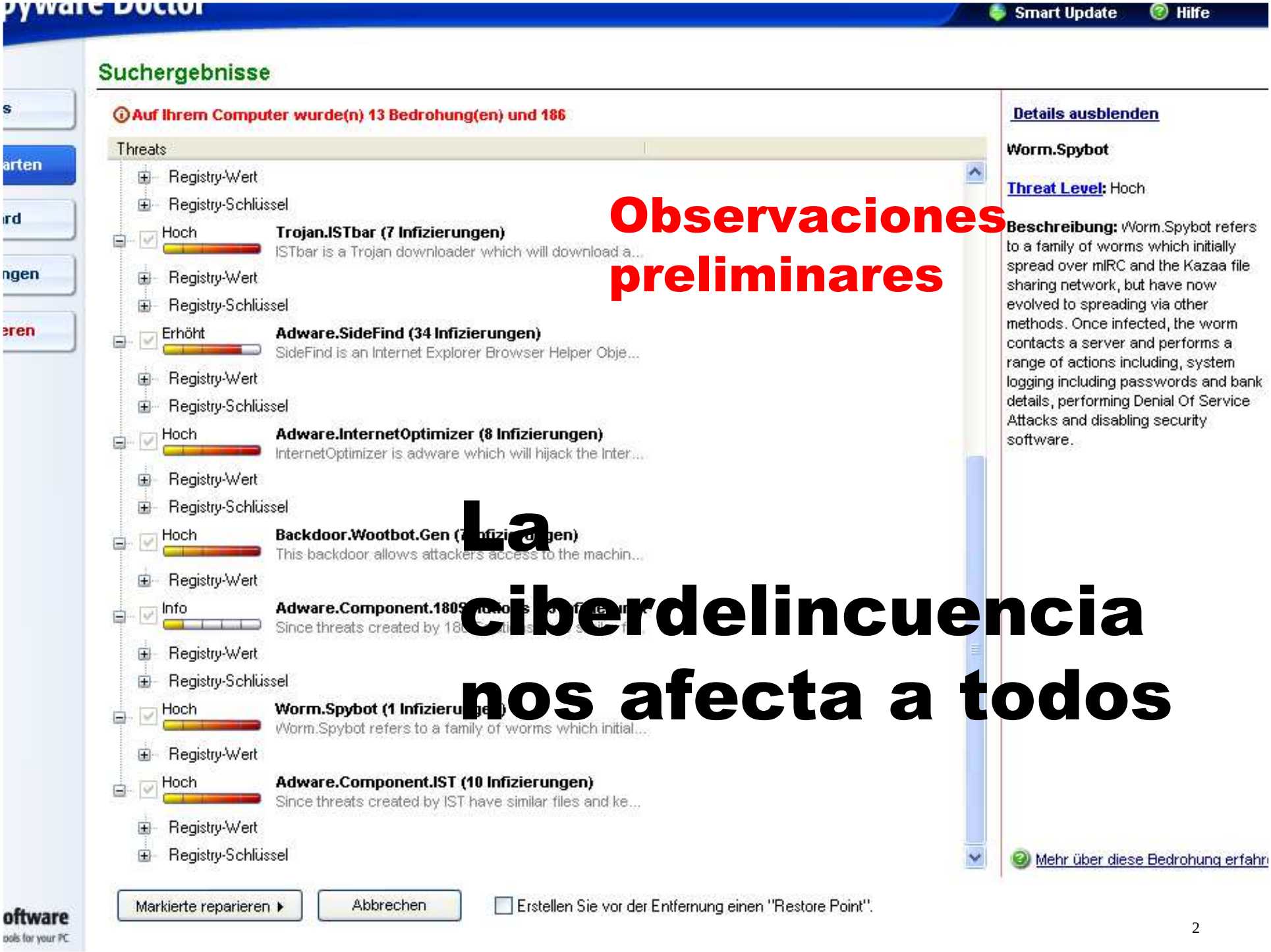
COUNCIL OF EUROPE CONSEIL DE L'EUROPE

www.coe.int/cybercrime

Tendencias del cibercrimen y medidas

América Latina: Taller Regional en Cibercrimen
Ciudad de México, 25 de Agosto 2010

