COMISIÓN DE LAS COMUNIDADES EUROPEAS

Bruselas, 22.5.2007
COM(2007) 267 final

COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO Y AL COMITÉ DE LAS REGIONES

Hacia una política general de lucha contra la ciberdelincuencia

{SEC(2007) 641}
{SEC(2007) 642}

COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO Y AL COMITÉ DE LAS REGIONES

Hacia una política general de lucha contra la ciberdelincuencia

1. INTRODUCCIÓN

1.1. ¿Qué es la ciberdelincuencia?

Los sistemas informáticos cobran cada vez mayor importancia en nuestras sociedades, y su seguridad abarca numerosos aspectos, entre los cuales la lucha contra la ciberdelincuencia constituye un elemento básico. A falta de una definición comúnmente aceptada de ciberdelincuencia, los términos «ciberdelincuencia», «delincuencia informática», «delincuencia relacionada con los ordenadores» o «delincuencia de alta tecnología» se utilizan a menudo indistintamente. A efectos de la presente Comunicación, por «ciberdelincuencia» se entienden las «actividades delictivas realizadas con ayuda de redes de comunicaciones y sistemas de información electrónicos o contra tales redes y sistemas».

En la práctica, el término ciberdelincuencia engloba tres tipos de actividades delictivas. El primero comprende **formas tradicionales de delincuencia,** como el fraude o la falsificación, aunque en el contexto cibernético se refiere específicamente a los delitos cometidos mediante las redes de comunicaciones y los sistemas de información electrónicos (en lo sucesivo, redes electrónicas). El segundo se refiere a la publicación de **contenidos ilegales** a través de medios de comunicación electrónicos (por ejemplo, imágenes de abuso sexual a menores o incitaciones al odio racial). El tercero incluye **delitos específicos de las redes electrónicas**, por ejemplo los ataques contra los sistemas informáticos, la denegación de servicio y la piratería. Estos ataques también se pueden dirigir contra infraestructuras críticas fundamentales en Europa y afectar a sistemas de alerta rápida existentes en numerosos ámbitos, con consecuencias potencialmente desastrosas para el conjunto de la sociedad. La característica común de los tres tipos de delitos es que pueden ser cometidos a gran escala y que puede mediar una enorme distancia geográfica entre el acto delictivo y sus efectos. Por lo tanto, los aspectos técnicos de los métodos de investigación aplicados son a menudo similares. La presente Comunicación se centrará en estos puntos comunes.

1.2. Evolución reciente en materia de ciberdelincuencia

1.2.1. Generalidades

Debido a la evolución constante de las actividades delictivas y a la falta de información fiable resulta difícil hacerse una idea exacta de la situación actual. Ahora bien, cabe discernir algunas tendencias generales:

- el número de delitos informáticos está aumentando y las actividades delictivas se están sofisticando e internacionalizando cada vez más[1];

- indicios inequívocos apuntan a una implicación creciente de grupos de delincuencia organizada en la ciberdelincuencia;

- sin embargo, el número de procedimientos incoados en Europa en el marco de la cooperación transfronteriza de los organismos encargados de la aplicación de ley no está aumentando.

1.2.2. Delincuencia tradicional en las redes electrónicas

La mayor parte de los delitos se pueden cometer con ayuda de las redes electrónicas. De hecho, diversos tipos de fraude o intentos de fraude son particularmente frecuentes y constituyen una forma de delincuencia cada vez más extendida en las redes electrónicas. Instrumentos como la usurpación de identidad, las estafas por internet (*phishing*[2]), los envíos masivos de correo basura y los códigos malévolos pueden servir para cometer fraudes a gran escala. El comercio ilícito nacional e internacional a través de internet constituye otro problema en aumento. Incluye el tráfico de drogas, armas y especies amenazadas.

1.2.3. Contenidos ilegales

Cada vez es mayor el número de sitios de contenido ilegal accesibles en Europa. Difunden imágenes de abuso sexual de menores, incitan a cometer atentados terroristas o hacen apología de la violencia, el terrorismo, el racismo y la xenofobia. La acción coercitiva contra ellos es muy difícil, pues sus propietarios y administradores se encuentran a menudo en países distintos del país afectado, con frecuencia fuera de la UE. Estos sitios pueden ser trasladados con gran rapidez, incluso fuera del territorio de la UE, y la definición de ilegalidad varía considerablemente de un Estado a otro.

