

ÍNDICE

| | |
|--|-----------|
| AGRADECIMIENTOS | 5 |
| ÍNDICE..... | 6 |
| ABREVIATURAS | 10 |
| INTRODUCCIÓN | 11 |
| CAPÍTULO 1 CRIPTOGRAFÍA Y CIFRADO | 17 |
| 1. INTRODUCCIÓN | 17 |
| 2. CRIPTOLOGÍA Y CRIPTOGRAFÍA | 18 |
| 3. CIFRADO O ENCRIPCIÓN | 20 |
| 4. CLASIFICACIONES DE LOS SISTEMAS DE CIFRADO..... | 22 |
| 4.1. Cifrado clásico..... | 22 |
| 4.2. Cifrado moderno | 24 |
| 4.2.1. Cifrado simétrico..... | 25 |
| 4.2.2. Cifrado asimétrico | 26 |
| 5. FUNCIONES DEL CIFRADO | 28 |
| 6. MODALIDADES DE IMPLEMENTACIÓN DEL CIFRADO | 30 |
| 6.1. Cifrado punto-a-punto..... | 30 |
| 6.2. Cifrado de dispositivo | 32 |
| 6.3. Cifrado de la capa de transporte..... | 32 |
| 6.4. Cifrado en el prestador de servicios..... | 33 |
| 6.5. Cifrado en el punto final..... | 34 |
| 7. FORTALEZAS DEL CIFRADO..... | 35 |
| 7.1. Robustez matemática | 36 |
| 7.2. Cifrado por defecto y punto-a-punto | 40 |
| 8. DEBILIDADES DEL CIFRADO | 41 |
| 8.1. Encontrar la llave..... | 42 |
| 8.2. Adivinar la llave..... | 43 |
| 8.3. Compeler la entrega de la llave | 44 |
| 8.4. Explotar una vulnerabilidad del sistema..... | 46 |

| | | |
|--|---|------------|
| 8.5. | Acceso en el dispositivo..... | 50 |
| 8.6. | Localizar copias sin encriptar..... | 52 |
| 9. | CONCLUSIONES DEL CAPÍTULO | 53 |
| CAPÍTULO 2 CRIPTOGRAFÍA Y DERECHO..... | | 55 |
| 1. | INTRODUCCIÓN | 55 |
| 2. | LA RELACIÓN ENTRE DERECHO Y CRIPTOGRAFÍA | 55 |
| 3. | ENFOQUES REGULATORIOS | 59 |
| 4. | TAXONOMÍA REGULATORIA | 66 |
| 5. | PANORAMA REGULATORIO INTERNACIONAL..... | 68 |
| 5.1. | Derecho general a la encriptación..... | 69 |
| 5.2. | Prohibición de uso de encriptación..... | 72 |
| 5.3. | Restricciones al uso de encriptación..... | 78 |
| 6. | ANÁLISIS DE LOS RESULTADOS | 99 |
| 7. | CONCLUSIONES DEL CAPÍTULO..... | 101 |
| CAPÍTULO 3 EL CIFRADO EN EL DEBATE PÚBLICO Y REGULATORIO ESTADOUNIDENSE | | 103 |
| 1. | INTRODUCCIÓN | 103 |
| 2. | CINCO DÉCADAS DE CRIPTODEBATES..... | 104 |
| 2.1. | El criptosecretismo (1950-1980)..... | 104 |
| 2.2. | Las criptoguerras (1980-2000) | 109 |
| 2.3. | Criptografía por defecto (2013 al presente) | 115 |
| 3. | CONCLUSIONES DEL CAPÍTULO | 119 |
| CAPÍTULO 4 EL CIFRADO EN EL DERECHO CONSTITUCIONAL ESTADOUNIDENSE | | 121 |
| 1. | INTRODUCCIÓN | 121 |
| 2. | EL CIFRADO COMO DISCURSO PROTEGIDO..... | 122 |
| 2.1. | Primera época: el discurso silenciado..... | 125 |
| 2.2. | Segunda época: el discurso obligado..... | 136 |
| 3. | EL CIFRADO COMO OBJETO DE PROTECCIÓN DEL DERECHO CONSTITUCIONAL A LA PRIVACIDAD | 141 |

