

*Editor*

Christian Scheechler Corona

*Coordinadora*

Rocío Riveros Saavedra

Los delitos informáticos  
Aspectos político-criminales,  
penales y procesales  
en la Ley N° 21.459

DER EDICIONES es una Editorial Jurídica creada por un grupo de Editores de larga trayectoria.

Estamos en la búsqueda de publicaciones de innegable valor científico. Nuestra propuesta pone énfasis en una cuidada elaboración técnica, colocando nuestra experiencia al servicio de la comunidad jurídica.

Nuestro catálogo editorial está compuesto por las siguientes colecciones: Ensayos Jurídicos, Monografías, Manuales, Cuadernos Jurídicos, Coediciones, Revistas y Obras prácticas.

Invitamos a aquellos profesores, investigadores o abogados en ejercicio, que hayan escrito una tesis de maestría, monografía, ensayo, manual u otra obra de interés práctico, a publicar con nosotros.

Para mayor información, escribanos a [info@derediciones.com](mailto:info@derediciones.com) o visite nuestra página web [www.derediciones.com](http://www.derediciones.com).

## LOS DELITOS INFORMÁTICOS

Aspectos político-criminales, penales y procesales en la Ley N° 21.459

© Christian Scheechler Corona (editor) y Rocío Riveros Saavedra (coordinadora)

2023 DER EDICIONES LIMITADA

Manuel Barros Borgoño 160, oficina 404, comuna de Providencia, ciudad de Santiago, Chile

[info@derediciones.com](mailto:info@derediciones.com)

[www.derediciones.com](http://www.derediciones.com)

Registro de Propiedad Intelectual N° EN TRÁMITE

ISBN 978-956-405-174-1

Primera edición, diciembre de 2023 DER Ediciones Limitada

Tiraje: 300 ejemplares

Impresores: Editora e Imprenta Maval SpA

Impreso en Chile / Printed in Chile

## ADVERTENCIA

La Ley N° 17.336 sobre Propiedad Intelectual prohíbe el uso no exceptuado de obras protegidas sin la autorización expresa de los titulares de los derechos de autor.

El fotocopiado o reproducción por cualquier otro medio o procedimiento de la presente publicación queda expresamente prohibido.

## ÍNDICE

ABREVIATURAS.....	VII
CAPÍTULO I: CIBERCRIMEN E INTELIGENCIA ARTIFICIAL .....	1
1. LA ATRIBUCIÓN DE RESPONSABILIDAD PENAL POR LOS HECHOS COMETIDOS POR SISTEMAS AUTÓNOMOS INTELIGENTES, ROBÓTICA Y TECNOLOGÍAS CONEXAS.....	3
Carlos María Romeo Casabona	
1.1. Introducción.....	4
1.2. ¿Necesitamos un nuevo sistema penal construido para la IA y los robots?	7
1.3. ¿Validez de los estándares legales para resolver problemas de responsabilidad de sistemas de IA por daños a personas o cosas? Responsabilidad penal por imprudencia .....	10
1.4. Lesiones de bienes jurídicos producidas intencionadamente .....	15
A) El robot o el sistema de IA como meros instrumentos de la acción humana.....	16
B) Sistemas autónomos inteligentes: ¿agentes criminales?.....	17
1.5. Aspectos específicos relativos a la responsabilidad penal de sistemas autónomos inteligentes.....	19
A) Argumentos a favor de atribuir responsabilidad penal a los robots, sistemas inteligentes y tecnologías conexas autónomas.....	20
B) Argumentos en contra.....	24
1.6. La atribución de responsabilidad penal a los robots autónomos y a los sistemas inteligentes: el control humano de los sistemas de IA como enfoque alternativo previo.....	27
1.7. Conclusiones: mirando al futuro .....	30
BIBLIOGRAFÍA .....	32
2. EL CIBERCRIMEN EN TIEMPOS DE LA NUEVA LEY DE DELITOS INFORMÁTICOS .....	35
Laura Mayer Lux	
2.1. Introducción.....	35

