COMISIÓN DE LAS COMUNIDADES EUROPEAS

Bruselas, 26.1.2001
COM(2000) 890 final

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

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

Resumen

La transición de Europa a la sociedad de la información se está caracterizando por grandes progresos en todos los aspectos de la vida humana: el trabajo, la educación y el ocio, el gobierno, la industria y el comercio. Las nuevas tecnologías de información y comunicación están teniendo un impacto revolucionario y fundamental en nuestras economías y sociedades. El éxito de la sociedad de la información es importante para el crecimiento, la competitividad y las posibilidades de empleo de Europa, y tiene repercusiones económicas, sociales y jurídicas de gran envergadura.

En diciembre de 1999, la Comisión puso en marcha la iniciativa *e*Europa, con el fin de garantizar que Europa se beneficie de las tecnologías digitales, y que la nueva sociedad de la información sea socialmente inclusiva. En junio de 2000, el Consejo Europeo de Feira adoptó el Plan de acción *e*Europa, y solicitó que se aplicase antes de finales de 2002. El plan de acción resalta la importancia de la seguridad de las redes y de la lucha contra la delincuencia informática.

Las infraestructuras de información y comunicación se han convertido en una parte crucial de nuestras economías. Desafortunadamente, estas infraestructuras tienen sus propias vulnerabilidades y ofrecen nuevas oportunidades para la delincuencia. Estas actividades delictivas pueden adoptar una gran variedad de formas y pueden cruzar muchas fronteras. Aunque, por diversas razones, no existen estadísticas fiables, no cabe duda de que estos delitos constituyen una amenaza para la inversión y los activos del sector, así como para la seguridad y la confianza en la sociedad de la información. Ejemplos recientes de denegación de servicio y ataques de virus han causado grandes perjuicios financieros.

Puede actuarse tanto en términos de prevención de la actividad delictiva, aumentando la seguridad de las infraestructuras de información, como garantizando que las autoridades responsables de la aplicación de ley cuenten con los medios adecuados para intervenir, respetando plenamente los derechos fundamentales de los individuos.

La Unión Europea ha tomado ya diversas medidas para luchar contra los contenidos ilícitos y nocivos en Internet, para proteger la propiedad intelectual y los datos personales, para promover el comercio electrónico y el uso de la firma electrónica y para aumentar la seguridad de las transacciones. En abril de 1998, la Comisión presentó al Consejo los resultados de un estudio sobre la delincuencia informática (el llamado estudio 'COMCRIME'). En octubre de 1999, la cumbre de Tampere del Consejo Europeo concluyó que la labor para acordar definiciones y sanciones comunes debe incluir la delincuencia de alta tecnología. El Parlamento Europeo también ha hecho un llamamiento para que se establezcan definiciones comúnmente aceptables de los delitos informáticos y se aproximen las legislaciones, en especial en el ámbito del derecho penal. El Consejo de la Unión Europea ha adoptado una posición común respecto a las negociaciones del Convenio del Consejo de Europa sobre delincuencia en el ciberespacio y ha adoptado varios elementos iniciales como parte de la estrategia de la Unión contra la delincuencia de alta tecnología. Algunos Estados miembros de la UE también han estado en la vanguardia de las actividades del G8 a este respecto.

La presente Comunicación trata la necesidad y las posibles formas de una iniciativa política amplia en el contexto de los objetivos más amplios de la *sociedad de la información* y de la *libertad, seguridad y justicia*, con el fin de mejorar la seguridad de las infraestructuras de información y luchar contra la delincuencia informática, de acuerdo con el compromiso de la Unión Europea de respetar los derechos humanos fundamentales.

A corto plazo, la Comisión opina que existe una clara necesidad de un instrumento de la UE que garantice que los Estados miembros dispongan de sanciones efectivas para luchar contra la pornografía infantil en Internet. La Comisión presentará a finales de este año una propuesta de decisión marco que, en un contexto más amplio que abarcará cuestiones asociadas con la explotación sexual de los niños y el tráfico de seres humanos, incluirá disposiciones para la aproximación de leyes y sanciones.

A más largo plazo, la Comisión presentará propuestas legislativas para seguir aproximando el derecho penal sustantivo en el ámbito de la delincuencia de alta tecnología. De acuerdo con las conclusiones del Consejo Europeo de Tampere de octubre de 1999, la Comisión considerará asimismo las opciones del reconocimiento mutuo de los autos anteriores al juicio, asociados con las investigaciones de delitos informáticos.

Paralelamente, la Comisión se propone promover la creación, donde no exista, de unidades de policía especializadas en delincuencia informática a escala nacional; apoyar la formación técnica pertinente para la aplicación de la ley; y fomentar las acciones europeas tendentes a la seguridad de la información.

En el plano técnico, y en línea con el marco jurídico, la Comisión promoverá la I+D para comprender y reducir los puntos vulnerables, y estimulará la difusión de conocimientos técnicos.

La Comisión se propone también crear un foro comunitario que reúna a los organismos competentes, a los proveedores de servicios de Internet, a los operadores de telecomunicaciones, a las organizaciones de libertades civiles, a los representantes de los consumidores, a las autoridades responsables de la protección de datos y a otras partes interesadas, con el objetivo de aumentar la comprensión y la cooperación mutuas a escala de la UE. El foro intentará aumentar la conciencia pública de los riesgos que presentan los delincuentes en Internet, promover las mejores prácticas para la seguridad, determinar instrumentos y procedimientos eficaces para luchar contra la delincuencia informática y fomentar el desarrollo futuro de mecanismos de detección temprana y gestión de crisis.

INVITACIÓN PARA REALIZAR COMENTARIOS SOBRE ESTA COMUNICACIÓN

La Comisión Europea desea invitar a las partes interesadas a que realicen comentarios sobre las cuestiones que se abordan en la presente Comunicación. Los comentarios podrán enviarse hasta el 23.03.2001, por correo electrónico, a la siguiente dirección:

infso-jai-cybercrime-comments@cec.eu.int

En principio, los comentarios se publicarán en Internet, a menos que un autor solicite expresamente que no se publique su comentario. Los comentarios anónimos no se publicarán. La Comisión se reserva el derecho a no publicar comentarios recibidos (p. ej., si contienen lenguaje ofensivo). Podrá accederse a los comentarios por medio de un enlace, en la siguiente dirección:

http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/crime1.html

En este sitio web se encontrarán sugerencias relativas al formato técnico y detalles de la política de publicaciones. Es conveniente comprobar el sitio antes de enviar cualquier comentario.