Alexander Seger
Council of Europe,
Strasbourg, France
Tel +33-3-9021-4506
alexander.seger@coe.int



Observaciones preliminares

La ciberdelincuencia nos afecta a todos

Sobre el Consejo de Europa ... www.coe.int

Estrategia contra el delito económico

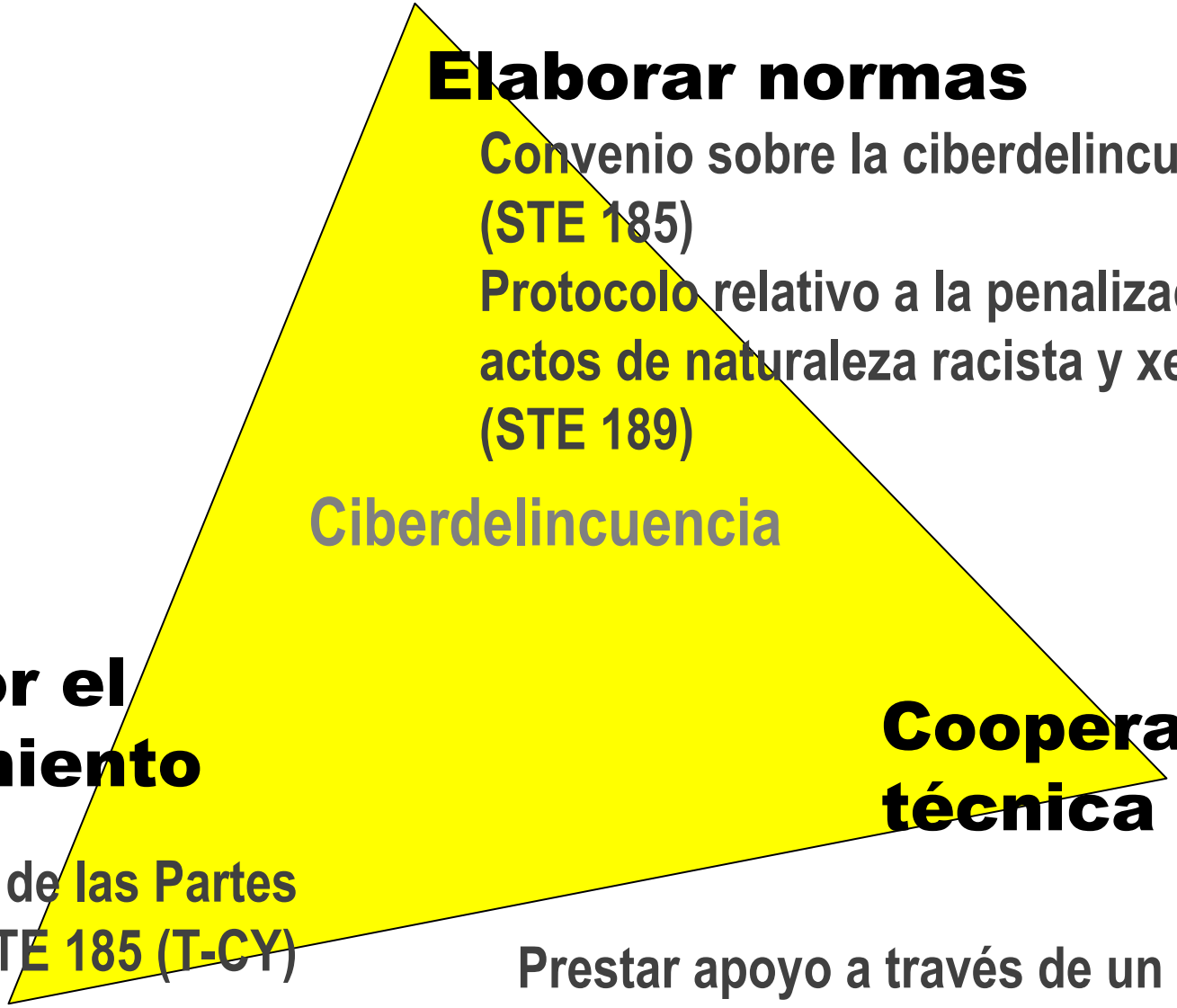
para promover

La democracia
El Estado de derecho
Los derechos humanos

Medidas contra el delito económico y el crimen organizado

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

El enfoque contra la ciberdelincuencia



1 Por qué deben tomarse medidas contra la ciberdelincuencia

Las sociedades de todo el mundo dependen considerablemente de las TIC, por lo que son muy vulnerables