| | | |
|---|--|------------|
| 3.1. | Los orígenes: el juez Thomas Cooley y <i>Right to privacy de Warren y Brandeis</i> | 142 |
| 3.2. | Primera época: el disenso | 145 |
| 3.3. | Segunda época: los votos de mayoría | 148 |
| 3.4. | La protección del cifrado bajo la Cuarta Enmienda | 152 |
| 4. | CONCLUSIONES DEL CAPÍTULO | 157 |
| CAPÍTULO 5 CRIPTOGRAFÍA Y DERECHOS FUNDAMENTALES..... | | 159 |
| 1. | INTRODUCCIÓN | 159 |
| 2. | PANORAMA INTERNACIONAL | 160 |
| 2.1. | OCDE | 160 |
| 2.2. | Sistema de Naciones Unidas | 162 |
| 3. | LIBERTAD DE EXPRESIÓN Y ENCRIPCIÓN | 166 |
| 3.1. | Contenido normativo del derecho a la libertad de expresión en el derecho internacional de los derechos humanos | 167 |
| 3.2. | Cifrado como habilitante o facilitador del ejercicio del derecho a la libertad de expresión..... | 171 |
| 3.3. | La regulación del cifrado como límite al ejercicio del derecho a la libertad de expresión 173 | |
| 4. | CRIPTOGRAFÍA Y DERECHO A LA PRIVACIDAD | 175 |
| 4.1. | Contenido normativo del derecho a la privacidad en el derecho internacional de los derechos humanos..... | 176 |
| 4.2. | El cifrado como habilitante o facilitador del ejercicio del derecho a la privacidad.. | 179 |
| 4.3. | La regulación del cifrado como límite al ejercicio del derecho a la privacidad..... | 180 |
| 5. | CONCLUSIONES DEL CAPÍTULO | 182 |
| CAPÍTULO 6 EL SISTEMA CONSTITUCIONAL DE PROTECCIÓN DE LA PRIVACIDAD EN EL DERECHO CHILENO..... | | 184 |
| 1. | INTRODUCCIÓN | 184 |
| 2. | EL DEBATE PREVIO: ¿INTIMIDAD, PRIVACIDAD O VIDA PRIVADA?..... | 185 |
| 3. | DERECHO A LA PRIVACIDAD..... | 188 |
| 3.1. | El derecho a la vida privada | 190 |
| 3.2. | El derecho a la autodeterminación informativa | 194 |

| | | |
|--|---|------------|
| 3.3. | El derecho a la inviolabilidad de las comunicaciones privadas..... | 202 |
| 3.4. | El derecho a la inviolabilidad de los documentos privados..... | 206 |
| 3.5. | El derecho a la inviolabilidad del hogar..... | 209 |
| 4. | CONCLUSIONES..... | 213 |
| CAPÍTULO 7 CRIPTOGRAFÍA Y PRIVACIDAD EN EL DERECHO CONSTITUCIONAL CHILENO | | 215 |
| 1. | INTRODUCCIÓN..... | 215 |
| 2. | CIFRADO COMO REFUERZO EXTRANORMATIVO..... | 216 |
| 3. | AUTOGESTIÓN DE LA PRIVACIDAD Y CIFRADO | 222 |
| 4. | EL CIFRADO FRENTE AL SISTEMA CONSTITUCIONAL DE PROTECCIÓN DE LA PRIVACIDAD..... | 226 |
| 4.1. | Cifrado y derecho a la vida privada..... | 226 |
| 4.2. | Cifrado y derecho a la autodeterminación informativa..... | 228 |
| 4.3. | Cifrado y derecho a la inviolabilidad de las comunicaciones privadas..... | 229 |
| 4.4. | Cifrado y el derecho a la inviolabilidad de los documentos privados | 232 |
| 4.5. | Cifrado y el derecho a la inviolabilidad del hogar..... | 233 |
| CONCLUSIONES..... | | 235 |
| REFERENCIAS BIBLIOGRÁFICAS..... | | 239 |