AUDIENCIA PÚBLICA

La Comisión Europea también organizará una audiencia pública para las partes interesadas, sobre las cuestiones que se abordan en la presente Comunicación. Esta audiencia se celebrará el 07.03.2001. Las peticiones de invitaciones para presentar declaraciones en esta audiencia podrán enviarse hasta el 20.02.2001 por correo electrónico, a la siguiente dirección:

infso-jai-cybercrime-hearing@cec.eu.int

O por correo, a la siguiente dirección:

Comisión Europea
Despacho BU33-5/9
200 Wetstraat/Rue de la Loi
B-1049 Bruselas
Bélgica

La Comisión Europea se reserva el derecho de efectuar una selección de las partes que serán oídas. La selección se basará en el número de peticiones y en el deseo de contar con una amplia cobertura de intereses.

ÍNDICE

1. OPORTUNIDADES Y AMENAZAS EN LA SOCIEDAD DE LA INFORMACIÓN

Nuestra era se caracteriza por una creciente asequibilidad y uso de las tecnologías de la sociedad de la información (TSI) y por la globalización de la economía. El desarrollo tecnológico y el mayor uso de redes abiertas, como Internet, en los próximos años, proporcionarán oportunidades nuevas e importantes y plantearán nuevos desafíos.

En la cumbre de Lisboa de marzo de 2000, el Consejo Europeo subrayó la importancia de la transición a una economía competitiva, dinámica y basada en el conocimiento, e invitó al Consejo y a la Comisión a elaborar el Plan de Acción *e*Europa para aprovechar al máximo esta oportunidad[1]. Este plan de acción, elaborado por la Comisión y el Consejo y adoptado por la cumbre del Consejo Europeo de Feira en junio de 2000, comprende acciones para aumentar la seguridad de la red y establecer un enfoque coordinado y coherente de la delincuencia informática para finales de 2002[2].

La infraestructura de la información se ha convertido en una parte vital del eje de nuestras economías. Los usuarios deberían poder confiar en la disponibilidad de los servicios informativos y tener la seguridad de que sus comunicaciones y sus datos están protegidos frente al acceso o la modificación no autorizados. El desarrollo del comercio electrónico y la realización completa de la sociedad de la información dependen de ello.

El uso de las nuevas tecnologías digitales y de la telefonía inalámbrica ya se ha generalizado. Estas tecnologías nos brindan la libertad para poder movernos y permanecer comunicados y conectados con miles de servicios construidos sobre redes de redes. Nos dan la posibilidad de participar; de enseñar y aprender, de jugar y trabajar juntos, y de intervenir en el proceso político. A medida que las sociedades dependen cada vez más de estas tecnologías, será necesario utilizar medios jurídicos y prácticos eficaces para gestionar los riesgos asociados.

Las tecnologías de la sociedad de la información pueden utilizarse, y se utilizan, para perpetrar y facilitar diversas actividades delictivas. En manos de personas que actúan de mala fe, con mala voluntad, o con negligencia grave, estas tecnologías pueden convertirse en instrumentos para actividades que ponen en peligro o atentan contra la vida, la propiedad o la dignidad de los individuos o del interés público.

El enfoque clásico de la seguridad exige una compartimentación organizativa, geográfica y estructural estricta de la información, según su sensibilidad y su categoría. Esto no es ya prácticamente posible en la práctica en el mundo digital, puesto que el tratamiento de la información se distribuye, se prestan servicios a usuarios móviles, y la interoperabilidad de los sistemas es una condición básica. Los enfoques tradicionales de la seguridad son sustituidos por soluciones innovadoras basadas en las nuevas tecnologías. Estas soluciones implican el uso del cifrado y las firmas digitales, de nuevos instrumentos de autenticación y de control del acceso, y de filtros de software de todo tipo[3]. Garantizar infraestructuras de información seguras y fiables no sólo exige la aplicación de diversas tecnologías, sino

---

1 Conclusiones de la Presidencia del Consejo Europeo de Lisboa de 23 y 24 de marzo de 2000, disponible en http://ue.eu.int/en/Info/eurocouncil/index.htm.

2 http://europa.eu.int/comm/information_society/eeurope/actionplan/index_en.htm.

3 Los flujos de información se filtran y se controlan en todos niveles; desde el cortafuego que examina los paquetes de datos, a través del filtro que busca software dañino, el filtro de correo electrónico que elimina discretamente los mensajes publicitarios no solicitados (spam), hasta el filtro del navegador que impide el acceso a material nocivo.

también su correcto despliegue y su uso efectivo. Algunas de estas tecnologías existen ya, pero a menudo los usuarios no son conscientes de su existencia, de la manera de utilizarlas, o de las razones por las que pueden ser necesarias.

1.1. Respuestas nacionales e internacionales

La delincuencia informática se comete en el ciberespacio, y no se detiene en las fronteras nacionales convencionales. En principio, puede perpetrarse desde cualquier lugar y contra cualquier usuario de ordenador del mundo. Se necesita una acción eficaz, tanto a nivel nacional como internacional, para luchar contra la delincuencia informática[4].

A escala nacional, en muchos casos no hay respuestas globales y con vocación internacional frente a los nuevos retos de la seguridad de la red y la delincuencia informática. En la mayoría de los países, las reacciones frente a la delincuencia informática se centran en el derecho nacional (especialmente el derecho penal), descuidando medidas alternativas de prevención.

A pesar de los esfuerzos de las organizaciones internacionales y supranacionales, las diversas leyes nacionales de todo el mundo ponen de manifiesto considerables diferencias, especialmente en las disposiciones del derecho penal sobre piratería informática, protección del secreto comercial y contenidos ilícitos. También existen considerables diferencias en cuanto al poder coercitivo de los organismos investigadores (especialmente por lo que respecta a los datos cifrados y a las investigaciones en redes internacionales), la jurisdicción en materia penal, y con respecto a la responsabilidad de los proveedores de servicios intermediarios por una parte y los proveedores de contenidos por otra. La Directiva 2000/31/CE[5] sobre el comercio electrónico modifica esto por lo que se refiere a la responsabilidad de los proveedores de servicios intermediarios sobre determinadas actividades intermediarias. Asimismo, la Directiva prohibe a los Estados miembros imponer a los proveedores de servicios intermediarios una obligación general de supervisar los datos que transmitan o almacenen.

A escala internacional y supranacional, se ha reconocido ampliamente la necesidad de luchar eficazmente contra la delincuencia informática, y diversas organizaciones han coordinado o han intentado armonizar actividades al respecto. Los Ministros de Justicia y de Interior del G8 adoptaron en diciembre de 1997 un conjunto de principios y un plan de acción de 10 puntos, que fue aprobado por la Cumbre del G8 en Birmingham en junio de 1998 y que se está aplicando en la actualidad[6]. El Consejo de Europa comenzó a elaborar un convenio internacional sobre la delincuencia cibernética en febrero de 1997 y se espera que acabe esta tarea en 2001[7]. La lucha contra la delincuencia cibernética también figura en el orden del día

---

4 Véase, por ejemplo, el Plan de Acción *e*-Europa en la dirección siguiente: http://europa.eu.int/comm/information_society/eeurope/actionplan/index_en.htm, y las declaraciones del Comisario europeo Antõnio Vitorino en: http://europa.eu.int/comm/commissioners/vitorino/speeches/2000/septembre/2000-19-09-en_brussels.pdf, y del Primer Ministro francés Lionel Jospin en: http://www.france.diplomatie.fr/actual/evenements/cybercrim/jospin.gb.html.