2.2. La suscripción del Convenio de Ciberdelincuencia como marco de referencia de una regulación de la criminalidad transnacional e internacional cometida en el ciberespacio.....	38
2.3. Algunos ámbitos de la nueva ley de delitos informáticos que se centran especialmente en la cibercriminalidad.....	40
2.4. Conclusiones.....	50
BIBLIOGRAFÍA .....	51
3. CIBERSEGURIDAD EN LA UNIÓN EUROPEA Y SU INFLUENCIA EN LA NUEVA LEY DE DELITOS INFORMÁTICOS .....	57
Bárbara Cortés Cabrera	
3.1. Introducción.....	57
3.2. La seguridad y ciberseguridad como rol del Estado.....	59
3.3. La Unión Europea y los desafíos en ciberseguridad .....	61
A) Directivas de la Unión Europea .....	61
B) Recomendaciones del Consejo Europeo.....	63
C) Naciones Unidas .....	64
D) Organización para la Seguridad y la Cooperación en Europa .....	65
E) Convenio sobre la Ciberdelincuencia del Consejo de Europa.....	66
F) Estrategia de Ciberseguridad de la Unión Europea: un ciberespacio abierto, protegido y seguro .....	69
3.4. Ciberseguridad y ciberdelitos en el marco normativo nacional .....	70
3.5. Conclusiones.....	74
BIBLIOGRAFÍA .....	75
CAPÍTULO II: LOS DELITOS DE LA NUEVA LEY DE DELITOS INFORMÁTICOS .....	79
4. EL DELITO DE ATAQUE A LA INTEGRIDAD DE LOS SISTEMAS INFORMÁTICOS DEL ARTÍCULO 1º DE LA LEY Nº 21.459 A LA LUZ DEL CONVENIO DE BUDAPEST.....	81
Rodrigo Paredes Domínguez	
4.1. Introducción.....	81
4.2. El compromiso de Chile con el Convenio de Budapest .....	82
4.3. El origen del delito de ataque a la integridad de un sistema informático...	84
4.4. Análisis del delito de ataque a la integridad de un sistema informático ....	85
A) Tipicidad objetiva .....	86
a. Sujeto activo.....	86
b. Conducta punible .....	86
c. Delito de resultado .....	89
B) Tipo subjetivo .....	90

4.5. El delito de ataque a la integridad de un sistema informático a la luz del Convenio de Budapest .....	91
4.6. Conclusiones generales .....	96
BIBLIOGRAFÍA .....	97
5. EL DELITO DE ACCESO ILÍCITO EN EL DERECHO PENAL CHILENO .....	101
Francisco Javier Bedecarratz Scholz	
5.1. Introducción.....	101
5.2. Antecedentes.....	102
5.3. Análisis dogmático del artículo 2° de la Ley N° 21.459.....	105
A) Sistemática .....	105
B) Bien jurídico protegido .....	106
C) Conducta y consumación .....	112
5.4. La investigación de vulnerabilidades y su punibilidad.....	115
A) Taxonomía del hacking .....	115
B) Investigación académica.....	117
C) Inscripción previa y notificación responsable.....	119
5.5. Conclusiones.....	120
BIBLIOGRAFÍA .....	121
6. LOS DELITOS DE INTERCEPTACIÓN ILÍCITA DEL ARTÍCULO 3° DE LA LEY N° 21.459: PROBLEMAS INTERPRETATIVOS .....	125
Valeska Fuentealba Sepúlveda	
6.1. Introducción.....	125
6.2. Análisis dogmático de la interceptación ilícita del inciso 1° del artículo 3°	130
6.3. Análisis dogmático de la captación no autorizada del inciso 2° del artículo 3°.....	136
6.4. Referencia al bien jurídico protegido .....	141
6.5. Conclusiones.....	144
BIBLIOGRAFÍA .....	147
7. LOS DATOS INFORMÁTICOS Y LA HIPÓTESIS DE SABOTAJE CONTENIDA EN EL ARTÍCULO 4° DE LA LEY N° 21.459.....	151
Verónica Rosenblut Gorodinsky	
7.1. Introducción.....	151
7.2. El dato informático como objeto de protección de los delitos informáticos	153
7.3. Historia legislativa del delito de ataque a la integridad de los datos informáticos.....	156
7.4. Estructura y características de tipo penal de ataque a la integridad de los datos informáticos .....	160

7.5. Carácter residual de la figura de ataque a la integridad de datos informáticos .....	165
BIBLIOGRAFÍA .....	167
8. ANÁLISIS POLÍTICO-CRIMINAL Y TÉCNICO-LEGISLATIVO DE LA FALSIFICACIÓN INFORMÁTICA DEL ARTÍCULO 5º DE LA LEY N° 21.459 .....	169
Jaime Vera Vega	
8.1. Introducción y planteamiento de la cuestión .....	169
8.2. Breve análisis del delito de falsificación informática .....	171
A) La falsificación informática como delito de falsedad .....	171
B) Elementos típicos del nuevo delito de falsificación informática .....	173
8.3. ¿Es la falsificación informática una figura distinta de las falsedades documentales tradicionales? .....	176
8.4. ¿Necesidad del establecimiento de un delito de falsificación informática? .....	183
8.5. Consecuencias técnico-legislativas del establecimiento de un delito de falsificación informática .....	187
A) Asistematicidad en cuanto a la regulación del comportamiento típico .....	189
B) Asistematicidad en el tratamiento del objeto material .....	190
C) Asistematicidad en el régimen punitivo de las falsedades recaídas en documentos privados .....	191
BIBLIOGRAFÍA .....	192
9. LA RECEPCIÓN DE DATOS INFORMÁTICOS (ART. 6º DE LA LEY N° 21.459) .....	195
Paulina Gutiérrez Peña	
9.1. Introducción .....	195
9.2. El mercado negro de datos informáticos .....	196
9.3. La recepción de datos informáticos .....	198
A) El concepto de recepción .....	199
B) Clasificación .....	200
C) Análisis típico del artículo 6º de la Ley de Delitos Informáticos .....	200
a. Faz objetiva .....	200
b. Faz subjetiva .....	202
D) Bien jurídico protegido .....	202
E) Penalidad .....	203
9.4. Conclusión .....	203
BIBLIOGRAFÍA .....	204
10. LA ESPERADA CONSAGRACIÓN DE UN GENUINO DELITO DE FRAUDE INFORMÁTICO EN EL DERECHO PENAL CHILENO (ART. 7º DE LA LEY N° 21.459) .....	207
Héctor Hernández Basualto	
10.1. Introducción .....	207