- Incremento apreciable de los ciberdelitos (mensajes fraudulentos "phishing", virus "botnets", etc.)
- Mayor número de ciberdelitos cometidos con ánimo lucrativo
- Incremento de sitios Web que fomentan el ocio, el racismo y la violencia
- Piratería de programas informáticos
- Pornografía infantil
- Aumento de la cibercrimen organizado
- Blanqueo de dinero por Internet
- Terrorismo por Internet
- Ciberdelicuencia: pocos riesgos y muchas oportunidades

En 2010, existen más de 1.500 millones de usuarios de Internet en todo el mundo. Aun cuando el 99,9% fueran legítimos, 1 millón serían delincuentes potenciales. La necesidad de armonizar los derechos y libertades fundamentales y las preocupaciones en materia de seguridad.

5

Cibercrimen?

1. **Delitos contra la confidencalidad, la integridad y la disponibilidad de las datos y sistemas informáticos**

- Acceso ilícito
- Interceptación ilícita
- Ataques a la integridad de los datos
- Ataques a la integridad del sistema
- Abuso de los dispositivos

2. **Estafa informática, Falsedad informática**

3. **Delitos relacionados con el contenido (Infracciones relativas a la pornografía infantil)**

4. **Infracciones vinculadas a los atentados a la propiedad intelectual y a los derechos afines**

2 La respuesta del derecho penal

- Penalizar una conducta determinada ▶ Derecho penal sustantivo

- Velar por que las autoridades policiales/la justicia penal tengan medios a su alcance para investigar, juzgar y sentenciar por los ciberdelitos (acciones inmediatas, pruebas electrónicas) ▶ Derecho procesal

- Prever una cooperación internacional eficiente ▶ armonizar la legislación, elaborar disposiciones y establecer instituciones para la cooperación policial y judicial, y concluir o suscribir acuerdos

Derecho penal sustantivo

Legislación para tratar – como mínimo:

- **Acceso ilícito**
- **Interceptación ilícita**
- **Ataques a la integridad de los datos**
- **Ataques a la integridad del sistema**
- **Abuso de los dispositivos**
- **Falsificación informática**
- **Fraude informático**
- **Delitos relacionados con la pornografía infantil**
- **Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines**

¿Penalizar técnicas/tecnologías específicas o conductas específicas?

Legislación para prever – como mínimo:

- Conservación rápida de los datos informáticos almacenados y de los datos relativos al tráfico
- Orden de presentación
- Registro y confiscación de datos informáticos almacenados
- Obtención en tiempo real de datos informáticos (datos de tráfico, interceptación de datos relativos al contenido)
- Condiciones y salvaguardias

Cooperación internacional

Bases jurídicas/acuerdos para:

- Cooperación internacional, extradición, etc., en casos de ciberlincuencia
- Conservación rápida de datos informáticos almacenados y de los datos informáticos conservados
- Asistencia en relación con el acceso a datos informáticos almacenados
- Acceso transfronterizo a datos informáticos almacenados, con consentimiento o cuando sean accesibles al público
- Asistencia para la obtención en tiempo real de datos de tráfico, asistencia en relación con la interceptación de datos relativos al contenido
- Red 24/7

3 Convenio sobre la ciberdelincuencia (STE 185)

- Elaborado por el Consejo de Europa con la participación de Canadá, Estados Unidos, Japón y Sudáfrica
- Abierto a la firma en Budapest, en noviembre de 2001
- En vigor desde julio de 2004

+

Protocolo adicional relativo a la penalización de actos de naturaleza racista y xenófoba cometidos por medio de sistemas informáticos (STE 189)

