



COLECCIÓN TIRANT 4.0

## **CRIPTOGRAFÍA Y PRIVACIDAD**



COLECCIÓN TIRANT 4.0

# CRIPTOGRAFÍA Y PRIVACIDAD

Dr. Daniel Álvarez Valenzuela<sup>1</sup>

**tirant lo blanch**

Valencia, 2024

---

<sup>1</sup> Doctor en derecho, magister en derecho público y licenciado en ciencias jurídicas y sociales, todo por la Universidad de Chile. Académico de la Facultad de Derecho de la Universidad de Chile.

Copyright © 2024

Todos los derechos reservados. Ni la totalidad ni parte de este libro puede reproducirse o transmitirse por ningún procedimiento electrónico o mecánico, incluyendo fotocopia, grabación magnética, o cualquier almacenamiento de información y sistema de recuperación sin permiso escrito del autor y del editor.

En caso de erratas y actualizaciones, la Editorial Tirant lo Blanch publicará la pertinente corrección en la página web [www.tirant.com](http://www.tirant.com).

© Daniel Álvarez Valenzuela

© **TIRANT LO BLANCH**

EDITA: TIRANT LO BLANCH  
C/ Artes Gráficas, 14 - 46010 - Valencia  
TELEF.: 96/361 00 48 - 50  
FAX: 96/369 41 51  
Email: [tlb@tirant.com](mailto:tlb@tirant.com)  
[www.tirant.com](http://www.tirant.com)  
Librería virtual: [www.tirant.es](http://www.tirant.es)  
ISBN: 978-84-1147-783-3  
MAQUETA: Innovatext

Si tiene alguna queja o sugerencia, envíenos un mail a:  
[atencioncliente@tirant.com](mailto:atencioncliente@tirant.com).

En caso de no ser atendida su sugerencia, por favor, lea nuestro procedimiento de quejas en:  
[www.tirant.net/index.php/empresa/politicas-de-empresa](http://www.tirant.net/index.php/empresa/politicas-de-empresa)

Responsabilidad Social Corporativa:  
<http://www.tirant.net/Docs/RSCTirant.pdf>

*“Cryptography rearranges power: it configures who can do what, from what. This makes cryptography an inherently political tool, and it confers on the field an intrinsically moral dimension.”*

Phillip Rogaway, 2015.





# ÍNDICE

<b>ABREVIATURAS</b> .....	13
<b>INTRODUCCIÓN</b> .....	15

## *Capítulo 1*

### **CRIPTOGRAFÍA Y CIFRADO**

1. INTRODUCCIÓN .....	19
2. CRIPTOLOGÍA Y CRIPTOGRAFÍA .....	20
3. CIFRADO O ENCRIPCIÓN .....	22
4. CLASIFICACIONES DE LOS SISTEMAS DE CIFRADO .....	24
4.1. Cifrado clásico .....	24
4.2. Cifrado moderno .....	26
5. FUNCIONES DEL CIFRADO .....	30
6. MODALIDADES DE IMPLEMENTACIÓN DEL CIFRADO .....	32
6.1. Cifrado punto-a-punto .....	32
6.2. Cifrado de dispositivo .....	34
6.3. Cifrado de la capa de transporte .....	34
6.4. Cifrado en el prestador de servicios .....	35
6.5. Cifrado en el punto final .....	36
7. FORTALEZAS DEL CIFRADO .....	37
7.1. Robustez matemática .....	38
7.2. Cifrado por defecto y punto-a-punto .....	42
8. DEBILIDADES DEL CIFRADO .....	43
8.1. Encontrar la llave .....	44
8.2. Adivinar la llave .....	46
8.3. Compeler la entrega de la llave .....	47
8.4. Explotar una vulnerabilidad del sistema .....	49
8.5. Acceso en el dispositivo .....	53
8.6. Localizar copias sin encriptar .....	54
9. CONCLUSIONES DEL CAPÍTULO .....	55

## *Capítulo 2*

### **CRIPTOGRAFÍA Y DERECHO**

1. INTRODUCCIÓN .....	59
2. LA RELACIÓN ENTRE DERECHO Y CRIPTOGRAFÍA .....	59
3. ENFOQUES REGULATORIOS .....	63
4. TAXONOMÍA REGULATORIA .....	70

5. PANORAMA REGULATORIO INTERNACIONAL .....	72
5.1. Derecho general a la encriptación .....	73
5.2. Prohibición de uso de encriptación.....	76
5.3. Restricciones al uso de encriptación .....	82
6. ANÁLISIS DE LOS RESULTADOS .....	101
7. CONCLUSIONES DEL CAPÍTULO.....	104