5 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 (Directiva sobre el comercio electrónico).

6 El Consejo JAI de la UE de 19 de marzo de 1998 aprobó los 10 principios para combatir la delincuencia de alta tecnología adoptados por el G8, e invitó a los Estados miembros de la UE no pertenecientes al G8 a unirse a la red. Disponible en el sitio de la Red Judicial Europea http://ue.eu.int/ejn/index.htm.

7 El proyecto de texto está disponible en Internet, en dos lenguas: francés: http://conventions.coe.int/treaty/fr/projets/delincuencia cibernética.htm.

de las discusiones bilaterales que la Comisión Europea celebra con algunos gobiernos (de fuera de la UE). Se ha creado un grupo de trabajo conjunto CE/EE.UU. sobre protección de infraestructuras críticas[8].

La ONU y la OCDE también han estado activas en este ámbito, y se está discutiendo en foros internacionales como el Diálogo Empresarial Global y el Diálogo Empresarial Transatlántico[9].

Hasta hace poco, la acción legislativa en la Unión Europea ha adoptado básicamente la forma de medidas en los ámbitos de los derechos de autor, la protección del derecho fundamental a la intimidad y la protección de datos, los servicios de acceso condicional, el comercio electrónico, la firma electrónica y en especial la liberalización del comercio de productos de cifrado, que están relacionados de forma indirecta con la delincuencia informática.

También se han adoptado varias medidas no legislativas importantes en los últimos 3 o 4 años. Entre éstas figuran el plan de acción contra los contenidos ilícitos y nocivos en Internet, que cofinancia acciones de concienciación, experimentos de clasificación y filtrado de contenidos y líneas directas, e iniciativas relativas a la protección de menores y de la dignidad humana en la sociedad de la información, la pornografía infantil y la interceptación legal de las comunicaciones[10]. La UE ha apoyado durante mucho tiempo proyectos I+D tendentes a promover la seguridad y la confianza en infraestructuras de información y transacciones electrónicas, y recientemente ha aumentado la dotación del presupuesto del programa asociado TSI. También se han apoyado proyectos operativos y de investigación dirigidos a promover la formación especializada de las autoridades competentes, así como la cooperación entre estas autoridades y el sector en cuestión, en el marco de programas del tercer pilar tales como STOP, FALCONE, OISIN y GROTIUS[11].

---

e inglés: http://conventions.coe.int/treaty/en/projets/delincuencia cibernética.htm.

8 Bajo los auspicios del grupo consultivo conjunto del Acuerdo de cooperación científica y tecnológica celebrado entre la UE y EE.UU.

9 Naciones Unidas elaboró un "Manual sobre la prevención y el control de la delincuencia informática", que se ha actualizado recientemente. En 1983, la OCDE inició un estudio sobre la posibilidad de aplicar a escala internacional y armonizar los derechos penales para abordar el problema del abuso informático o de la delincuencia informática. En 1986, publicó el informe "Delincuencia informática: Análisis de las medidas jurídicas", donde se examinaban las leyes y propuestas existentes para la reforma en varios Estados miembros y se recomendaba una lista mínima de abusos que los países deberían prohibir y penalizar con leyes penales. Finalmente, en 1992, la OCDE elaboró un conjunto de directrices para la seguridad de los sistemas de información, que deberían en principio proporcionar una base sobre la cual los Estados y el sector privado pudieran construir un marco para la seguridad de los sistemas de información.

10 Recomendación 98/560/CE del Consejo de 24 de septiembre de 1998 relativa al desarrollo de la competitividad de la industria europea de servicios audiovisuales y de información mediante la promoción de marcos nacionales destinados a lograr un nivel de protección comparable y efectivo de los menores y de la dignidad humana;
Libro Verde sobre la protección de los menores y de la dignidad humana en los nuevos servicios audiovisuales y de información; COM (96) 483, octubre de 1996, , http://europa.eu.int/en/record/green/gp9610/protec.htm;
Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones - Contenidos ilícitos y nocivos en Internet (COM (96) 487 final);
Resolución sobre la Comunicación de la Comisión sobre contenidos ilícitos y nocivos en Internet (COM(96)487 - C4-0592/96);
Resolución del Consejo de 17 de enero de 1995 sobre la interceptación legal de las telecomunicaciones (DO C 329 de 04.11.1996, pág. 1-6).

11 http://europa.eu.int/comm/justice_home/jai/prog_en.htm.

El plan de acción para luchar contra la delincuencia organizada, adoptado por el Consejo JAI en mayo de 1997 y aprobado por el Consejo Europeo de Amsterdam, incluía una petición para que la Comisión elaborase, para finales de 1998, un estudio sobre la delincuencia informática. Este estudio, llamado 'estudio COMCRIME', fue presentado por la Comisión al grupo de trabajo multidisciplinar del Consejo contra la delincuencia organizada en abril de 1998[12]. La presente Comunicación es en parte una respuesta a la petición del Consejo JAI.

Antes de elaborar esta Comunicación, la Comisión consideró apropiado realizar consultas informales con representantes de las autoridades competentes de los Estados miembros y de las autoridades de control de la protección de datos[13], así como de la industria europea (especialmente PSI y operadores de telecomunicaciones)[14].

Basándose en los análisis y las recomendaciones del estudio, las conclusiones extraídas de la consulta, las nuevas posibilidades previstas por el Tratado de Amsterdam y los trabajos ya realizados en la UE, el G8 y el Consejo de Europa, la presente Comunicación examinará diversas opciones para nuevas medidas de la UE contra la delincuencia informática. En la Unión Europea, las soluciones elegidas no deberían obstaculizar ni dar lugar a la fragmentación del mercado interior, ni a medidas que socaven la protección de los derechos fundamentales[15].

2. SEGURIDAD DE LAS INFRAESTRUCTURAS DE INFORMACIÓN

En la sociedad de la información, las redes globales controladas por los usuarios están sustituyendo gradualmente a la generación más antigua de redes nacionales de comunicaciones. Una de las razones del éxito de Internet es que ha proporcionado a los usuarios acceso a las tecnologías más vanguardistas. Según la ley de Moore[16], la capacidad informática se duplica cada 18 meses; pero la tecnología de las comunicaciones se está desarrollando a un ritmo incluso más rápido[17]. Esto supone que el volumen de datos transportados por Internet se ha estado duplicando en periodos inferiores a un año.