1.2.4. Delitos específicos de las redes electrónicas

Todo parece indicar que se está produciendo un aumento de la frecuencia de los ataques de gran envergadura dirigidos contra sistemas informáticos, organizaciones o particulares (a menudo a través de las llamadas «redes de zombis»[3]). Recientemente también se han registrado casos de ataques directos sistemáticos, bien coordinados y a gran escala, contra las infraestructuras informáticas críticas de un Estado. El fenómeno se ha agravado por la fusión de las tecnologías y la interconexión acelerada de los sistemas informáticos, que han hecho más vulnerables dichos sistemas. Con frecuencia los ataques están bien organizados y se realizan con fines de extorsión. Cabe suponer que la amplitud de estos incidentes se minimiza, en parte debido al perjuicio comercial que podría entrañar la divulgación de los problemas de seguridad.

---

1 La mayoría de las afirmaciones sobre las tendencias actuales incluidas en esta Comunicación proceden del Estudio de evaluación del impacto de una Comunicación sobre la ciberdelincuencia encargado por la Comisión en 2006 (contrato nº JLS/2006/A1/003).

2 Por «*phishing*» se entiende el intento de obtener información confidencial (contraseñas y datos de tarjetas de crédito, por ejemplo) de manera fraudulenta, usurpando la personalidad de un interlocutor fiable en una comunicación electrónica.

3 La red de zombis o «*botnet*» es una red de ordenadores controlados de modo remoto por un pirata informático para la ejecución de diversos programas.

1.3. Objetivos

Habida cuenta de este entorno en mutación, urge tomar medidas, a escala nacional y europea, contra todas las formas de ciberdelincuencia, las cuales constituyen amenazas cada vez más graves para las infraestructuras críticas, la sociedad, las empresas y los ciudadanos. La protección de las personas contra la ciberdelincuencia se ve a menudo complicada por problemas relativos a la determinación de la jurisdicción competente, la legislación aplicable, la aplicación transfronteriza o el reconocimiento y la utilización de pruebas electrónicas. La dimensión esencialmente transfronteriza de la ciberdelincuencia acentúa estas dificultades. Para afrontar estas amenazas, la Comisión está poniendo en marcha una iniciativa de política general destinada a mejorar la coordinación europea e internacional en materia de lucha contra la ciberdelincuencia.

El objetivo es consolidar la lucha contra la ciberdelincuencia a escala nacional, europea e internacional. La Comisión y los Estados miembros consideran prioritaria desde hace tiempo la profundización del desarrollo de una política específica de la UE. La iniciativa se centrará en dos dimensiones de esta lucha, el cumplimiento de la legislación y el Derecho penal. La política, que complementará otras medidas adoptadas por la UE para mejorar la seguridad en el ciberespacio en general, comprenderá a la postre los siguientes aspectos: mejora de la cooperación operativa de las autoridades policiales y judiciales; mejora de la cooperación y la coordinación políticas entre los Estados miembros; cooperación política y jurídica con terceros países; sensibilización; formación; investigación; intensificación del diálogo con la industria y posibles medidas legislativas.

La política en materia de lucha contra la ciberdelincuencia y su enjuiciamiento se definirá y aplicará de manera plenamente respetuosa con los derechos fundamentales, en especial los de la libertad de expresión, el respeto de la vida privada y familiar y la protección de los datos personales. Todas las medidas legislativas adoptadas en el marco de dicha política serán examinadas en primer lugar por lo que respecta a su compatibilidad con tales derechos, en especial los consagrados en la Carta de los Derechos Fundamentales de la UE. Procede también señalar que todas las iniciativas de esta naturaleza se llevarán a cabo teniendo debidamente presentes los artículos 12 a 15 de la Directiva sobre el comercio electrónico[4], en todos los casos en que este instrumento jurídico sea de aplicación.

El objetivo de la presente Comunicación se puede dividir en tres aspectos operativos principales, sintetizados como sigue:

- mejorar y facilitar la coordinación y la cooperación entre las unidades especializadas en la ciberdelincuencia, las autoridades competentes y otros expertos de la Unión Europea;

- desarrollar, en colaboración con los Estados miembros y las organizaciones y partes interesadas a escala internacional y de la UE, un marco político coherente para la UE en materia de lucha contra la ciberdelincuencia;

- sensibilizar sobre los costes y los peligros que conlleva la ciberdelincuencia.

---

[4] Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (DO L 178, 17.7.200, p. 1).