### Capítulo 3

#### EL CIFRADO EN EL DEBATE PÚBLICO Y REGULATORIO ESTADOUNIDENSE

1. INTRODUCCIÓN .....	107
2. CINCO DÉCADAS DE CRIPTODEBATES.....	108
2.1. El criptosecretismo (1950-1980).....	108
2.2. Las criptoguerras (1980-2000).....	113
2.3. Criptografía por defecto (2013 al presente) .....	119
3. CONCLUSIONES DEL CAPÍTULO.....	123

### Capítulo 4

#### EL CIFRADO EN EL DERECHO CONSTITUCIONAL ESTADOUNIDENSE

1. INTRODUCCIÓN .....	125
2. EL CIFRADO COMO DISCURSO PROTEGIDO .....	126
2.1. Primera época: el discurso silenciado .....	129
2.2. Segunda época: el discurso obligado .....	139
3. EL CIFRADO COMO OBJETO DE PROTECCIÓN DEL DERECHO CONSTITU- CIONAL A LA PRIVACIDAD .....	145
3.1. Los orígenes: el juez Thomas Cooley y <i>Right to privacy</i> de Warren y Bran- deis .....	145
3.2. Primera época: el disenso .....	148
3.3. Segunda época: los votos de mayoría .....	151
3.4. La protección del cifrado bajo la Cuarta Enmienda .....	155
4. CONCLUSIONES DEL CAPÍTULO.....	160

### Capítulo 5

#### CRIPTOGRAFÍA Y DERECHOS FUNDAMENTALES

1. INTRODUCCIÓN .....	163
2. PANORAMA INTERNACIONAL .....	163
2.1. OCDE .....	164
2.2. Sistema de Naciones Unidas.....	165
3. LIBERTAD DE EXPRESIÓN Y ENCRIPCIÓN .....	169
3.1. Contenido normativo del derecho a la libertad de expresión en el derecho internacional de los derechos humanos .....	170

3.2. Cifrado como habilitante o facilitador del ejercicio del derecho a la libertad de expresión.....	174
3.3. La regulación del cifrado como límite al ejercicio del derecho a la libertad de expresión.....	176
4. CRIPTOGRAFÍA Y DERECHO A LA PRIVACIDAD.....	178
4.1. Contenido normativo del derecho a la privacidad en el derecho internacional de los derechos humanos.....	179
4.2. El cifrado como habilitante o facilitador del ejercicio del derecho a la privacidad.....	182
4.3. La regulación del cifrado como límite al ejercicio del derecho a la privacidad..	183
5. CONCLUSIONES DEL CAPÍTULO.....	185

### Capítulo 6

#### EL SISTEMA CONSTITUCIONAL DE PROTECCIÓN DE LA PRIVACIDAD EN EL DERECHO CHILENO

1. INTRODUCCIÓN.....	187
2. EL DEBATE PREVIO: ¿INTIMIDAD, PRIVACIDAD O VIDA PRIVADA?.....	188
3. DERECHO A LA PRIVACIDAD.....	191
3.1. El derecho a la vida privada.....	193
3.2. El derecho a la autodeterminación informativa.....	197
3.3. El derecho a la inviolabilidad de las comunicaciones privadas.....	204
3.4. El derecho a la inviolabilidad de los documentos privados.....	208
3.5. El derecho a la inviolabilidad del hogar.....	211
4. CONCLUSIONES.....	215

### Capítulo 7

#### CRIPTOGRAFÍA Y PRIVACIDAD EN EL DERECHO CONSTITUCIONAL CHILENO

1. INTRODUCCIÓN.....	217
2. CIFRADO COMO REFUERZO EXTRANORMATIVO.....	218
3. AUTOGESTIÓN DE LA PRIVACIDAD Y CIFRADO.....	224
4. EL CIFRADO FRENTE AL SISTEMA CONSTITUCIONAL DE PROTECCIÓN DE LA PRIVACIDAD.....	227
4.1. Cifrado y derecho a la vida privada.....	228
4.2. Cifrado y derecho a la autodeterminación informativa.....	229
4.3. Cifrado y derecho a la inviolabilidad de las comunicaciones privadas.....	231
4.4. Cifrado y el derecho a la inviolabilidad de los documentos privados.....	234
4.5. Cifrado y el derecho a la inviolabilidad del hogar.....	235

<b>CONCLUSIONES.....</b>	<b>237</b>
--------------------------	------------

<b>REFERENCIAS BIBLIOGRÁFICAS.....</b>	<b>241</b>
--	------------