Convención del Consejo de Europa contra la Ciberdelincuencia

Elvira Tejada de la Fuente

Fiscal de Sala contra la Criminalidad Informática

Fiscalía General del Estado

Convenio contra la Ciberdelincuencia

* Origen: Consejo de Europa.- Budapest Noviembre 2001)

-Ratificación por España .- Junio 2010

-Ratificación Republica Domíncana.-Febrero 2013

-Documentos complementarios:

-Protocolo Adicional contra el Racismo y la Xenofobia en Internet

-Segundo Protocolo Adicional sobre obtención de evidencias electrónicas

* Proyección territorial.- Vocación de universalidad

-Países Miembros del Consejo de Europa (45 ratificaciones)

-Otros países firmantes: EEUU, Israel, Japón, Canadá, Sudáfrica..etc

-Países Iberoamericanos.

* Objeto: Articular mecanismos legales frente a la ciberdelincuencia

-Armonización normativa

-Reforzamiento instrumentos cooperación internacional

Convenio contra la Ciberdelincuencia

Estructura de la Convención

Capitulo I.- Terminología y definiciones

Capitulo II- Disposiciones para impulsar la elaboración de legislación adecuada para actuar frente a la ciberdelincuencia

-Sección Primera.- Normas penal-sustantivas
-Sección segunda.- Normas procesales

Capitulo III.-Cooperación Internacional

Capitulo IV.- Disposiciones Finales

Convención contra la Ciberdelincuencia
Armonización normativa: Aspectos Penal-sustantivo

-Definición de tipos penales (artículos 2 a 10 y 13)

a) Delitos c/ la confidencialidad, integridad y disponibilidad de datos y sistemas (arts. 2 a 6)

-acceso ilícito a sistemas, interceptación ilícita de datos y sistemas
ataques a la integridad de los datos y sistemas y abuso de dispositivos

b) Delitos informáticos (arts. 7 y 8)

-falsificación y fraude informático

c) Delitos relacionados con el contenido (art.9)

- delitos de pornografía infantil.- concepto de pornografía infantil

d) Delitos relacionados con infracciones de propiedad intelectual y otros derechos afines (art. 10)

- Disposiciones de carácter general (artículos 11 y 12)

-Tentativa y complicidad
- Responsabilidad penal de personas jurídicas.

Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas

Acceso ilícito a sistemas informáticos (art. 2º C Budapest)

* Requisitos obligatorios:

-Acceso deliberado e ilegitimo

-Intencionalidad de la conducta

- A la totalidad o una parte de un sistema informático

* Requisitos facultativos:

- Con vulneración de medida de seguridad

- Con intención de obtener datos informáticos

- Con otra intención delictiva

Legislación española.- art. 197 bis 1º CP

Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas

Interceptación ilícita (art. 3 Convención Budapest)

- Conductas:

  * Interceptar transmisiones no públicas de datos entre sistemas o entre dispositivos de un mismo sistema.

  * Captar emisiones electromagnéticas de los sistemas

- Requisitos comunes:

  - De forma deliberada e ilegítima

  - Utilizando artificios o instrumentos técnicos adecuados

Legislación española.- Art 197 bis 2º CP.

Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas

Delitos contra la integridad de datos y sistemas (arts. 4 y 5 Convención de Budapest):

-Art 4.- Realizar conductas que dañen, borren, deterioren, alteren o suprimen datos informáticos

requisito facultativo.- causar daños graves

-Art 5.- Obstaculizar gravemente el funcionamiento de un sistema mediante daños o alteraciones en los datos

*Requisitos comunes a ambas conductas:

-Actuación deliberada e ilegítima

Legislación española.- arts. 264 y 264 bis a 264 quater CP

Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas

*Abuso de dispositivos (artículo 6º C. de Budapest)

Acción: Producir, vender, adquirir para su uso, importar, o poner a disposición de otros :

-programas informáticos principalmente preparados

-contraseñas, códigos de acceso o datos similares

Requisitos:

- de forma deliberada e ilegítima

(por personas o entidades no autorizadas)

- para realizar acciones de acceso o interceptación ilícita o ataques a la integridad de los datos o de los sistemas

Legislación española.- arts. 197 ter y 264 ter C.P

Convención contra la Ciberdelincuencia Armonización Normativa

* **Aspectos procesales**:

Ámbito de aplicación de las disposiciones procesales del Convenio de Budapest (art 14):

- Delitos relacionados en los artículos 2 a 10
- Delitos cualquiera que sea su naturaleza cometidos a través de un sistema de información
- Obtención de pruebas electrónicas de cualquier delito

Convención contra la Ciberdelincuencia
Armonización normativa

* **Aspectos procesales**:

- Establecimiento de normativa común sobre aspectos procesales y de investigación:

a) conservación rápida de datos informáticos almacenados (art 16)

b) conservación y revelación parcial rápida de datos de tráfico (art 17)

c) solicitud a terceros de información o datos informáticos almacenados orden de presentación (art 18)

d) registro y confiscación de datos informáticos almacenados (art 19)

e) obtención en tiempo real de datos relativos al tráfico (art 20)

f) interceptación en tiempo real de datos relativos al contenido (art 21)

Registro y confiscación datos informáticos

***Artículo 19 Convención de Budapest**

*Contenido de la medida:

a) registro/acceso: a un sistema informático o parte del mismo o a los datos.

a un dispositivo de almacenamiento de datos.

- Acceso lícito a datos alojados en otro sistema situado en el propio territorio

b) Confiscación/incautación de datos o informaciones

objetivo: Preservación de la integridad de los datos

*Incautación física del dispositivo o del sistema

*Realización y conservación de copias de los datos

*Hacer inaccesibles o suprimir los datos.

*Deber de colaboración

Registro de dispositivos informáticos legislación española

***art 588 sexies LECrim.)**

-Objeto: dispositivos/sistemas informáticos incautados

- Exigencia de autorización judicial y motivación individualizada

  -excepción: supuestos urgencia.-convalidación posterior

- Contenido de la resolución judicial

  - Justificación de la medida.- principios art 588 bis a)
  - Contenido y alcance del registro
  - Medidas para preservar y garantizar la integridad de los datos
  - Realización de copias: posibilidad incautación dispositivos

- Acceso lícito a otro sistema informático.- autorización judicial

  -excepción: supuestos de urgencia.-convalidación posterior

- Deber de colaboración por parte de terceros.

Registro remoto de equipos informáticos legislación española

*** Artículo 588 septies LECrim.**

- Objeto del registro:

  dispositivos electrónicos; sistemas informáticos; sistemas de almacenamiento masivo y bases de datos.

- Herramienta limitada en su utilización a determinados delitos
- Autorización judicial motivada.- criterios y principios informadores
  - Contenido de la resolución judicial
    - -Aspectos específicos.- determinación del software o herramienta utilizada
      - agentes autorizados para la ejecución.
- Acceso ilícito a otro sistema informático con autorización judicial
- Deber de colaboración y sigilo de terceros.
- Periodo de duración de la medida .-un mes prorrogable hasta tres meses

Muchas Gracias