2. INSTRUMENTOS JURÍDICOS VIGENTES EN MATERIA DE LUCHA CONTRA LA CIBERDELINCUENCIA

2.1. Instrumentos y medidas existentes a escala de la UE

La presente Comunicación, relativa a la política en materia de ciberdelincuencia, consolida y desarrolla la Comunicación de 2001 titulada «Creación de una sociedad de la información más segura mediante la mejora de la seguridad de las infraestructuras de información y la lucha contra los delitos informáticos»[5] (en lo sucesivo, la Comunicación de 2001). Al hilo de esta última, que contemplaba diversas disposiciones legislativas, sustantivas y de procedimiento, dirigidas a reprimir las actividades delictivas nacionales y transnacionales, surgieron varias propuestas importantes, en particular la que dio lugar a la Decisión marco 2005/222/JAI, relativa a los ataques contra los sistemas de información[6]. En este contexto, procede también señalar la adopción de otros instrumentos legislativos más generales, que abarcan asimismo aspectos de la lucha contra la ciberdelincuencia, como la Decisión marco 2001/413/JAI, sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo[7].

La Decisión marco 2004/68/JAI, relativa a la lucha contra la explotación sexual de los niños y la pornografía infantil[8], constituye un buen ejemplo de la especial atención que presta la Comisión a la **protección de la infancia**, sobre todo en relación con la lucha contra todo tipo de material de abuso sexual de menores que se pueda difundir ilícitamente a través de los sistemas informáticos, una prioridad horizontal que se mantendrá en el futuro.

Para abordar los desafíos que se plantean en relación con la seguridad en la sociedad de la información, la Comunidad Europea ha elaborado un enfoque en favor de la seguridad de las redes y la información centrado en tres ejes: medidas específicas de seguridad de las redes y la información, el marco reglamentario para las comunicaciones electrónicas y la lucha contra la ciberdelincuencia. Si bien es cierto que estos tres aspectos pueden, hasta cierto punto, desarrollarse por separado, sus numerosas interdependencias abogan a favor de una estrecha coordinación. En el ámbito conexo de la seguridad de las redes y la información, una Comunicación titulada «Seguridad de las redes y de la información: Propuesta para un enfoque político europeo[9]» fue adoptada en 2001 por la Comisión, en paralelo a la dedicada ese mismo año a la ciberdelincuencia. La Directiva 2002/58/CE sobre la privacidad y las comunicaciones electrónicas establece la obligación, para los proveedores de servicios de comunicaciones electrónicas disponibles al público, de salvaguardar la seguridad de sus servicios. También contempla disposiciones contra los envíos masivos de correo basura y los programas espía. Desde entonces, la política relativa a la seguridad de las redes y la información se ha ido completando mediante varias iniciativas, en particular: la Comunicación titulada «Una estrategia para una sociedad de la información segura[10]», que presenta una estrategia revitalizada y define el marco que permite profundizar y precisar un planteamiento coherente en este ámbito; la Comunicación sobre la lucha contra el *spam*, los programas espía y los programas maliciosos[11]; y la creación, en 2004, de la Agencia Europea

---

5 COM(2000) 890, 26.1.2001.
6 DO L 69, 16.3.2005, p. 67.
7 DO L 149, 2.6.2001, p. 1.
8 DO L 13, 20.1.2004, p. 44.
9 COM(2001) 298.
10 COM(2006) 251.
11 COM(2006) 688.

de Seguridad de las Redes y de la Información[12], cuyo objetivo principal es prestar ayuda a la Comisión y a los Estados miembros y desarrollar conocimientos especializados en aras del fomento de la cooperación entre los sectores público y privado. Los **resultados de la investigación** en el ámbito de las tecnologías de protección de los sistemas informáticos desempeñarán también un papel importante en la lucha contra la ciberdelincuencia. Por consiguiente, tanto las tecnologías de la información y la comunicación como la seguridad figuran entre los objetivos del Séptimo Programa Marco de Investigación de la UE, que se aplicará durante el período 2007-2013[13]. La revisión del marco reglamentario de las comunicaciones electrónicas podría dar lugar a modificaciones que aumenten la eficacia de las disposiciones relativas a la seguridad de la Directiva sobre la privacidad y las comunicaciones electrónicas y de la Directiva relativa al servicio universal (2002/22/CE)[14].