---

12 "Aspectos jurídicos de la delincuencia informática en la sociedad de la información - COMCRIME". El estudio fue elaborado por el profesor U. Sieber de la Universidad de Würzburg, en virtud de un contrato con la Comisión Europea. El informe final está disponible en: http://www2.echo.lu/legal/en/crime/crime.html.

13 En la UE, las autoridades de control de la protección de datos componen el Grupo de protección de las personas en lo que respecta al tratamiento de datos personales, que es el organismo consultivo independiente de la UE sobre protección de datos y de la intimidad. Véanse los art. 29 y 30 de la Directiva 95/46/CE.

14 Se celebraron dos reuniones con las autoridades competentes el 10.12.99 y 1.3.2000. El 13.3.2000 tuvo lugar una reunión con los representantes de la industria de Internet. El 31.3.2000 tuvo lugar una reunión con un pequeño número de expertos en protección de datos personales. El 17.4.2000 tuvo lugar una reunión final con todos los anteriormente mencionados. Las actas de las reuniones pueden solicitarse por escrito a: Comisión Europea, Unidad INFSO/A5, o a: Comisión Europea, Unidad JAI/B2, Wetstraat/Rue de la Loi 200, 1049 Bruselas, Bélgica.

15 Carta de los Derechos Fundamentales de la UE (http://europa.eu.int/comm/justice_home/unit/charte_en.htm), Artículo 6 del TUE y jurisprudencia del Tribunal de Justicia de las Comunidades Europeas.

16 Observación realizada en 1965 por Gordon Moore, cofundador de Intel, sobre la velocidad a la que crecía la densidad de los transistores en circuitos integrados. Actualmente, esta densidad se está prácticamente duplicando cada 18 meses, lo que tiene un impacto directo en el precio y el rendimiento de los microprocesadores de ordenador. Muchos expertos opinan que esto se mantendrá al menos durante otra década.

17 La tecnología más avanzada permite a un solo cable de fibra óptica transportar simultáneamente el equivalente a 100 millones de llamadas de voz.

Las redes telefónicas clásicas fueron construidas y gestionadas por organizaciones nacionales. Sus usuarios tenían poca opción en cuanto a servicios y ningún control sobre el medio. Las primeras redes de datos que se desarrollaron se construyeron con la misma filosofía de un medio con control centralizado, lo que se vio reflejado en la seguridad de estos medios.

Internet y otras redes nuevas son muy diferentes, y la seguridad ha de gestionarse en consecuencia. La inteligencia y el control en estas redes se da sobre todo en la periferia, donde se encuentran los usuarios y los servicios. El núcleo de la red es sencillo y eficaz, y esencialmente se dedica a transmitir datos. Apenas se verifican o controlan los contenidos. Únicamente en el destino final los bits se convierten en una voz, la imagen de una radiografía o la confirmación de una transacción bancaria. La seguridad es por tanto, en gran medida, responsabilidad de los usuarios, pues sólo ellos pueden apreciar el valor de los bits enviados o recibidos, y pueden determinar el nivel de protección necesario.

El medio de los usuarios es por tanto una parte esencial de la infraestructura de la información. En él hay que aplicar las técnicas de seguridad, con el permiso y la participación de los usuarios y de acuerdo con sus necesidades. Esto es particularmente importante si se considera la creciente gama de actividades que los usuarios realizan desde el mismo terminal. Trabajan y juegan, ven la televisión y autorizan transferencias bancarias, todo ello desde el mismo instrumento.

Existen diversas tecnologías de seguridad, y se están desarrollando otras nuevas. Las ventajas del desarrollo de las fuentes de información de acceso público en términos de seguridad se están poniendo de manifiesto. Se ha trabajado mucho en métodos formales y en criterios de evaluación de la seguridad. El uso de las tecnologías de cifrado y de firma electrónica se están haciendo imprescindibles, particularmente con el desarrollo de los accesos por telefonía inalámbrica. Cada vez se necesita una mayor variedad de mecanismos de autenticación para cubrir nuestras necesidades en el medio donde actuamos. En algunos medios, podemos necesitar o querer permanecer en el anonimato. En otros, podemos necesitar demostrar una característica determinada, sin revelar nuestra identidad, tal como ser adulto o empleado o cliente de una empresa concreta. En otras situaciones, puede ser necesario demostrar nuestra identidad. También los filtros de software son cada vez más sofisticados, y nos permiten protegernos o proteger a los nuestros de datos no deseados, como por ejemplo contenidos nocivos, mensajes publicitarios no solicitados (spam), programas informáticos perjudiciales y otras formas de ataque. La aplicación y la gestión de estos requisitos de seguridad en Internet y en las nuevas redes supone asimismo un considerable gasto para el sector y los usuarios. Por tanto, es importante fomentar la innovación y el uso comercial de los servicios y tecnologías de seguridad.

Naturalmente, también la infraestructura compartida de enlaces de comunicación y servidores de nombre tiene sus aspectos de seguridad. La transmisión de datos depende de las conexiones físicas por donde se transportan los datos de un ordenador a otro. Estas conexiones han de establecerse y protegerse de forma que la transmisión siga siendo posible a pesar de los accidentes, de los ataques y de un volumen cada vez mayor de tráfico. La comunicación también depende de servicios críticos como los proporcionados por los servidores de nombre, y en especial del pequeño número de servidores de nombre de primer nivel, que proporcionan las direcciones necesarias. Cada uno de estos componentes también necesitará una protección adecuada, que variará en función de la parte del espacio nominal y de la base de usuarios a que sirva.

Con el objetivo de aportar una mayor flexibilidad y respuesta a las necesidades de las personas, las tecnologías de infraestructura de la información se han vuelto cada vez más complejas, y a menudo no se han dedicado los suficientes esfuerzos a la seguridad. Además, esta complejidad supone la aplicación de programas informáticos cada vez más sofisticados e interconectados, lo que a veces da lugar a deficiencias y lagunas en la seguridad, que pueden aprovecharse fácilmente para atacar. A medida que el ciberespacio gana en complejidad y sus componentes en sofisticación, pueden surgir vulnerabilidades nuevas y no previstas.

Ya existen varios mecanismos tecnológicos, y se están desarrollando otros destinados a mejorar la seguridad en el ciberespacio. La respuesta incluye medidas destinadas a:

- Asegurar los elementos críticos de la infraestructura, mediante la utilización de infraestructuras públicas clave, el desarrollo de protocolos de seguridad, etc.

- Asegurar los medios privados y públicos mediante el desarrollo de software de calidad, cortafuegos, programas antivirus, sistemas electrónicos de gestión de los derechos, cifrado, etc.

- Asegurar la autenticación de los usuarios autorizados, la utilización de tarjetas inteligentes, la identificación biométrica, las firmas electrónicas, las tecnologías de roles, etc.

Todo esto exige un mayor esfuerzo para desarrollar tecnologías de seguridad, utilizando la cooperación con el fin de lograr la interoperabilidad necesaria entre las soluciones, mediante acuerdos sobre normas internacionales.

