

Índice General

Página

| | |
|--|----|
| INTRODUCCIÓN | 17 |
| CAPÍTULO I | |
| LA ARMONIZACIÓN SUPRANACIONAL DEL ACCESO ILÍCITO | 31 |
| I. Introducción | 31 |
| II. OCDE: El Informe <i>Computer-Related Crime</i> | 32 |
| A) <i>Uso no autorizado de un ordenador</i> | 34 |
| B) <i>Acceso no autorizado</i> | 35 |
| III. Consejo de Europa: recomendación 89 (9), de 13 de septiembre, sobre delincuencia informática | 36 |
| A) <i>Acceso ilícito a un sistema informático</i> | 37 |
| B) <i>Uso no autorizado de un ordenador</i> | 39 |
| IV. Naciones Unidas: Manual <i>Computer-Related Crime</i> | 40 |
| A) <i>Congreso Internacional de Derecho Penal</i> | 41 |
| 1. <i>Uso no autorizado de un ordenador</i> | 41 |
| 2. <i>Acceso no autorizado</i> | 42 |
| 3. <i>Recomendaciones de la Asociación</i> | 43 |
| B) <i>Manual Computer-Related Crime</i> | 43 |
| C) <i>Etapa posterior a la elaboración del manual</i> | 45 |
| V. Plan de acción del G8 | 45 |
| A) <i>Subgroup on High-tech Crime</i> | 46 |
| B) <i>Derecho sustantivo: Ten principles and action plan in the combat against computer crime</i> | 46 |
| C) <i>Derecho procesal: Birmingham submit y six principles on transborder access to stored computer data</i> | 46 |

| | | |
|--------------|--|----|
| | D) <i>De la delincuencia informática al cibercrimen: Okinawa Submit</i> | 47 |
| VI. | Consejo de Europa: convenio sobre cibercrimen | 48 |
| | A) <i>Estructura y contenido</i> | 50 |
| | B) <i>El delito de acceso ilícito</i> | 52 |
| VII. | Normativa aprobada por la Unión Europea | 59 |
| | A) <i>Preliminares: las comunicaciones</i> | 59 |
| | B) <i>Decisión Marco 2005/222/JAI, del Consejo, de 24 de febrero, relativa a los ataques a sistemas de información</i> | 60 |
| | 1. <i>Estructura</i> | 60 |
| | 2. <i>Acceso ilícito</i> | 61 |
| | C) <i>Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión Marco 2005/222/JAI</i> | 63 |
| | 1. <i>Estructura</i> | 64 |
| | 2. <i>Acceso ilícito</i> | 64 |
| | D) <i>Otras actuaciones de la Unión Europea</i> | 65 |
| VIII. | Aplicación del convenio y la directiva | 66 |
| | A) <i>Tabla de aplicación del delito de acceso ilícito</i> | 66 |
| | B) <i>Definición de sistema y datos informáticos</i> | 69 |

CAPÍTULO II

| | | |
|------------|---|----|
| | EL TRATAMIENTO PENAL DEL ACCESO ILÍCITO EN EL DERECHO COMPARADO A LA LUZ DE LOS INSTRUMENTOS SUPRANACIONALES | 79 |
| I. | Introducción | 79 |
| II. | Alemania | 80 |
| | A) <i>Marco normativo</i> | 80 |
| | B) <i>Literalidad del precepto</i> | 81 |
| | C) <i>Bien jurídico protegido</i> | 81 |
| | D) <i>Objeto material del delito</i> | 83 |
| | E) <i>Modalidades típicas</i> | 87 |

| | | |
|-------------|---|-----|
| 1. | Apoderamiento de los datos contenidos en el sistema informático: <i>Verschaffen von Daten</i> | 87 |
| 2. | Acceso a los datos: <i>Verschaffen des Zugangs Zu Daten</i> | 88 |
| F) | <i>Elementos del tipo objetivo</i> | 89 |
| 1. | Sin autorización | 89 |
| 2. | La especial protección de los datos | 90 |
| G) | <i>Tipo subjetivo</i> | 92 |
| H) | <i>Tratamiento del error</i> | 93 |
| I) | <i>Autoría y participación</i> | 93 |
| J) | <i>Pena</i> | 94 |
| III. | Italia | 94 |
| A) | <i>Marco normativo</i> | 94 |
| B) | <i>Literalidad de la norma</i> | 94 |
| C) | <i>Bien jurídico protegido</i> | 95 |
| 1. | Domicilio informático | 95 |
| a) | El domicilio informático como bien jurídico | 95 |
| b) | Crítica a esta opinión | 98 |
| 2. | <i>Riservatezza individuale</i> (intimidad) | 99 |
| 3. | Otros bienes jurídicos | 100 |
| D) | <i>Tipo objetivo</i> | 101 |
| 1. | Conducta | 101 |
| a) | Acceso abusivo | 101 |
| i) | Consumación y tentativa | 101 |
| ii) | Tipos de acceso | 103 |
| iii) | Vulneración de medidas de seguridad | 103 |
| b) | Mantenimiento abusivo | 106 |
| i) | Consumación y tentativa | 107 |
| ii) | Consentimiento | 107 |
| c) | Objeto material: sistema informático/telemático | 108 |
| d) | La expresión abusivamente | 109 |