2.2. Instrumentos internacionales existentes

Debido a la naturaleza global de las redes informáticas, ninguna política de lucha contra la ciberdelincuencia puede ser eficaz si los esfuerzos se circunscriben al interior de la UE. Los delincuentes no sólo pueden atacar los sistemas informáticos o cometer delitos de un Estado miembro a otro, sino que también pueden hacerlo fácilmente desde puntos ajenos a la jurisdicción de la UE. Por consiguiente, la Comisión participa activamente en los foros y las estructuras de cooperación internacionales, en particular en el Grupo de Lyón-Roma del G8, sobre la delincuencia de alta tecnología, y en los proyectos gestionados por Interpol. En especial, la Comisión sigue atentamente la labor de la Red de contactos permanentes en el ámbito de la delincuencia internacional de alta tecnología (Red 24/7)[15], a la que se han adherido numerosos países de todo el mundo, entre ellos la mayoría de los Estados miembros de la UE. Dicha Red permite agilizar los contactos entre los Estados participantes y establece puntos de contacto disponibles las veinticuatro horas del día para los casos en que son necesarias pruebas electrónicas o la ayuda urgente de las autoridades policiales y judiciales de otros países.

Sin duda, el principal instrumento europeo e internacional en este ámbito es el Convenio del Consejo de Europa de 2001 sobre la ciberdelincuencia[16]. Este Convenio, adoptado en 2004 y en vigor desde ese mismo año, contiene definiciones comunes de diversos tipos de delitos informáticos y sienta las bases de una cooperación judicial operativa entre los Estados signatarios. Lo han suscrito numerosos países, entre ellos todos los Estados miembros, los Estados Unidos de América y otros Estados no europeos. No obstante, algunos Estados miembros todavía no han ratificado el Convenio ni el Protocolo adicional relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos. Vista la importancia que se atribuye al Convenio, la Comisión animará a los Estados miembros y a los terceros países pertinentes a ratificarlo y estudiará la posibilidad de que la Comunidad Europea devenga Parte del mismo.

---

12 Reglamento (CE) n° 460/2004, por el que se crea la Agencia Europea de Seguridad de las Redes y de la Información, (DO L 77, 13.3.2004, p. 1).

13 En el marco del 6º Programa Marco de Investigación y Desarrollo Tecnológico, la Unión Europea ya ha apoyado, con buenos resultados, varios proyectos de investigación pertinentes en este ámbito.

14 COM(2006) 334, SEC(2006) 816, SEC(2006) 817.

15 Véase el artículo 35 del Convenio del Consejo de Europa sobre la ciberdelincuencia.

16 https://www.gdt.guardiacivil.es/media/Convenio_Ciberdelincuencia.pdf

3. DESARROLLO ULTERIOR DE INSTRUMENTOS ESPECÍFICOS EN LA LUCHA CONTRA LA CIBERDELINCUENCIA

3.1. Consolidación de la colaboración operativa de las autoridades policiales y judiciales y de la labor de formación a escala comunitaria

La ausencia o la infrautilización de estructuras inmediatas para la **cooperación operativa transfronteriza** constituye todavía una deficiencia grave en el ámbito de la justicia, la libertad y la seguridad. En los casos urgentes de ciberdelincuencia, la ayuda mutua tradicional ha resultado lenta e ineficaz, y el desarrollo de las nuevas estructuras de cooperación sigue siendo insuficiente. Si bien es cierto que las autoridades judiciales y policiales de los distintos países europeos colaboran estrechamente a través de Europol, Eurojust y otras estructuras, queda patente la necesidad de reforzar y clarificar las responsabilidades. De las consultas emprendidas por la Comisión se desprende que estos canales cruciales no se utilizan de manera óptima. El planteamiento europeo, más coordinado, debe ser tan operativo como estratégico y englobar también el intercambio de información y buenas prácticas.

En el futuro próximo la Comisión pondrá especial énfasis en las necesidades de **formación**. Como es bien sabido, la evolución tecnológica obliga a actualizar constantemente los conocimientos de las autoridades judiciales y policiales en materia de ciberdelincuencia, razón por la se ha previsto aumentar la cuantía y mejorar la coordinación de la ayuda financiera proporcionada por la UE a programas de formación multinacionales. Asimismo, la Comisión, en estrecha colaboración con los Estados miembros y otros órganos competentes (Europol, Eurojust, Escuela Europea de Policía, Red Europea de Formación Judicial, etc.), velará por coordinar y vincular a escala de la UE todos los programas de formación pertinentes.