También es importante que los futuros marcos conceptuales sobre seguridad formen parte de la arquitectura global, abordando las amenazas y las vulnerabilidades desde el inicio del proceso de diseño. Esto contrasta con los enfoques tradicionales acumulativos, que han intentado necesariamente ir llenando las lagunas explotadas por una comunidad delictiva cada vez más sofisticada.

El Programa de Tecnologías de la Sociedad de la Información de la UE (TSI)[18], en especial los trabajos relativos a la información, la seguridad de la red, y otras tecnologías dirigidas a crear seguridad[19], proporcionan un marco para desarrollar la capacidad y la tecnología para comprender y abordar nuevos retos relacionados con la delincuencia informática. Estas tecnologías incluyen herramientas técnicas para la protección contra la violación de los derechos fundamentales a la intimidad y los datos personales y otros derechos personales, y para la lucha contra la delincuencia informática. Además, en el contexto del Programa TSI, se ha puesto en marcha una iniciativa de seguridad. Esta iniciativa contribuirá a la seguridad y a la confianza en infraestructuras de información muy interconectadas y en sistemas de alta integración en redes, promoviendo la toma de conciencia respecto a la seguridad y las tecnologías que proporcionan seguridad. Parte integrante de esta iniciativa es la cooperación internacional. El Programa TSI ha desarrollado relaciones de trabajo con la Agencia de Proyectos de Investigación Avanzada para la Defensa (DARPA) y la Fundación Nacional para la Ciencia (NSF), y ha establecido, en colaboración con el Departamento de Estado de

---

[18] El programa TSI lo gestiona la Comisión Europea. Forma parte del 5º Programa Marco 1998-2002. Para más información, consúltese http://www.cordis.lu/ist.

[19] En la Acción clave 2 - Nuevos métodos de trabajo y comercio electrónico.

EE.UU., un grupo de trabajo conjunto CE/EE.UU. sobre protección de infraestructuras críticas[20].

Por último, el establecimiento de obligaciones relativas a la seguridad, derivadas en particular de las Directivas comunitarias sobre protección de datos[21], contribuye a mejorar la seguridad de las redes y del procesamiento de datos.

3. DELINCUENCIA INFORMÁTICA

Los sistemas modernos de información y comunicación permiten realizar actividades ilegales desde cualquier parte del mundo en cualquier momento. No existen estadísticas fiables sobre la magnitud del fenómeno de la delincuencia informática. El número de intrusiones detectadas y comunicadas hasta ahora, probablemente subestima la dimensión del problema. Debido a la limitada experiencia y conocimientos de los administradores y usuarios de sistemas, muchas intrusiones no se detectan. Además, muchas empresas no están dispuestas a comunicar los casos de abuso informático, para evitar la publicidad negativa y la exposición a ataques futuros. Muchos servicios de policía no mantienen estadísticas sobre el uso de ordenadores y sistemas de comunicación utilizados en estos y otros delitos. Sin embargo, se puede esperar que el número de actividades ilegales crezca a medida que aumenta el uso de ordenadores y redes. Existe una clara necesidad de reunir pruebas fiables sobre la importancia de la delincuencia informática.

En esta Comunicación se aborda la delincuencia informática en el sentido más amplio; cualquier delito que de alguna manera implique el uso de tecnología de la información. Sin embargo, existen distintos puntos de vista sobre lo que constituye la "delincuencia informática". Suelen utilizarse indistintamente los términos "delincuencia informática", "delincuencia relacionada con la informática", "delincuencia de alta tecnología" y "delincuencia cibernética". Cabe diferenciar entre los delitos informáticos específicos y los delitos tradicionales perpetrados con ayuda de la informática. Un ejemplo típico se encuentra en el ámbito aduanero, donde Internet se utiliza como instrumento para cometer delitos típicos contra la normativa de aduanas, tales como el contrabando, la falsificación, etc. Mientras que los delitos informáticos específicos requieren una actualización de las definiciones de los delitos en los códigos penales nacionales, los delitos tradicionales perpetrados con ayuda de la informática requieren una mejora de la cooperación y de las medidas procesales.

Sin embargo, todos ellos se benefician de la disponibilidad de las redes de información y comunicación sin fronteras y de la circulación de datos, intangible y sumamente volátil. Estas características exigen una revisión de las actuales medidas dirigidas a abordar las actividades ilegales realizadas en estas redes y sistemas o utilizando los mismos.

Muchos países han adoptado legislación dirigida a abordar la delincuencia informática. En los Estados miembros de la Unión Europea, se han establecido varios instrumentos jurídicos. Aparte de una Decisión del Consejo sobre pornografía infantil en Internet, por ahora no existen instrumentos jurídicos de la UE que aborden directamente la delincuencia informática, pero sí existen diversos instrumentos jurídicos que tratan indirectamente la cuestión.

---

[20] Bajo los auspicios del Grupo consultivo conjunto del Acuerdo de cooperación científica y tecnológica firmado entre la UE y EE.UU.

[21] Véase el artículo 4 de la Directiva 97/66/CE (que incluye también la obligación de informar acerca de los riesgos para la seguridad) y el artículo 17 de la Directiva 95/46/CE.

Las principales cuestiones que trata la legislación relativa a los delitos informáticos específicos, en la UE o en los Estados miembros, son las siguientes:

Delitos contra la intimidad: Varios países han introducido disposiciones penales sobre recogida, almacenamiento, modificación, revelación o difusión ilegales de datos personales. En la Unión Europea, se han adoptado dos Directivas para la aproximación de las normas nacionales sobre protección de la intimidad por lo que se refiere al tratamiento de datos personales[22]. El artículo 24 de la Directiva 95/46/CE obliga claramente a los Estados miembros a adoptar las medidas adecuadas para garantizar la plena aplicación de las disposiciones de la misma y a determinar, en particular, las sanciones que deben aplicarse en caso de incumplimiento de las disposiciones de las leyes nacionales. Los derechos fundamentales a la intimidad y la protección de datos se incluyen, además, en la Carta de los Derechos Fundamentales de la Unión Europea.

Delitos relativos al contenido: La difusión, especialmente por Internet, de pornografía, y en especial de pornografía infantil, las declaraciones racistas y la información que incita a la violencia plantea la cuestión de hasta qué grado estos actos pueden combatirse con ayuda del derecho penal. La Comisión apoya la opinión de que lo que es ilegal fuera del mundo de la informática también lo es en éste. El autor o el proveedor de contenidos[23] puede ser responsable en virtud del derecho penal. Se ha adoptado una Decisión del Consejo para luchar contra la pornografía infantil en Internet[24].

La responsabilidad de los proveedores de servicios intermediarios, cuyas redes o servidores se utilizan para la transmisión o el almacenamiento de información de terceros, se aborda en la Directiva sobre el comercio electrónico.

