ÍNDICE

CAPÍTULO I. LA ARMONIZACIÓN SUPRANACIONAL DEL ACCESO ILÍCITO

I. Introducción

II. OCDE: El Informe Computer-Related Crime

A) Uso no autorizado de un ordenador

B) Acceso no autorizado

III. Consejo de Europa: recomendación 89 (9), de 13 de septiembre, sobre delincuencia informática

A) Acceso ilícito a un sistema informático

B) Uso no autorizado de un ordenador

IV. Naciones Unidas: Manual Computer-Related Crime

A) Congreso Internacional de Derecho Penal

1. Uso no autorizado de un ordenador

2. Acceso no autorizado

3. Recomendaciones de la Asociación

B) Manual Computer-Related Crime

C) Etapa posterior a la elaboración del manual

V. Plan de acción del G8

A) Subgroup on High-tech Crime

B) Derecho sustantivo: Ten principles and action plan in the combat against computer crime

C) Derecho procesal: Birmingham submit y six principles on transborder access to stored computer data

D) De la delincuencia informática al cibercrimen: Okinawa Submit

VI. Consejo de Europa: convenio sobre cibercrimen

A) Estructura y contenido

B) El delito de acceso ilícito

VII. Normativa aprobada por la Unión Europea

A) Preliminares: las comunicaciones

B) Decisión Marco 2005/222/JAI, del Consejo, de 24 de febrero, relativa a los ataques a sistemas de información

1. Estructura

2. Acceso ilícito

C) 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

1. Estructura

2. Acceso ilícito

D) Otras actuaciones de la Unión Europea

VIII. Aplicación del convenio y la directiva

A) Tabla de aplicación del delito de acceso ilícito

B) Definición de sistema y datos informáticos

CAPÍTULO II. EL TRATAMIENTO PENAL DEL ACCESO ILÍCITO EN EL DERECHO COMPARADO A LA LUZ DE LOS INSTRUMENTOS SUPRANACIONALES

I. Introducción

II. Alemania

A) Marco normativo

B) Literalidad del precepto

C) Bien jurídico protegido

D) Objeto material del delito

E) Modalidades típicas

1. Apoderamiento de los datos contenidos en el sistema informático: Verschaffen von Daten
2. Acceso a los datos: Verschaffen des Zugangs Zu Daten

F) Elementos del tipo objetivo

1. Sin autorización
2. La especial protección de los datos

G) Tipo subjetivo

H) Tratamiento del error

I) Autoría y participación

J) Pena

III. Italia

A) Marco normativo

B) Literalidad de la norma

C) Bien jurídico protegido

1. Domicilio informático
   a) El domicilio informático como bien jurídico
   b) Crítica a esta opinión
2. Riservatezza individuale (intimidad)
3. Otros bienes jurídicos

D) Tipo objetivo

1. Conducta
   a) Acceso abusivo
      i) Consumación y tentativa
      ii) Tipos de acceso
      iii) Vulneración de medidas de seguridad
   b) Mantenimiento abusivo

i) Consumación y tentativa
ii) Consentimiento
c) Objeto material: sistema informático/telemático
d) La expresión abusivamente
E) Tipo subjetivo
F) Pena
IV. Estados Unidos de América
A) Legislación federal
1. Marco legal
2. Literalidad de la norma
3. Elementos del tipo objetivo
a) Modalidades típicas
i) Acceso
ii) Exceso de autorización
b) Objeto material: ordenador protegido
B) Legislación de los Estados Federales
1. Estado de Georgia
2. Estado de California
3. Estado de Washington
4. Estado de Nueva York
5. Estado de Texas
6. Estado de Wisconsin

CAPÍTULO III. BIEN JURÍDICO PROTEGIDO

I. La intimidad como bien jurídico
II. Domicilio informático
A) Concepto, naturaleza y contenido esencial del domicilio informático como bien jurídico
1. Excesiva vinculación con la intimidad
2. Noción físico-espacial de domicilio
3. Ubicación sistemática
III. Integridad, disponibilidad y confidencialidad de los datos, redes y sistemas informáticos
IV. Seguridad informática
A) Seguridad como expresión de la integridad, disponibilidad y confidencialidad
B) Seguridad de la información
C) Concepción formal
V. Otros bienes jurídicos
VI. Toma de postura: la seguridad informática como bien jurídico protegido
A) Justificación de la intervención penal

B) Engarce constitucional

C) Naturaleza jurídica

1. El bien jurídico supraindividual inmediatamente protegido: la seguridad informática

2. Bienes jurídicos mediatamente protegidos

D) Núcleo esencial del Derecho: vertiente positiva y negativa del mismo

E) Afectación de la seguridad informática

1. Acceso ilícito como delito obstáculo

2. Acceso ilícito como delito de peligro

i) Modalidad de acceso

ii) Modalidad de mantenimiento

3. Acceso ilícito como delito de lesión-peligro

F) Propuesta de reubicación del delito conforme al bien jurídico protegido seguridad informática