10.2. La inaplicabilidad de los tipos penales tradicionales .....	208
10.3. Cobertura indirecta a través de la Ley N° 19.223.....	212
10.4. Por una cobertura directa: modelos posibles de <i>lege ferenda</i> .....	213
10.5. La solución de la Ley N° 21.459 .....	218
A) Caracterización general.....	218
B) Formas de comisión.....	222
C) La curiosa regla de autoría del inciso tercero .....	227
D) La relación con el fraude del nuevo inciso segundo del artículo 468 del Código Penal (o “la vida breve” del artículo 7°).....	229
BIBLIOGRAFÍA .....	234
11. EL DELITO DE ABUSO DE DISPOSITIVOS EN LA NUEVA LEY DE DELITOS INFORMÁ- TICOS (N° 21.459).....	239
Mauricio Fernández Montalbán	
11.1. Introducción.....	239
11.2. El delito de abusos de dispositivos en el Convenio de Budapest.....	240
11.3. El delito de abuso de dispositivos en la Ley N° 21.459 sobre Delitos Informáticos.....	243
11.4. El delito de abusos de dispositivos en la legislación española .....	247
11.5. El delito de abuso de dispositivos en las propuestas de una Convención por la Organización de las Naciones Unidas.....	250
11.6. Conclusiones.....	251
BIBLIOGRAFÍA .....	253
CAPÍTULO III: ASPECTOS PROCESALES Y PENOLÓGICOS.....	257
12. DILIGENCIAS INTRUSIVAS EN LA NUEVA LEY DE DELITOS INFORMÁTICOS: ANÁLISIS CRÍTICO.....	259
Agustina Alvarado Urizar	
12.1. Introducción.....	259
12.2. Sobre la necesidad de promover la incorporación de técnicas especiales de investigación .....	261
A) Características especiales de los delitos informáticos .....	261
B) Especial referencia al “ciberespacio”: web superficial y web profunda	263
12.3. Diligencias intrusivas contenidas en la Ley N° 21.459 .....	268
A) Interceptación de comunicaciones. ....	268
B) Otros medios técnicos de investigación.....	278
C) Agente encubierto “online” .....	283
12.4. Conclusiones.....	291
BIBLIOGRAFÍA .....	292

13. LAS ESPECIALES CIRCUNSTANCIAS MODIFICATORIAS DE LA RESPONSABILIDAD PENAL EN LOS DELITOS INFORMÁTICOS.....	297
Christian Scheechler Corona	
13.1. Introducción.....	297
13.2. Circunstancia atenuante especial: la cooperación eficaz .....	298
13.3. Las circunstancias agravantes en la LDI .....	302
A) Agravante de especial posición frente al sistema o datos informáticos	303
B) La agravante de abuso de situación desventajosa de menores y adultos mayores .....	303
C) La circunstancia agravante de afectación de servicios de utilidad pública o de procesos electorales.....	305
D) La agravante eliminada: utilizar tecnologías de encriptación sobre datos informáticos contenidos en sistemas informáticos que tengan por principal finalidad la obstaculización de la acción de la justicia...	306
13.4. Conclusiones.....	307
BIBLIOGRAFÍA .....	308
14. RESPONSABILIDAD DE LAS PERSONAS JURÍDICAS EN LA NUEVA LEY N° 21.459 SOBRE DELITOS INFORMÁTICOS.....	309
Rocío Riveros Saavedra	
14.1. Introducción.....	309
14.2. Paso de la inimputabilidad a la responsabilidad de las personas jurídicas	310
14.3. Responsabilidad penal de las personas jurídicas en Chile. La regulación de la Ley N° 20.393 y su avance .....	312
14.4. Regulación en la Convención de Budapest de la responsabilidad de las personas jurídicas .....	317
14.5. Análisis sobre la nueva Ley N° 21.459 que establece normas sobre delitos informáticos, y su regulación sobre la responsabilidad penal de las personas jurídicas .....	319
14.6. Conclusión .....	322
BIBLIOGRAFÍA .....	323