La Comisión organizará en 2007 una **reunión** de expertos de las autoridades policiales y judiciales de los Estados miembros, Europol, la Escuela Europea de Policía y la Red Europea de Formación Judicial, para estudiar cómo mejorar la cooperación estratégica y operativa y la formación en materia de ciberdelincuencia en Europa. Entre las cuestiones tratadas figurará la creación, a escala de la UE, de un punto de contacto permanente para el intercambio de información y de una plataforma de formación en materia de ciberdelincuencia. La reunión de 2007 será la primera de una serie de encuentros previstos en el futuro próximo.

3.2. Consolidar el diálogo con la industria

Tanto el sector privado como el sector público tienen interés en colaborar en la elaboración de métodos de detección y prevención de los daños causados por las actividades delictivas. La intervención conjunta de los sectores público y privado, basada en la confianza mutua y en un mismo objetivo —reducir los daños— promete ser un medio eficaz para aumentar la seguridad, en particular en el marco de la lucha contra la ciberdelincuencia. Con el tiempo, las dimensiones pública y privada de la política de la Comisión en materia de ciberdelincuencia se integrarán en la política global planificada por la UE relativa al diálogo entre ambos sectores, que abarcará todos los aspectos de la seguridad europea. Esta política será impulsada en especial por el Foro Europeo de Investigación e Innovación en materia de Seguridad, que la Comisión tiene previsto crear próximamente y en el que participarán las partes interesadas de los sectores público y privado.

La evolución de las tecnologías de la información y los sistemas de comunicaciones electrónicos modernos está en gran medida controlada por operadores privados. Empresas privadas evalúan las amenazas, establecen programas de lucha contra la delincuencia y elaboran soluciones técnicas de prevención. La industria ha mostrado gran diligencia en ayudar a las autoridades públicas a combatir la ciberdelincuencia, en particular por lo que se refiere a la lucha contra la pornografía infantil[17] y otros tipos de contenido ilícitos en internet.

Otra cuestión se refiere a la aparente falta de intercambio de información, competencias especializadas y buenas prácticas entre los sectores público y privado. A menudo, en aras de la protección de modelos y secretos empresariales, los operadores privados se muestran reacios —o la legislación no les obliga claramente— a comunicar a las autoridades policiales y judiciales información pertinente sobre la incidencia de los delitos. Ahora bien, estos datos pueden ser indispensables para que las autoridades públicas puedan elaborar una política de lucha contra la criminalidad eficaz y adecuada. Las posibilidades de mejorar los intercambios de información intersectoriales se analizarán también a la luz de las normas vigentes en materia de protección de los datos personales.

La Comisión desempeña ya un papel importante en distintas estructuras de lucha contra la ciberdelincuencia que agrupan a los sectores público y privado, como el Grupo de Expertos en materia de Prevención del Fraude[18]. Está persuadida de que una política general eficaz de lucha contra la ciberdelincuencia debe también incluir una estrategia de cooperación entre los operadores de los sectores público y privado, incluidas las organizaciones de la sociedad civil.

Para ampliar la cooperación entre los sectores público y privado en este ámbito, en 2007 la Comisión organizará una conferencia destinada a especialistas de los servicios policiales y judiciales y representantes del sector privado, especialmente proveedores de servicios de internet, para estudiar cómo mejorar la cooperación operativa entre ambos sectores en Europa[19]. En ella se abordarán todos los temas que se considera aportan valor añadido para ambos sectores, en particular las siguientes medidas:

- Mejorar la cooperación operativa en la lucha contra las actividades y los contenidos ilícitos en internet, en concreto en el ámbito del terrorismo, el material de abuso sexual de menores y otras actividades ilegales especialmente problemáticas desde la perspectiva de la protección de la infancia.

- Iniciar acuerdos entre los sectores público y privado, con el objetivo de bloquear, a escala de la UE, los sitios que contienen contenidos ilícitos, en particular, imágenes de abuso sexual de menores.

- Concebir un modelo europeo para el intercambio de la información necesaria y pertinente entre los sectores público y privado, cultivando al mismo tiempo un clima de confianza mutua y teniendo en cuenta los intereses de todas las partes.

---

17 Un ejemplo reciente de cooperación en este ámbito es la colaboración entre los servicios represivos y las sociedades emisoras de tarjetas de crédito, en el marco de la cual éstas han ayudado a la policía a localizar a los compradores de pornografía infantil en línea.