| | |
|--|-----|
| E) <i>Tipo subjetivo</i> | 109 |
| F) <i>Pena</i> | 110 |
| IV. Estados Unidos de América | 110 |
| A) <i>Legislación federal</i> | 111 |
| 1. Marco legal | 111 |
| 2. Literalidad de la norma | 112 |
| 3. Elementos del tipo objetivo | 113 |
| a) Modalidades típicas | 113 |
| i) Acceso | 114 |
| ii) Exceso de autorización | 115 |
| b) Objeto material: ordenador protegido | 116 |
| B) <i>Legislación de los Estados Federales</i> | 118 |
| 1. Estado de Georgia | 118 |
| 2. Estado de California | 118 |
| 3. Estado de Washington | 119 |
| 4. Estado de Nueva York | 119 |
| 5. Estado de Texas | 120 |
| 6. Estado de Wisconsin | 120 |

CAPÍTULO III

| | |
|---|-----|
| BIEN JURÍDICO PROTEGIDO | 121 |
| I. La intimidad como bien jurídico | 121 |
| II. Domicilio informático | 125 |
| A) <i>Concepto, naturaleza y contenido esencial del domicilio informático como bien jurídico</i> | 125 |
| 1. Excesiva vinculación con la intimidad | 128 |
| 2. Noción físico-espacial de domicilio | 129 |
| 3. Ubicación sistemática | 132 |
| III. Integridad, disponibilidad y confidencialidad de los datos, redes y sistemas informáticos | 132 |
| IV. Seguridad informática | 138 |

| | | |
|------------|--|-----|
| A) | <i>Seguridad como expresión de la integridad, disponibilidad y confidencialidad</i> | 139 |
| B) | <i>Seguridad de la información</i> | 140 |
| C) | <i>Concepción formal</i> | 141 |
| V. | Otros bienes jurídicos | 143 |
| VI. | Toma de postura: la seguridad informática como bien jurídico protegido | 146 |
| A) | <i>Justificación de la intervención penal</i> | 147 |
| B) | <i>Engarce constitucional</i> | 148 |
| C) | <i>Naturaleza jurídica</i> | 150 |
| | 1. El bien jurídico supraindividual inmediatamente protegido: la seguridad informática | 150 |
| | 2. Bienes jurídicos mediatamente protegidos | 152 |
| D) | <i>Núcleo esencial del Derecho: vertiente positiva y negativa del mismo</i> | 153 |
| E) | <i>Afectación de la seguridad informática</i> | 154 |
| | 1. Acceso ilícito como delito obstáculo | 155 |
| | 2. Acceso ilícito como delito de peligro | 155 |
| | i) Modalidad de acceso | 156 |
| | ii) Modalidad de mantenimiento | 156 |
| | 3. Acceso ilícito como delito de lesión-peligro | 157 |
| F) | <i>Propuesta de reubicación del delito conforme al bien jurídico protegido seguridad informática</i> | 158 |

CAPÍTULO IV

| | | |
|---|------------------------------------|-----|
| CONDUCTA TÍPICA | 161 | |
| I. Introducción | 161 | |
| II. La acción de acceder o facilitar el acceso | 161 | |
| A) <i>Tipos de acceso</i> | 164 | |
| | 1. Acceso físico vs. acceso remoto | 164 |
| | 2. Acceso total vs. acceso parcial | 166 |
| B) <i>Consumación y tentativa</i> | 167 | |

| | <i>Página</i> |
|---|---------------|
| 1. Consumación | 167 |
| 2. Tentativa | 172 |
| C) <i>Autoría y participación: especial referencia a la acción de facilitación del acceso y su relación con el artículo 197 ter</i> | 173 |
| 1. Autoría y participación en el acceso | 173 |
| 2. El concepto extensivo de autor | 175 |
| 3. Los actos preparatorios del acceso y la facilitación de claves de acceso al sistema: el artículo 197 ter | 177 |
| III. La acción de mantenimiento | 179 |
| A) <i>Origen</i> | 180 |
| 1. “Exceso de autorización” en la sección 1030 del Código Penal Federal de Estados Unidos | 181 |
| 2. Mantenimiento ilícito en el artículo 615 <i>ter</i> del Código Penal Italiano | 183 |
| B) <i>Contenido típico</i> | 184 |
| C) <i>Consumación</i> | 186 |
| D) <i>Valoración personal</i> | 187 |
| 1. Crítica a la tipificación de la conducta: ausencia de lesividad de la acción | 187 |
| 2. Críticas a la redacción vigente | 188 |
| a) Ubicación sistemática | 188 |
| b) Indebida restricción de la conducta | 189 |