Delitos económicos, acceso no autorizado y sabotaje: Muchos países han aprobado leyes que abordan los delitos económicos perpetrados por ordenador y tipifican nuevos delitos relacionados con el acceso no autorizado a sistemas informáticos (por ejemplo, la piratería, el sabotaje informático y la distribución de virus, el espionaje informático, y la falsificación y el fraude informáticos[25]) y nuevas formas de cometer delitos (por ejemplo, manipulación de un ordenador en vez de engañar a una persona). El objeto del delito suele ser intangible, por ejemplo, dinero en depósitos bancarios o programas de ordenador. Actualmente, no existen instrumentos comunitarios que contemplen estos tipos de actividad ilegal. Por lo que respecta

---

22 Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y Directiva 97/66/CE del Parlamento Europeo y del Consejo de 15 de diciembre de 1997 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones. El artículo 24 de la Directiva 95/46/CE obliga a los Estados miembros a determinar las sanciones que deben aplicarse en caso de incumplimiento de las disposiciones sobre protección de datos.

23 El proveedor de contenidos no deberá confundirse con el proveedor de servicios.

24 Decisión del Consejo, de 29 de mayo de 2000, relativa a la lucha contra la pornografía infantil en Internet (DO L 138 de 9.6.2000, p.1).

25 Los medios de comunicación han prestado mucha atención a los recientes ataques de "denegación de servicio" en grandes sitios de Internet y a la distribución del llamado virus LoveBug. No obstante, esto debe mantenerse en perspectiva. Los ataques de denegación de servicio, deliberados o accidentales, y los virus relacionados con el correo electrónico existen desde hace muchos años. El gusano de Morris y el mensaje electrónico del árbol de Navidad de IBM son ejemplos anteriores. Existen productos y procedimientos para abordarlos. Hay también mucha cooperación positiva en la comunidad de Internet para limitar el daño producido por dichos incidentes, a medida que suceden. Existe una cooperación similar para limitar los abusos del spam.

a la prevención, el recientemente adoptado Reglamento sobre bienes de doble uso ha contribuido considerablemente a liberalizar la disponibilidad de productos de cifrado.

Delitos contra la propiedad intelectual: Se han adoptado dos Directivas, sobre la protección jurídica de programas de ordenador y sobre la protección jurídica de las bases de datos[26], directamente relacionadas con la sociedad de la información y que determinan sanciones. El Consejo ha adoptado una posición común sobre una propuesta de Directiva relativa a los derechos de autor y derechos afines en la sociedad de la información, y se espera que se adopte a principios de 2001[27]. La violación de los derechos de autor y derechos afines debe sancionarse, al igual que la elusión de las medidas tecnológicas diseñadas para proteger estos derechos. Por lo que se refiere a la falsificación y a la piratería, la Comisión presentará, antes de finales de 2000, una comunicación que examinará el proceso de consulta iniciado con su Libro Verde de 1998 y que anunciará un plan de acción pertinente. A medida que Internet crece en importancia desde el punto de vista comercial, están surgiendo nuevos conflictos en torno a nombres de dominio, relacionados con la ciberocupación, el acaparamiento y el secuestro de nombre de dominio, lo que, naturalmente, exige normas y procedimientos para abordar estos problemas[28].

También es necesario abordar la ejecución de las obligaciones fiscales. En el caso de transacciones comerciales en que el receptor del suministro en línea de un servicio electrónico esté ubicado en la UE, en la mayoría de los casos surgirán obligaciones fiscales en la jurisdicción donde se realiza tal servicio[29]. El incumplimiento de las obligaciones fiscales expone a los operadores a sanciones civiles (y en algunos casos penales), que pueden incluir el embargo de cuentas bancarias o de otros bienes. Si bien el cumplimiento voluntario es siempre la mejor opción, en último caso dichas obligaciones han de hacerse cumplir. La cooperación entre las administraciones fiscales es un elemento clave para lograr este objetivo.

Al posibilitar la protección de las transacciones legales, se proporciona a los delincuentes los mismos medios para proteger sus transacciones ilegales. Los instrumentos que protegen el comercio electrónico también pueden utilizarse para apoyar el tráfico de drogas. Será necesario establecer prioridades y tomar opciones.

La protección de las víctimas frente a la delincuencia informática exige asimismo cubrir aspectos de responsabilidad, reparación y compensación, que surgen cuando se cometen delitos informáticos. La confianza no depende sólo del uso de la tecnología adecuada, sino también de las garantías económicas y jurídicas adjuntas. Estas cuestiones deberán examinarse respecto de todos los delitos informáticos.

---

[26] Directiva 91/250/CEE del Consejo, de 14 de mayo de 1991, sobre la protección jurídica de programas de ordenador (DO L 122 de 17.5.1991, pág. 42 - 46).
Directiva 96/9/CE del Parlamento Europeo y del Consejo, de 11 de marzo de 1996, sobre la protección jurídica de las bases de datos (DO L 77 de 27.3.1996, pág. 20 - 28).

[27] Posición común adoptada por el Consejo con vistas a la adopción de una Directiva del Parlamento Europeo y del Consejo relativa a la armonización de determinados aspectos de los derechos de autor y derechos afines en la sociedad de la información (CS/2000/9512).

[28] Comunicación de la Comisión al Consejo y al Parlamento Europeo - La organización y gestión de Internet - Cuestiones de política europea e internacional 1998 - 2000, abril de 2000, COM (2000) 202.

[29] La Comisión ha propuesto una serie de enmiendas al sistema de IVA de la UE, con el fin de clarificar la jurisdicción sobre las obligaciones fiscales (COM (2000) 349 - Propuesta de directiva del Consejo por la que se modifica la Directiva 77/388/CEE respecto del régimen del impuesto sobre el valor añadido aplicable a algunos servicios prestados por vía electrónica), que se está estudiando actualmente en el Consejo y en el Parlamento. No obstante, en algunas circunstancias, la obligación de pago puede corresponder al proveedor, incluso aunque éste no esté presente físicamente en la jurisdicción fiscal.

Se necesitan instrumentos jurídicos sustantivos y procesales eficaces aproximados a escala mundial, o al menos europea, para proteger a las víctimas de la delincuencia informática y para llevar a los autores ante la Justicia. Al mismo tiempo, las comunicaciones personales, la protección de datos y de la intimidad, y el acceso y la difusión de la información, son derechos fundamentales en las democracias modernas. Por ello es necesario contar con la disponibilidad y el uso de medidas eficaces de prevención, para reducir la necesidad de aplicar medidas de ejecución. Cualquier medida legislativa que pueda resultar necesaria para abordar la delincuencia informática ha de alcanzar un equilibrio entre estos importantes intereses.