- Abierto a la firma en enero de 2003
- En vigor desde marzo de 2006

Estructura del Convenio

Capítulo I – Terminología

Capítulo II - Medidas que deberán adoptarse a nivel nacional

- Sección 1 – Derecho penal sustantivo (delitos que deberán penalizarse)
- Sección 2 – Derecho procesal
- Sección 3 – Jurisdicción

Capítulo III - Cooperación internacional

- Sección 1 – Principios generales
- Sección 2 – Disposiciones específicas

Capítulo IV – Cláusulas finales

Capítulo II - Medidas que deberán adoptarse a nivel nacional

Sección 1 - Derecho penal sustantivo

- Título 1 – Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos (acceso ilícito, interceptación ilícita, ataques a la integridad de los datos, ataques a la integración del sistema, abuso de los dispositivos)
- Título 2 – Delitos informáticos (falsificación informática, fraude informático)
- Título 3 – Delitos relacionados con el contenido (pornografía infantil)
- Título 4 – Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines
- Título 5 – Otras formas de responsabilidad y de sanción (tentativa y complicidad, responsabilidad de las personas jurídicas, sanciones y medidas)

Sección 2 – Derecho procesal

- Título 1 – Disposiciones comunes (ámbito de aplicación de las disposiciones de procedimiento, condiciones y salvaguardias)
- Título 2 – Conservación rápida de datos informáticos almacenados (y de los datos relativos al tráfico)
- Título 3 – Orden de presentación
- Título 4 – Registro y confiscación de datos informáticos almacenados
- Título 5 – Obtención en tiempo real de datos informáticos (datos relativos al tráfico, interceptación de datos relativos al contenido)

Sección 3 – Jurisdicción

Capítulo III – Cooperación internacional

Sección 1 – Principios generales

- Artículo 23 – Principios generales relativos a la cooperación internacional
- Artículo 24 – Extradición
- Artículo 25 – Principios generales relativos a la asistencia mutua
- Artículo 26 – Información espontánea
- Artículo 27 – Procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables
- Artículo 28 – Confidencialidad y restricciones de uso

Sección 2 – Disposiciones específicas

- Art.29 – Conservación rápida de datos informáticos almacenados
- Art. 30 – Revelación rápida de datos conservados
- Art. 31 – Asistencia mutua en relación con el acceso a datos almacenados
- Art. 32 – Acceso transfronterizo a datos almacenados, con consentimiento o cuando sean accesibles al público
- Art. 33 – Asistencia mutua para la obtención en tiempo real de datos relativos al tráfico
- Art. 34 – Asistencia mutua en relación con la interceptación de datos relativos al contenido
- Art. 35 – Red 24/7

Capítulo IV – Cláusulas finales

- Art. 36 – Firma (abierta a los Estados miembros y no miembros del Consejo de Europa que hayan participado en su elaboración) y entrada en vigor
- Art. 37 – Adhesión al Convenio (todo Estado puede adherirse al Convenio tras haber obtenido el voto mayoritario del Comité de Ministros y el consentimiento unánime de las Partes que tengan derecho a formar parte del Comité de Ministros)
- Art. 40-43 – Declaraciones, reservas
- Art. 46 – Consultas entre las Partes

Aplicación – situación actual

- Entró en vigor en julio de 2004
- 30 ratificaciones + 16 firmas
- Firmado asimismo por Canadá, Estados Unidos (ratificación), Japón y Sudáfrica
- Se ha invitado a Chile, Costa Rica, Filipinas y México a adherirse al Convenio
- En muchos otros países se han adoptado o están en curso enmiendas legislativas y está considerándose la adhesión al Convenio

= Importante tendencia mundial a mejorar la legislación sobre la ciberdelincuencia

= El Convenio proporciona una norma mundial

4 Función del Convenio como legislación modelo

- Utilizar como lista de comprobación
- Comparar las disposiciones
- Utilizar el texto

Perfiles de los países en relación con la legislación sobre la ciberdelincuencia como instrumento para el análisis y el intercambio de buenas prácticas

www.coe.int/cybercrime

Disposicion del Convenio	Disposición en la legislación nacional
Art 4 Interferencias en el sistema	?
Art 6 Abuso de los dispositivos	?
Art 9 Pornografia infantil	?
Art 16 Conser-vación rápida	?
Art 18 Orden de presentación	?