CAPÍTULO IV. CONDUCTA TÍPICA

I. Introducción

II. La acción de acceder o facilitar el acceso

A) Tipos de acceso

1. Acceso físico vs. acceso remoto

2. Acceso total vs. acceso parcial

B) Consumación y tentativa

1. Consumación

2. Tentativa

C) Autoría y participación: especial referencia a la acción de facilitación del acceso y su relación con el artículo 197 ter

1. Autoría y participación en el acceso

2. El concepto extensivo de autor

3. Los actos preparatorios del acceso y la facilitación de claves de acceso al sistema: el artículo 197 ter

III. La acción de mantenimiento

A) Origen

1. “Exceso de autorización” en la sección 1030 del Código Penal Federal de Estados Unidos

2. Mantenimiento ilícito en el artículo 615 ter del Código Penal Italiano

B) Contenido típico

C) Consumación

D) Valoración personal

1. Crítica a la tipificación de la conducta: ausencia de lesividad de la acción

2. Críticas a la redacción vigente

a) Ubicación sistemática

b) Indebida restricción de la conducta

CAPÍTULO V. EL OBJETO MATERIAL DEL DELITO

I. Introducción

II. Concepto en la normativa supranacional

A) Sistema de información vs. sistema informático

1. Concepto de sistema de información

a) Concepto legal de sistema de información

i) Concepto y tipología de software informático

ii) Aplicación a la definición de software

b) Concepto técnico de sistema de información

2. Relación de los conceptos de sistema de información y sistema informático.

3. Conclusión

B) Concepto de sistema informático

1. Aspecto estructural: componentes del sistema

2. Aspecto funcional: funciones del sistema

3. Concreción del concepto de sistema informático

III. Sistema informático: objeto material del delito

A) La protección jurídico-penal del software

1. Programas de ordenador

a) Concepto civil de programa de ordenador

i) Programa de ordenador como creación original

ii) Expresión material del programa de ordenador

b) Concepto penal de programa de ordenador

2. Bases de datos electrónicas

3. Páginas Web

B) El elemento físico del sistema: hardware

1. Dispositivos de transmisión de datos

2. Memoria

3. Procesador

IV. Contenido del sistema: resultado del programa. Crítica

A) Obra resultante del programa

B) Acceso al sistema como acceso a datos

C) Valoración personal

CAPÍTULO VI. DELIMITACIÓN DE LOS MEDIOS COMISIVOS DEL DELITO: LA VULNERACIÓN DE LAS MEDIDAS DE SEGURIDAD ESTABLECIDAS PARA IMPEDIR EL ACCESO

I. Introducción

II. El inciso por cualquier medio o procedimiento

III. Vulneración de medidas de seguridad

A) Restricción del ámbito aplicativo

1. Consecuencias
2. La inclusión del inciso vulneración medidas de seguridad
3. Aplicación a ambas modalidades
4. Valoración personal

B) Concepto, naturaleza y tipología de medidas de seguridad

1. Concepto
2. Tipología
   a) Medidas de seguridad física
      i) Instrumentos Hardware: medios dispuestos directamente sobre el objeto
      ii) Instrumentos de tipo organizativo (establecidos para custodiar el sistema)
   b) Medidas de seguridad lógica
3. Naturaleza
   a) Discusión sobre las medidas de tipo lógico
   b) Discusión sobre las medidas de tipo físico
4. Cuestiones concursales
   a) Delito de allanamiento de morada
   b) Delito de daños

C) Vulneración de las medidas de seguridad

1. Presencia de las medidas
   a) Sistemas sin medidas de protección
   b) Estado de la medida en el momento de la comisión del delito
2. Criterio de la idoneidad
   a) Idoneidad cualitativa: complejidad técnica o eficacia de las medidas
   b) Idoneidad cuantitativa
3. Superación de las medidas

CAPÍTULO VII. EL ELEMENTO NEGATIVO DEL TIPO: LA AUTORIZACIÓN Y VOLUNTAD DEL TITULAR DEL SISTEMA

I. Introducción

II. La expresión sin estar debidamente autorizado

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

B) El concepto de autorización: presupuestos

1. Presupuestos objetivos de la autorización

a) Autorización como habilitación legal

b) Autorización como mera aquiescencia

c) Autorización oficial

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

C) El adverbio “debidamente”

1. Significación jurídica

2. ¿Accesoriedad del Derecho Penal?

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

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

A) Literalidad

B) Contenido

BIBLIOGRAFÍA