4. CUESTIONES DE DERECHO SUSTANTIVO

La aproximación del derecho sustantivo en el ámbito de la delincuencia de alta tecnología garantizará un nivel mínimo de protección para las víctimas de la delincuencia informática (por ejemplo, las víctimas de la pornografía infantil), contribuirá al cumplimiento del requisito de que una actividad debe constituir delito en ambos países para que pueda prestarse asistencia jurídica mutua en una investigación penal (requisito de doble tipicidad), y aportará mayor claridad al sector (por ejemplo, respecto a lo que constituyen contenidos ilícitos).

De hecho, a raíz de la Cumbre de Tampere del Consejo Europeo en octubre de 1999, se ha introducido en la agenda de la UE un instrumento legislativo comunitario para aproximar el derecho penal sustantivo en el ámbito de la delincuencia informática[30]. La Cumbre incluyó la delincuencia de alta tecnología en una lista limitada de ámbitos en los que deben concentrarse esfuerzos para acordar definiciones, tipificaciones y sanciones comunes. Esto se incluye en la recomendación 7 de la estrategia de la Unión Europea para el nuevo milenio sobre prevención y control de la delincuencia organizada, adoptada por el Consejo JAI en marzo de 2000[31]. Forma también parte del programa del trabajo de la Comisión para el año 2000 y del Marcador para la creación de un espacio de libertad, seguridad y justicia, elaborado por la Comisión y adoptado por el Consejo de Justicia e Interior el 27 de marzo de 2000[32].

La Comisión ha seguido el trabajo del Consejo de Europa relativo al Convenio sobre la delincuencia en el ciberespacio. En el actual proyecto de Convenio del Consejo de Europa sobre delincuencia cibernética figuran cuatro categorías de delitos: 1) delitos contra la confidencialidad, la integridad y la disponibilidad de los sistemas y datos informáticos; 2) delitos informáticos; 3) delitos relativos al contenido; y 4) delitos relativos a la violación de los derechos de autor y derechos afines.

La aproximación de la UE podría ir más lejos que el Convenio del Consejo de Europa, que representará una aproximación mínima a escala internacional. Esta armonización podría ser operativa en un plazo más corto que la entrada en vigor del Convenio del Consejo de Europa[33]. Introduciría el delito informático en el ámbito del derecho comunitario e introduciría mecanismos jurídicos de la UE.

---

30 http://db.consilium.eu.int/en/Info/eurocouncil/index.htm.

31 Prevención y control de la delincuencia organizada - Estrategia de la Unión Europea para el comienzo del nuevo milenio (DO 2000 C124, 3.5.2000).

32 http://europa.eu.int/comm/dgs/justice_home/index_en.htm.

33 La entrada en vigor del Convenio del CdE no se producirá hasta después de la ratificación.

La Comisión otorga una gran importancia a garantizar que la Unión Europea pueda tomar medidas efectivas, en especial contra la pornografía infantil en Internet. La Comisión acoge con satisfacción la Decisión del Consejo para luchar contra la pornografía infantil en Internet, pero comparte la opinión del Parlamento Europeo de que se requieren nuevas medidas para aproximar las leyes nacionales. La Comisión se propone introducir a finales de este año una propuesta de decisión marco del Consejo que incluya disposiciones para la aproximación de leyes y sanciones sobre pornografía infantil en Internet[34].

De acuerdo con las conclusiones de Tampere, la Comisión presentará una propuesta legislativa en virtud del Título VI del TUE, con el fin de aproximar los delitos de alta tecnología. Esta medida aprovechará los progresos realizados en el Consejo de Europa y abordará, en particular, la necesidad de aproximar la legislación relativa a la piratería y la denegación de servicio. La propuesta incluirá definiciones estándar para la Unión Europea en este ámbito. Esto podría ir más allá que el proyecto de Convenio del Consejo de Europa, garantizando que los casos graves de piratería y de denegación de servicio sean castigados con una pena mínima en todos los Estados miembros.

Además, la Comisión examinará el alcance de las medidas contra el racismo y la xenofobia en Internet, con vistas a presentar una propuesta para una decisión marco del Consejo, en virtud del Título VI del TUE, que cubra las actividades racistas y xenófobas en línea y fuera de línea. Para ello, se tendrá en cuenta la próxima evaluación de la aplicación por los Estados miembros de la acción común de 15 de julio de 1996 sobre medidas para luchar contra el racismo y la xenofobia[35]. La acción común constituyó un primer paso hacia la aproximación de los delitos relativos al racismo y la xenofobia, pero es necesaria una mayor aproximación en la Unión Europea. La importancia y sensibilidad de esta cuestión se subrayaron en la decisión del un tribunal francés de 20 de noviembre de 2000, en la que se exigía a Yahoo que bloquease a los usuarios franceses el acceso a sitios de venta de recuerdos nazis[36].

Por último, la Comisión estudiará cómo mejorar la eficacia de los esfuerzos contra el comercio ilícito de drogas en Internet, cuya importancia se reconoce en la estrategia de la Unión Europea contra las drogas 2000-2004, aprobada en el Consejo Europeo de Helsinki[37].

5. CUESTIONES DE DERECHO PROCESAL

La propia naturaleza de los delitos informáticos acerca a un primer plano de la atención nacional e internacional las cuestiones procesales, debido a la intervención de distintas soberanías, jurisdicciones y normativas. Más que en cualquier otro delito transnacional, la velocidad, movilidad y flexibilidad del delito informático suponen un reto a las actuales normas de derecho procesal penal.

---

34 Esta iniciativa formará parte de un paquete de propuestas que cubrirá también cuestiones más amplias asociadas con la explotación sexual de los niños y la trata de seres humanos, según se anunció en la Comunicación de la Comisión sobre la trata de seres humanos de diciembre de 1998.

35 DO L 185, 24/07/1996, P0005-0007. También disponible en el sitio web de la Red Judicial Europea http://ue.eu.int/ejn/index.htm.

36 Tribunal De Grande Instance de Paris, Ordonnance de Référé rendue le 20 November 2000, No. RG 00/05308.

37 Plan de acción de la Unión Europea en materia de lucha contra la droga (2000 – 2004). COM(1999)239 final. http://europa.eu.int/comm/justice_home/unit/drogue_en.htm

La aproximación de las competencias previstas por el derecho procesal mejorará la protección de las víctimas, al garantizar que los servicios responsables de la aplicación de la ley cuentan con los poderes necesarios para investigar delitos en su propio territorio, y garantizará que estos servicios puedan responder rápida y eficazmente a las peticiones de cooperación de otros países.

También es importante garantizar que las medidas adoptadas en virtud del derecho penal, que suelen ser competencia de los Estados miembros y del Título VI del TUE, cumplen los requisitos del derecho comunitario. En particular, el Tribunal de Justicia ha mantenido reiteradamente que tales disposiciones legislativas no podrán suponer una discriminación contra las personas a las que el derecho comunitario confiere el derecho a la igualdad de trato, ni restringir las libertades fundamentales garantizadas por el derecho comunitario[38]. Toda nueva competencia que se defina para los servicios responsables de la aplicación de la ley deberá evaluarse a la vista del derecho comunitario y de su impacto en la intimidad.