Definiciones

Términos clave

- "sistema informático"
- "datos informáticos"
- "proveedor de servicios"
- "datos relativos al tráfico"

¿Cómo están definidos en su legislación?

Función del Convenio como legislación modelo - por ejemplo:

Artículo 1 del Convenio – Definiciones

- por "sistema informático" se entenderá todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa;

- por "datos informáticos" se entenderá toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función;

Función del Convenio como legislación modelo - por ejemplo:

Artículo 1 del Convenio – Definiciones

Art.35 (1) de la Ley de Rumania núm. 161/2003

- **por "sistema informático" se entenderá todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos por medio de un programa informático**

- **por "datos informáticos" se entenderá toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático. Esta categoría incluye todo programa informático diseñado para que un sistema informático ejecute una función**

Función del Convenio como legislación modelo - por ejemplo:

Artículo 1 del Convenio – Definiciones

Ley de la República Dominicana

Artículo 4.- Definiciones

- **Computadora: Cualquier dispositivo electrónico, independientemente de su forma, tamaño, capacidad, tecnología, capaz de procesar datos y/o señales, que realiza funciones lógicas, aritméticas y de memoria por medio de la manipulación de impulsos electrónicos, ópticos, magnéticos, electroquímicos o de cualquier otra índole, incluyendo todas las facilidades de entrada, salida, procesamiento, almacenaje, programas, comunicación o cualesquiera otras facilidades que estén conectadas, relacionadas o integradas a la misma.**

- **Datos: Es toda información que se transmite, guarda, graba, procesa, copia o almacena en un sistema de información de cualquiera naturaleza o en cualquiera de sus componentes, como son aquellos cuyo fin es la transmisión, emisión, almacenamiento, procesamiento y recepción de señales electromagnéticas, signos, señales, escritos, imágenes fijas o en movimiento, vídeo, voz, sonidos, datos por medio óptico, celular, radioeléctrico, sistemas electromagnéticos o cualquier otro medio útil a tales fines.**

Derecho penal sustantivo

¿Cómo trata su legislación:

- Acceso ilícito
- Interceptación ilícita
- Ataques a la integridad de los datos
- Ataques a la integridad del sistema
- Abuso de los dispositivos
- Falsificación informática
- Fraude informático
- Delitos relacionados con la pornografía infantil
- Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines

Artículo 2 del Convenio – Acceso ilícito

- Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno el acceso deliberado e ilegítimo a todo o parte de un sistema informático. Las Partes podrán exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos u otra intención delictiva, o en relación con un sistema informático conectado a otro sistema informático.

Función del Convenio como legislación modelo - por ejemplo:

Artículo 2 del Convenio – Acceso ilícito

Art.42 de la Ley de Rumania núm. 161/2003

1.El acceso, sin derecho, a un sistema informático.

Toda persona actuará sin derecho en las siguientes situaciones:

a) no está autorizada, en términos de la legislación o de un contrato;

b) supera los límites de la autorización;

c) no ha recibido la autorización de la persona cualificada para concederla, de conformidad con la legislación, para utilizar, administrar o controlar un sistema informático, o llevar a cabo investigaciones científicas en un sistema informático.

2. El acto se comete con el propósito de obtener datos informáticos.

3. El acto se comete infringiendo medidas de seguridad.

Función del Convenio como legislación modelo - por ejemplo:

Artículo 2 del Convenio – Acceso ilícito

República Dominicana (Ley 53-07)

Art. 6 Sec.1 Derecho Penal Sustantivo: El hecho de acceder a un sistema electrónico, informático, telemático o de telecomunicaciones, o a sus componentes, utilizando o no una identidad ajena, o excediendo una autorización, se sancionará con las penas de tres meses a un año de prisión y multa desde una vez a doscientas veces el salario mínimo.