18 Véase http://ec.europa.eu/internal_market/payments/fraud/index_en.htm

19 La conferencia podría ser considerada la prolongación del Foro de la UE presentado en la sección 6.4 de la Comunicación relativa a la ciberdelincuencia.

- Constituir una red de puntos de contacto policiales y judiciales tanto en el sector privado como en el sector público.

3.3. Legislación

Una armonización general de las definiciones de los delitos y las legislaciones penales nacionales en el ámbito de la ciberdelincuencia todavía no es conveniente, debido a la diversidad de los tipos de infracciones que abarca este concepto. Dado que la eficacia de la cooperación entre las autoridades policiales y judiciales depende a menudo de disponer de definiciones de las infracciones al menos parcialmente armonizadas, la continuación de la aproximación de las legislaciones de los Estados miembros sigue constituyendo un objetivo a largo plazo[20]. Con la Decisión marco relativa a los ataques contra los sistemas de información se ha dado ya un paso importante en lo tocante a algunas definiciones de delitos clave. Como se ha descrito en los apartados anteriores, posteriormente han ido apareciendo nuevas amenazas, y la Comisión sigue atentamente esta evolución, dada la importancia de valorar constantemente la necesidad de legislación adicional. La vigilancia de estas amenazas, que van variando sin cesar, es objeto de estrecha coordinación con el Programa Europeo de Protección de las Infraestructuras Críticas.

Conviene, no obstante, contemplar desde ahora la adopción de legislación específica de lucha contra la ciberdelincuencia. Un problema concreto que podría requerir la aprobación de legislación se refiere a los delitos informáticos cometidos en el marco de una **usurpación de identidad**. En general, por «usurpación de identidad» se entiende la utilización de datos de identificación personales, por ejemplo un número de tarjeta de crédito, para cometer otros delitos. En la mayoría de los Estados miembros, más que por la usurpación de identidad, el responsable será probablemente procesado por el fraude o los demás delitos que cometa, puesto que el fraude se considera una infracción más grave. En sí, la usurpación de identidad todavía no constituye delito en todos los Estados miembros. A menudo es más fácil probar este delito que el de fraude, de modo que la cooperación policial y judicial a escala de la UE se vería facilitada si la usurpación de identidad se tipificara como delito en todos los Estados miembros. En 2007, la Comisión emprenderá consultas para determinar la conveniencia de legislar al respecto.

3.4. Elaboración de estadísticas

En general se admite que la información relativa a la frecuencia de los delitos es claramente insuficiente y que conviene, en particular, mejorarla sensiblemente para poder proceder a comparaciones de datos entre los Estados miembros. En la Comunicación de la Comisión de 7 de agosto de 2006 titulada «*Desarrollo de una estrategia global y coherente de la UE para evaluar la delincuencia y la justicia penal: Plan de acción de la UE 2006 - 2010*[21]» se exponía un ambicioso plan quinquenal para solucionar este problema. El Grupo de Expertos instituido en el marco de este Plan constituiría un foro adecuado para elaborar indicadores pertinentes que permitan apreciar la amplitud de la ciberdelincuencia.

---

[20] Este objetivo a largo plazo ya se mencionaba en la página 3 de la Comunicación de 2001.

[21] COM(2006) 437, 7.8.2006.

4. CAMINO A SEGUIR

La Comisión se propone profundizar la política general de lucha contra la ciberdelincuencia. Vista la limitación de las competencias de que ésta dispone en el ámbito del Derecho penal, esta política no podrá sino complementar las medidas adoptadas por los Estados miembros y otras instancias. Las medidas más importantes —cada una de las cuales conllevará la utilización de uno, varios o todos los instrumentos presentados en el capítulo 3— recibirán también apoyo a través del programa de financiación sobre prevención y lucha contra la delincuencia.

4.1. Lucha contra la ciberdelincuencia en general

- Establecer una cooperación operativa reforzada entre las autoridades policiales y judiciales de los Estados miembros. Esta acción comenzará por la organización de una reunión específica de expertos en 2007 y podría incluir la instauración de un punto de contacto central de la UE en materia de ciberdelincuencia.

- Aumentar el apoyo financiero concedido a las iniciativas destinadas a mejorar la formación de las autoridades policiales y judiciales en materia de tratamiento de los casos de ciberdelincuencia y adoptar medidas para coordinar todas las iniciativas de formación multinacionales en este ámbito mediante la creación de una plataforma de formación de la UE.

