacktivismo</i> y protesta social en Internet	301
7.17. Acceso no autorizado en redes sociales	303
a) Acceso a un perfil público de un usuario de la red social	304
b) Acceso no autorizado a un perfil de una red social	305
c) Acceso a un perfil cerrado a través de un "amigo"	306
d) Acceso a un perfil a través de un "amigo falso"	308
e) Acceso no autorizado a una página de una red social	308
7.18. Ingeniería reversa y medidas de protección tecnológicas (DRM)	309
7.19. Acceso a bancos de datos online mediante bots (<i>web scraping</i>)	315
8. Acceso autorizado por parte de agentes estatales en ejercicio de sus funciones	317
9. Agravantes	319
10. Cuestiones procesales	320
10.1. Naturaleza de la acción	320
10.2. Competencia judicial	321
10.3. Persona legitimada para querellar. Investigación preliminar	322
10.4. Prueba del acceso no autorizado	324
Capítulo V. Publicación indebida de comunicaciones	325
1. Introducción	327
2. La figura en el Código Penal argentino	327
3. Acción punible	328
4. Objeto del delito	329
5. Concepto de ilegitimidad	331
6. Consentimiento para la publicación de correspondencia	332
7. Exención de responsabilidad penal en los casos de interés público	334
7.1. Regla introducida por la Ley de Delitos Informáticos (Ley N.º 26.388)	334
7.2. Criterios para determinar la existencia de interés público	335

7.3. El problema de las filtraciones de datos (<i>leaks</i>) en Internet	343
7.4. Republicación de secretos por la prensa	344
7.5. Republicación de filtraciones en blogs o sitios web	345
8. Delito de acción privada	348
9. Tutela civil	348

Capítulo VI. Revelación de secretos **351**

1. Bien jurídico protegido	353
1.1. Introducción	353
1.2. Hechos, actuaciones, documentos o datos que por ley deben ser secretos	353
1.3. Influencia de la publicidad y transparencia estatal en la obligación de guardar secreto	356
2. Sujeto activo	358
3. Acción típica	358
4. Culpabilidad	360
5. Concurso con otras figuras	360
6. Delito de acción pública	361

Capítulo VII. Protección penal de los datos personales **363**

1. Introducción a los delitos informáticos relacionados con bancos de datos personales. Derecho Comparado	365
2. La Ley N.º 25.326 y su reforma por la Ley N.º 26.388. Fundamentos	374
3. Debate sobre el bien jurídico protegido	378
4. Influencia de la Ley de Protección de Datos en la interpretación de esta figuras	383
5. Las acciones punibles	386
5.1. Acceso no autorizado a un banco de datos personales	386
5.2. Revelación de datos personales registrados en una base de datos	395
5.3. Inserción de datos en un banco de datos	408
5.4. Concurso con otras figuras	413

6. Cuestiones procesales	414
6.1. Naturaleza de la acción	414
6.2. Competencia judicial	416
6.3. Persona legitimada para querellar	417
Bibliografía	421