Barbados (Abusos informáticos)

CONDUCTA PROHIBIDA

4. 1) Toda persona que, intencional o temerariamente, y sin una excusa o justificación legal,

a) acceda a todo el sistema informático o a una parte del mismo;

b) provoque que un programa se ejecute;

c) utilice el programa para acceder a datos;

d) copie o mueva el programa o los datos

i) a cualquier medio de almacenamiento distinto de aquél en el que se conservan el programa o los datos, o

ii) a un lugar diferente en el medio de almacenamiento en el que se conservan el programa o los datos, o

e) altere o suprima el programa o datos

será culpable de un delito y será castigada en un proceso acusatorio a una multa de 25.000 dólares o a una pena de prisión de dos años o a ambas cosas.

+ Secciones 9-12

Artículo 5 del Convenio – Ataques a la integridad del sistema

- Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.

Función del Convenio como legislación modelo - por ejemplo:

Artículo 5 del Convenio – Ataques a la integridad del sistema

Art.45 de la Ley de Rumania núm. 161/2003

Art. 45 – El acto consistente en obstaculizar seriamente, sin derecho, el funcionamiento de un sistema informático, mediante la introducción, transmisión, alteración, supresión o deterioro de datos informáticos, o mediante la restricción del acceso a dichos datos, constituye un delito penal y será castigado con una pena de prisión de tres a quince años.

Función del Convenio como legislación modelo - por ejemplo:

Artículo 5 del Convenio – Ataques a la integridad del sistema

República Dominicana (Ley 53-07)

- **Artículo 11.- Sabotaje. El hecho de alterar, maltratar, trabar, inutilizar, causar mal funcionamiento, dañar o destruir un sistema electrónico, informático, telemático o de telecomunicaciones, o de los programas y operaciones lógicas que lo rigen, se sancionará con las penas de tres meses a dos años de prisión y multa desde tres hasta quinientas veces el salario mínimo.**

Función del Convenio como legislación modelo - por ejemplo:

Artículo 5 del Convenio – Ataques a la integridad del sistema

Barbados

6. Toda persona que, intencional o temerariamente, y sin una excusa o justificación legal,

a) obstaculice el funcionamiento de un sistema informático

i) impidiendo el suministro de electricidad, permanentemente o de otro modo, a un sistema informático;

ii) causando interferencias electromagnéticas en un sistema informático;

iii) corrompiendo el sistema informático a través de cualquier medio;

iv) añadiendo, suprimiendo o alterando datos informáticos, o

b) interfiera en el funcionamiento de un sistema informático o con

una persona que esté utilizando o ejecutando legalmente un sistema informático, será culpable de un delito y será castigada en un proceso acusatorio a una multa de 50.000 dólares o a una pena de prisión de cinco años, o a ambas cosas.

Derecho procesal

¿Qué prevé su legislación procesal para:

- Conservación rápida de los datos informáticos almacenados y de los datos relativos al tráfico
- Orden de presentación
- Registro y confiscación de datos informáticos almacenados
- Obtención en tiempo real de datos informáticos (datos de tráfico, interceptación de datos relativos al contenido)
- Condiciones y salvaguardias?

Función del Convenio como legislación modelo - por ejemplo:

Artículo 16 del Convenio – Conservación rápida de datos informáticos almacenados

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para permitir a sus autoridades competentes ordenar o imponer de otro modo la conservación rápida de datos electrónicos específicos, incluidos los datos relativos al tráfico, almacenados por medio de un sistema informático, en particular cuando existan motivos para creer que dichos datos son particularmente susceptibles de pérdida o de modificación.

2. Cuando una Parte aplique lo dispuesto en el párrafo 1 anterior por medio de una orden impartida a una persona de que conserve determinados datos almacenados que se encuentren en poder o bajo el control de esa persona, la Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a dicha persona a conservar y a proteger la integridad de los datos durante el tiempo necesario, hasta un máximo de noventa días, con el fin de que las autoridades competentes puedan obtener su revelación. Las Partes podrán prever la renovación de dicha orden.

3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a la persona que custodia los datos o a otra persona encargada de su conservación a mantener en secreto la ejecución de dichos procedimientos durante el tiempo previsto en su derecho interno.