CAPÍTULO V

| | |
|--|-----|
| EL OBJETO MATERIAL DEL DELITO | 191 |
| I. Introducción | 191 |
| II. Concepto en la normativa supranacional | 192 |
| A) <i>Sistema de información vs. sistema informático</i> | 192 |
| 1. Concepto de sistema de información | 193 |
| a) Concepto legal de sistema de información | 193 |
| i) Concepto y tipología de software informático | 194 |
| ii) Aplicación a la definición de software | 195 |

| | <u>Página</u> |
|--|---------------|
| b) Concepto técnico de sistema de información | 195 |
| 2. Relación de los conceptos de sistema de información y sistema informático | 198 |
| 3. Conclusión | 199 |
| B) <i>Concepto de sistema informático</i> | 200 |
| 1. Aspecto estructural: componentes del sistema | 201 |
| 2. Aspecto funcional: funciones del sistema | 202 |
| 3. Concreción del concepto de sistema informático | 202 |
| III. Sistema informático: objeto material del delito | 203 |
| A) <i>La protección jurídico-penal del software</i> | 205 |
| 1. Programas de ordenador | 206 |
| a) Concepto civil de programa de ordenador | 207 |
| i) Programa de ordenador como creación original | 208 |
| ii) Expresión material del programa de ordenador | 209 |
| b) Concepto penal de programa de ordenador | 211 |
| 2. Bases de datos electrónicas | 212 |
| 3. Páginas Web | 212 |
| B) <i>El elemento físico del sistema: hardware</i> | 213 |
| 1. Dispositivos de transmisión de datos | 214 |
| 2. Memoria | 214 |
| 3. Procesador | 215 |
| IV. Contenido del sistema: resultado del programa. Crítica | 215 |
| A) <i>Obra resultante del programa</i> | 215 |
| B) <i>Acceso al sistema como acceso a datos</i> | 217 |
| C) <i>Valoración personal</i> | 221 |

CAPÍTULO VI

| | |
|--|------------|
| DELIMITACIÓN DE LOS MEDIOS COMISIVOS DEL DELITO: LA VULNERACIÓN DE LAS MEDIDAS DE SEGURIDAD ESTABLECIDAS PARA IMPEDIR EL ACCESO | 223 |
|--|------------|

| | |
|------------------------------|------------|
| I. Introducción | 223 |
|------------------------------|------------|

| | <i>Página</i> |
|--|---------------|
| II. El inciso <i>por cualquier medio o procedimiento</i> | 224 |
| III. Vulneración de medidas de seguridad | 225 |
| A) <i>Restricción del ámbito aplicativo</i> | 226 |
| 1. Consecuencias | 226 |
| 2. La inclusión del inciso vulneración medidas de seguridad | 229 |
| 3. Aplicación a ambas modalidades | 232 |
| 4. Valoración personal | 234 |
| B) <i>Concepto, naturaleza y tipología de medidas de seguridad</i> | 236 |
| 1. Concepto | 236 |
| 2. Tipología | 239 |
| a) Medidas de seguridad física | 240 |
| i) Instrumentos Hardware: medios dispuestos directamente sobre el objeto | 240 |
| ii) Instrumentos de tipo organizativo (establecidos para custodiar el sistema) | 241 |
| b) Medidas de seguridad lógica | 241 |
| 3. Naturaleza | 243 |
| a) Discusión sobre las medidas de tipo lógico | 244 |
| b) Discusión sobre las medidas de tipo físico | 245 |
| 4. Cuestiones concursales | 248 |
| a) Delito de allanamiento de morada | 248 |
| b) Delito de daños | 251 |
| C) <i>Vulneración de las medidas de seguridad</i> | 251 |
| 1. Presencia de las medidas | 252 |
| a) Sistemas sin medidas de protección | 252 |
| b) Estado de la medida en el momento de la comisión del delito | 253 |
| 2. Criterio de la idoneidad | 254 |
| a) Idoneidad cualitativa: complejidad técnica o eficacia de las medidas | 254 |
| b) Idoneidad cuantitativa | 257 |
| 3. Superación de las medidas | 258 |

CAPÍTULO VII

EL ELEMENTO NEGATIVO DEL TIPO: LA AUTORIZACIÓN Y VOLUNTAD DEL TITULAR DEL SISTEMA 261

I. Introducción 261

II. La expresión *sin estar debidamente autorizado* 262

 A) *Naturaleza jurídica: ¿autorización como elemento de la tipicidad o de la antijuricidad?* 263

 B) *El concepto de autorización: presupuestos* 265

 1. *Presupuestos objetivos de la autorización* 267

 a) *Autorización como habilitación legal* 267

 b) *Autorización como mera aquiescencia* 267

 c) *Autorización oficial* 268

 2. *Presupuestos subjetivos: los sujetos con potestad para autorizar, especial referencia a la diversa titularidad de derechos* 268

 C) *El adverbio “debidamente”* 274

 1. *Significación jurídica* 274

 2. *¿Accesoriedad del Derecho Penal?* 274

 D) *La expresión without right en la normativa supranacional y la interpretación del artículo 197 bis 1 conforme a la misma* 275

III. La expresión *en contra de la voluntad de quien tenga un legítimo derecho a excluirlo* 277

 A) *Literalidad* 277

 B) *Contenido* 278

BIBLIOGRAFÍA 281

Libro electrónico. Guía de uso