COUNCIL OF EUROPE CONSEIL DE L'EUROPE

www.coe.int/cybercrime

el Convenio sobre cibercriminalidad del Consejo de Europa

Bogota, Colombia, October 2007

Alexander Seger
Consejo de Europa
Estrasburgo (Francia)
Tel +33-3-9021-4506
alexander.seger@coe.int
www.coe.int/economiccrime

1

1 Por qué deben tomarse medidas contra la cibercriminalidad

- Incremento apreciable de los cibercrímenes (mensajes fraudulentos "phising", virus "botnets", etc.)
- Mayor número de cibercrímenes 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 cibercriminalidad organizada
- Blanqueo de dinero por Internet
- Terrorismo por Internet
- Cibercriminalidad: poco riesgo y muchas oportunidades

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

En 2007, existen más de 1.000 millones de usuarios de Internet en todo el mundo. Aun cuando el 99.9% fueran legítimos, 1 millón serían delincuentes potenciales

La necesidad de equilibrar los derechos y libertades fundamentales y las preocupaciones en materia de seguridad.

2

2

Consejo de Europa

Convenio sobre cibercriminalidad (ETS 185)

+

Protocolo adicional relativo a actos de naturaleza racista y xenófoba cometidos a través de sistemas informáticos (ETS 189)

3

Estructura del Convenio

Capítulo I – Terminología

Capítulo II - Medidas que deben ser adoptadas a nivel nacional
- Sección 1 – Derecho penal material (delitos que deben penalizarse)
- Sección 2 – Derecho procesal
- Sección 3 – Jurisdicción

Capítulo III - Cooperación internacional
- Sección 1 – Principios generales
- Sección 2 – Disposiciones específicas

Capítulo IV – Cláusulas finales

4

Capítulo II - Medidas que deben ser adoptadas a nivel nacional

Sección 1 - Derecho penal material

- Título 1 – Infracciones contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos (acceso ilícito, inter-ceptación ilícita, atentados contra la integridad de los datos, atentados contra la integración del sistema, abuso de equipos e instrumentos técnicos)
- Título 2 – Infracciones informáticas (falsedad informática, estafa informática)
- Título 3 – Infracciones relativas al contenido (pornografía infantil)
- Título 4 – Infracciones vinculadas a los atentados a la propiedad intelectual y a los derechos afines
- Título 5 – Otras formas de responsabilidad y sanción (tentativa y complicidad, responsabilidad de las personas jurídicas, sanciones y medidas)

5

Sección 2 – Derecho procesal

- Título 1 – Disposiciones comunes (ámbito de aplicación de las medidas de derecho procesal, condiciones y garantías)
- Título 2 – Conservación inmediata de datos informáticos almacenados (y de los datos de tráfico)
- Título 3 – Mandato de comunicación
- Título 4 – Registro y decomiso de datos informáticos almacenados
- Título 5 – Recogida en tiempo real de datos informáticos (datos de tráfico, interceptación de datos relativos al contenido)

Sección 3 – Jurisdicción

6

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 cooperación
- Artículo 26 – Información espontánea
- Artículo 27 – Procedimiento relativo a las demandas de colaboración en ausencia de acuerdo internacional aplicable
- Artículo 28 – Confidencialidad y restricciones de uso

Capítulo III – Cooperación internacional ...

Sección 2 – Disposiciones específicas

- Art.29 – Conservación inmediata de datos informáticos almacenados
- Art. 30 – Comunicación inmediata de los datos informáticos conservados
- Art. 31 – Asistencia concerniente al acceso a datos informáticos almacenados
- Art. 32 – Acceso transfronterizo a los datos informáticos almacenados, con consentimiento o de libre acceso
- Art. 33 – Asistencia para la recogida en tiempo real de datos de tráfico
- Art. 34 – Asistencia en materia de interceptación de datos relativos al contenido
- Art. 35 – Red 24/7

Capítulo IV – Cláusulas finales

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

Protocolo adicional relativo a actos de naturaleza racista y xenófoba cometidos a través de sistemas informáticos (ETS 189)

- Art. 3 – Difusión de material racista y xenófobo a través de sistemas informáticos
- Art. 4 – Amenaza motivada por el racismo y la xenofobia
- Art. 5 – Insulto motivado por el racismo y la xenofobia
- Art. 6 – Denegación, minimización flagrante, aprobación o justificación del genocidio o de otros crímenes contra la humanidad.