Función del Convenio como legislación modelo - por ejemplo:

Artículo 16 del Convenio – Conservación rápida de datos informáticos almacenados

Art.54 de la Ley de Rumania núm. 161/2003

- En casos urgentes y debidamente justificados, si existen datos o indicaciones confirmadas relativas a la preparación o comisión de un delito penal por medio de sistemas informáticos, a efectos de obtener pruebas o de identificar a los delincuentes, puede ordenarse la conservación rápida de los datos informáticos o de los datos relativos al tráfico, que están en peligro de ser destruidos o alterados.
- La conservación será ordenada por el fiscal por conducto de una ordenanza motivada, a solicitud del órgano de investigación penal o *ex-officio* y, durante el juicio, por mandato judicial.
- La medida se ordena por un período que no excederá de 90 días y que podrá ser superado, sólo una vez, por un período que no excederá de 30 días.
- La ordenanza del fiscal o el mandato judicial se enviará, inmediatamente, a todo proveedor de servicios o toda otra persona que esté en posesión de los datos, y se obligará a la persona respectiva a conservar rápidamente los datos en condiciones de confidencialidad.

Función del Convenio como legislación modelo - por ejemplo:

Artículo 16 del Convenio – Conservación rápida de datos informáticos almacenados

República Dominicana

Artículo 53.- Conservación de los datos. Las autoridades competentes actuarán con la celeridad requerida para conservar los datos contenidos en un sistema de información o sus componentes, o los datos de tráfico del sistema, principalmente cuando éstos sean vulnerables a su pérdida o modificación.

[La reglamentación para dar cumplimiento a esta disposición está en curso de elaboración]

Función del Convenio como legislación modelo - por ejemplo:

Artículo 16 del Convenio – Conservación rápida de datos informáticos almacenados

Barbados

20. 1) En los casos en que un agente de policía convenza a un Juez sobre la base de una
solicitud ex parte acerca de que

a) los datos almacenados en un sistema informático serán solicitados razonablemente a los efectos de una investigación penal, y

***b) existe el riesgo de que los datos sean destruidos o se hagan inaccesibles*,**

el Juez podrá emitir una orden que exija a la persona que controla el sistema informático conservar los datos especificados en la orden por un período de hasta 14 días.

2) El período podrá prolongarse más de 14 días, tras los cuales, sobre la base de una solicitud ex parte*, el Juez autorizará una extensión por otro período específico de tiempo*.

Cooperación internacional

- ¿Cuál es la base jurídica de su país para:
- Cooperación internacional, extradición, etc., en casos de ciberlincuencia
- Conservación rápida de datos informáticos almacenados y de los datos informáticos conservados
- Asistencia en relación con el acceso a datos informáticos almacenados
- Acceso transfronterizo a datos informáticos almacenados, con consentimiento o cuando sean accesibles al público
- Asistencia para la obtención en tiempo real de datos de tráfico, asistencia en relación con la interceptación de datos relativos al contenido
- Red 24/7

5 El Convenio como marco para la cooperación internacional

- El Convenio (capítulo III) se utiliza cada vez más como base jurídica para la cooperación internacional
- Contribuye a la creación de 24/7 puntos adicionales de contacto
- Ejemplos de buenas prácticas disponibles

Cuestiones:

- Necesidad de aumentar el número de Estados Partes en el Convenio
- Necesidad de aumentar la eficacia de 24/7 puntos de contacto
- Unas medidas preliminares (p.ej., la conservación rápida) deben ir seguidas de un proceso eficiente de asistencia jurídica mutua

38

6 Adhesión al Convenio – Beneficios para los países de las Américas

- Enfoque nacional coherente de la legislación sobre la ciberdelincuencia
- Instrumentos para la recopilación de pruebas electrónicas
- Instrumentos para la investigación del blanqueo de dinero por Internet, el ciberterrorismo y otros delitos graves
- Armonización y compatibilidad de las disposiciones de derecho penal relativas a la ciberdelincuencia con las de otros países
- Base jurídica e institucional para el cumplimiento de la legislación a nivel internacional y la cooperación judicial con otras Partes en el Convenio
- Participación en las consultas celebradas por las Partes en el Convenio
- El tratado como plataforma que facilita la cooperación público-privada

7 Medidas que deberán adoptarse

- Tomar medidas para fortalecer la legislación, según proceda

- Adhesión al Convenio como un marco para la cooperación internacional

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Gracias.

Alexander.seger@coe.int