- Animar a los Estados miembros y a todas las autoridades públicas a implicarse en mayor medida en la adopción de medidas eficaces contra la ciberdelincuencia y la asignación de recursos suficientes para la lucha contra este fenómeno.

- Apoyar la investigación que contribuya a la lucha contra la ciberdelincuencia.

- Organizar al menos una gran conferencia (en 2007) en la que participen las autoridades policiales y judiciales y los operadores privados, con el fin de emprender la cooperación en el ámbito de la lucha contra las ciberactividades ilícitas realizadas en las redes electrónicas y contra tales redes, promover un intercambio más eficaz de datos no personales y dar seguimiento a las conclusiones de dicha conferencia de 2007 con proyectos concretos de cooperación entre los sectores público y privado.

- Tomar la iniciativa y participar en acciones que asocien a los sectores público y privado y se centren en la sensibilización de la población, en especial los consumidores, sobre los costes y peligros que entraña la ciberdelincuencia, evitando al mismo tiempo minar la confianza de consumidores y usuarios centrándose únicamente en los aspectos negativos en relación con la seguridad.

- Participar activamente y fomentar una cooperación internacional global en materia de lucha contra la ciberdelincuencia.

- Iniciar, contribuir y proporcionar apoyo a proyectos internacionales acordes con la política de la Comisión en este ámbito, por ejemplo los desarrollados por el G8 que sean coherentes con los documentos de estrategia regional o nacional (en materia de cooperación con terceros países).

- Adoptar medidas concretas para animar a todos los Estados miembros y terceros países pertinentes a ratificar tanto el Convenio del Consejo de Europa sobre la Ciberdelincuencia como su Protocolo adicional, y examinar la posibilidad que la Comunidad devenga Parte del Convenio.

- Analizar, junto con los Estados miembros, el fenómeno de los ataques coordinados masivos contra las infraestructuras informáticas de los Estados miembros, con el fin de prevenirlos y luchar contra ellos, incluidas respuestas coordinadas e intercambio de información y buenas prácticas.

4.2. Lucha contra la delincuencia tradicional en las redes electrónicas

- Emprender un análisis detallado con vistas a la elaboración de una propuesta de normativa específica de la UE contra la usurpación de identidad.

- Promover el desarrollo de métodos y procedimientos técnicos para combatir el fraude y el comercio ilícito en internet, incluso mediante proyectos de cooperación de los sectores público y privado.

- Proseguir y profundizar la labor realizada en ámbitos específicos seleccionados, por ejemplo en el Grupo de Expertos en materia de Prevención del Fraude en lo tocante a la lucha contra el fraude con medios de pago distintos del efectivo en las redes electrónicas.

4.3. Contenidos ilícitos

- Seguir elaborando medidas de lucha contra contenidos ilícitos específicos, en especial los que se refieren al abuso sexual de menores o la apología del terrorismo, en particular mediante el seguimiento de la aplicación de la Decisión marco relativa a la lucha contra la explotación sexual de los niños y la pornografía infantil.

- Instar a los Estados miembros a asignar recursos financieros suficientes para intensificar la labor de los servicios policiales y judiciales, en especial las medidas de identificación de las víctimas de abusos sexuales que puedan aparecer en material gráfico distribuido en línea.

- Poner en marcha y apoyar medidas de lucha contra los contenidos ilícitos que puedan incitar a los menores a adoptar comportamientos violentos u otros comportamientos ilícitos graves, en particular algunos tipos de videojuegos extremadamente violentos accesibles en línea.

- Iniciar y promover el diálogo entre los Estados miembros y con terceros países sobre las técnicas de lucha contra los contenidos ilícitos y sobre los procedimientos de cierre de sitios web ilegales, en concreto para la posible elaboración de acuerdos formales en la materia con países limítrofes y otros países.

- Elaborar acuerdos y convenios voluntarios en la UE, entre las autoridades públicas y los operadores privados, sobre todo proveedores de servicios de internet, relativos a los procedimientos de bloqueo y cierre de los sitios de internet ilegales.

4.4. Seguimiento

La Comisión impulsará la serie de medidas de próxima aplicación que se describen en la presente Comunicación, destinadas a mejorar las estructuras de cooperación en la UE, evaluará los avances realizados en la ejecución de las actividades correspondientes e informará al Consejo y al Parlamento.