3 Aplicación – situación actual

Convenio sobre la cibercriminalidad (ETS 185)
Entró en vigor en julio de 2004

- 21 ratificaciones + 22 firmas
- Firmado asimismo por Canadá, Estados Unidos (ratificacion), Japón y Sudáfrica
- Legislative amendments and ratification process underway in many other countries

Protocolo adicional relativo a actos de naturaleza racista y xenófoba cometidos a través de sistemas informáticos (ETS 189)

- 10 ratificaciones + 21 firmas (incluido Canadá)
- Entró en vigor el 1º de marzo de 2006

Ejemplo: Rumania

- Firmó el Convenio en 2001
- Analizó la legislación en vigor
- Redactó la ley 161/2003 sobre la transparencia, prevención y control de la corrupción, incluido el Título III sobre la prevención y lucha contra la cibercriminalidad
- Disposiciones relativas a la cooperación sustantiva, procesal e internacional
- Texto del Convenio como base
- Otras leyes sobre pornografía, y sobre derechos de autor y derechos relacionados
- Examinado por el Consejo de Europa en marzo de 2004
- Ratificó el Convenio en mayo de 2004
- Autoridad rumana competente: Servicio para la lucha contra la cibercriminalidad, establecido en la Oficina del Fiscal del Tribunal Supremo de Casación

Problemas que han surgido:

- Numerosas investigaciones y enjuiciamientos, pero poco veredictos
- Motivos: orden de comparecencia de testigos extranjeros y falta de formación de la policía, fiscales y jueces (en particular los de primera instancia)

4 Supervisión del tratado

El Comité para el Convenio sobre cibercriminalidad (T-CY) – Secunda consulta de las Partes (sobre el art. 46) en Estrasburgo (Francia), junio de 2007.

- Eficacia del Convenio
- Papel de los funcionarios de servicios policiales
- Cooperación del sector encargado del cumplimiento de la ley y el sector privado
- Operación de la red 24/7
- Ampliación o enmienda del Convenio

www.coe.int/economiccrime

5 Adhesión al Convenio – Beneficios para Colombia

- Enfoque nacional coherente de la legislación sobre cibercriminalidad
- 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 cibercriminalidad 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 de las partes en el Convenio
- El tratado como plataforma que facilita la cooperación público-privada

6 Conclusiones

The legislative response to cybercrime

- Criminalise certain conduct ▪ substantive criminal law
- Give law enforcement/criminal justice the means to investigate, prosecute and adjudicate cybercrimes (immediate actions, electronic evidence) ▪ criminal procedure law
- Allow for efficient international cooperation ▪ harmonise legislation, provisions and institutions for police and judicial cooperation provisions, conclude or join agreements

Key terms:

- "Computer system"
- "Computer data"
- "Service provider"
- "Traffic data"

How are these defined in your legislation?

Terminología:

- "sistema informático"
- "datos informáticos"
- "prestator de servicio"
- "datos de tráfico"

Definiciones en su legislacion?

Substantive law

How does your legislation deal with:

- Illegal access to a computer system
- Illegal interception
- Data interference
- System interference
- Misuse of devices
- Computer-related forgery
- Computer-related fraud
- Child pornography
- Infringement of copyright and related rights by means of a computer system?

Derecho penal material

Medidas legislativas para prever como infraccion penal:

- Acceso ilícito
- Interception ilicitá
- Attentados contra la integridad de los datos
- Attentados contra la integridad del sistema
- Abuso de equipos e instrumentos técnicos
- Falsedad informática
- Estafa informática
- Pornografía infantil
- Atentados a la propiedad intelectual y a los derechos afines

Procedural measures

How does your procedural legislation provide for:

- Expedited preservation of stored computer data
- Expedited preservation and partial disclosure of traffic data
- Production order
- Search and seizure of stored computer data
- Real-time collection of traffic data
- Interception of content data
- Procedural safeguards?

Derecho procesal

Medidas legislativas para :

- Conservación inmediata de datos informáticos almacenados
- Conservación inmediata de los datos de tráfico
- Mandato de comunicación
- Registro y decomiso de datos informáticos almacenados
- Recogida en tiempo real de datos informáticos
- interceptación de datos relativos al contenido
- condiciones y garantías?

International cooperation

How does your legislation provide for:

- Expedited preservation of computer data
- Expedited disclosure of preserved computer data
- Mutual assistance regarding accessing stored computer data
- Trans-border access to stored computer data (public/with consent)
- Mutual assistance in real-time collection of traffic data
- Mutual assistance regarding interception of content data
- 24/7 network

Cooperación internacional

Medidas legislativas para :

- Conservación inmediata de datos informáticos almacenados
- Comunicación inmediata de los datos informáticos conservados
- Asistencia concerniente al acceso a datos informáticos almacenados
- Acceso transfronterizo a los datos informáticos almacenados, con consentimiento o de libre acceso
- Asistencia para la recogida en tiempo real de datos de tráfico
- Asistencia en materia de interceptación de datos relativos al contenido
- Art. 35 – Red 24/7

Muchos buenos argumentos para aplicar el Convenio y su protocolo!

Gracias por su atención.

alexander.seger@coe.int
www.coe.int/economiccrime