5.1. Interceptación de las comunicaciones

En la Unión Europea, existe un principio general de confidencialidad de las comunicaciones (y de los correspondientes datos sobre tráfico). Las interceptaciones son ilegales a menos que estén autorizadas por ley, cuando sea necesario en casos específicos para objetivos concretos. Esto se desprende del artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos, mencionado en el artículo 6 del TUE, y más concretamente de las Directivas 95/46/CE y 97/66/CE.

Todos los Estados miembros tienen un marco jurídico que permite a las autoridades competentes obtener mandatos judiciales (o, en caso de dos Estados miembros, mandatos autorizados personalmente por un Ministro) para interceptar comunicaciones en la red pública de telecomunicaciones[39]. Esta legislación, que debe ser acorde con el derecho comunitario en la medida en que éste contenga disposiciones al respecto, contiene salvaguardias que protegen el derecho fundamental de los individuos a la intimidad, tales como la limitación del uso de la interceptación a las investigaciones sobre delitos graves, la exigencia de que la interceptación en investigaciones individuales sea necesaria y proporcionada, y la garantía de que los individuos sean informados acerca de la interceptación tan pronto como ello deje de obstaculizar la investigación. En muchos Estados miembros, la legislación sobre interceptación contiene obligaciones para los operadores de telecomunicaciones (de servicio público) de establecer posibilidades de interceptación. Una Resolución del Consejo de 1995 coordina los requisitos de la interceptación[40].

---

38 Asunto C-274/96 Bickel & Franz (1998) REC I-7637 ap.17, Asunto C-186/87 Cowan (1989) REC 195 ap. 19. En particular, las sanciones o medidas administrativas no deberán exceder de lo estrictamente necesario, los procedimientos de control no deberán concebirse de forma que restrinjan la libertad requerida por el Tratado, y no deberán ir acompañados de sanciones que sean tan desproporcionadas con la gravedad de la infracción que suponga un obstáculo para el ejercicio de dicha libertad (Asunto C-203/80 Casati (1981) REC 2595 ap.27).

39 Dos Estados miembros no admiten las comunicaciones interceptadas como prueba en los procedimientos penales.

40 Resolución del Consejo de 17 de enero de 1995 sobre la interceptación legal de las telecomunicaciones (DO C 329 de 4.11.1996, pág. 1-6). El anexo contiene una lista de los requisitos que deben cumplir las autoridades competentes para interceptar legalmente las telecomunicaciones, que los Estados miembros hubieron de tener en cuenta en la definición y puesta en práctica de las medidas y políticas nacionales pertinentes. En 1998, la Presidencia austríaca propuso una resolución del Consejo de la UE para ampliar el ámbito de la resolución de 1995, con el fin de cubrir las nuevas tecnologías, incluidos Internet y las comunicaciones vía satélite. Esto ha sido objeto de debate en dos comisiones del Parlamento Europeo,

Los operadores tradicionales de redes, en especial los que ofrecen servicios de voz, establecieron en el pasado relaciones de trabajo con las autoridades competentes, con el fin de facilitar la interceptación legal de las comunicaciones. La liberalización de las telecomunicaciones y el auge del uso de Internet han atraído al mercado a muchos nuevos participantes, que han debido hacer frente a los requisitos para la interceptación. Será necesario debatir sobre normativas, viabilidad técnica, asignación de costes e impacto comercial en los diálogos entre el gobierno y el sector, junto con las demás partes involucradas, incluidas las autoridades de control de la protección de datos.

Las nuevas tecnologías exigen que los Estados miembros trabajen juntos si desean mantener sus capacidades para la interceptación legal de las comunicaciones. En caso de que los Estados miembros introduzcan nuevos requisitos técnicos sobre interceptación para los operadores de telecomunicaciones y los proveedores de servicios de Internet, la Comisión opina que estas normas deberán coordinarse a escala internacional para prevenir la distorsión del mercado único, minimizar los costes para el sector y respetar los requisitos de protección de los datos y de la intimidad. Las normas deberán ser públicas y abiertas siempre que sea posible y no deberán introducir debilidades en la infraestructura de las comunicaciones.

En el contexto del Convenio sobre asistencia judicial en materia penal[41], se ha acordado un enfoque para facilitar la cooperación en materia de interceptación legal[42]. El Convenio contiene disposiciones sobre interceptación de las comunicaciones telefónicas vía satélite[43], y sobre interceptación de comunicaciones de una persona en el territorio de otro Estado miembro[44]. La Comisión opina que las normas sobre interceptación del Convenio sobre asistencia judicial en materia penal constituyen el grado máximo posible en la fase actual. El texto del Convenio es tecnológicamente neutro; habrá que probar cómo funciona en la práctica antes de que puedan estudiarse mejoras. La Comisión revisará su aplicación con los Estados miembros, el sector, los usuarios y las autoridades de control de la protección de

---

la Comisión de Libertades Públicas y Asuntos de Interior y la Comisión de Asuntos Jurídicos y de Derechos de los Ciudadanos, que llegaron a distintas conclusiones. La primera consideró que esta resolución era una aclaración y una actualización de la antigua, y la consideró aceptable. La segunda fue muy crítica, tanto respecto a las posibles violaciones de los derechos humanos como a los costes de los operadores, y rechazó la propuesta del Consejo de la UE e invitó a la Comisión a elaborar una nueva propuesta una vez que el Tratado de Amsterdam entrase en vigor. Ni el Consejo ni sus grupos de trabajo han tenido en cuenta activamente en los últimos meses el proyecto de resolución del Consejo.

41 DO C 197 de 12.7.2000, p.1. El Convenio fue adoptado el 29 de mayo de 2000. Las disposiciones sobre interceptación del Convenio se aplican solamente a los Estados miembros de la Unión Europea y no a los terceros países.

42 El Convenio prevé salvaguardas mínimas por lo que respecta a la protección de la intimidad y de los datos personales.

43 El propósito inicial de las negociaciones era proporcionar una capacidad de interceptación con respecto a las personas que utilizan teléfonos vía satélite, en el territorio del Estado miembro que realiza la interceptación. Técnicamente, el punto crítico para interceptar estas comunicaciones se encuentra en la estación del satélite en tierra. Era por tanto necesario contar con la asistencia técnica del Estado miembro donde estaba situada la estación en tierra. El Convenio contiene dos opciones para esta cuestión: un procedimiento de asistencia legal mutua acelerado que exige solicitudes individuales de asistencia al Estado miembro donde se halla situada la estación del satélite en tierra, y una solución técnica basada en el acceso a distancia a la estación del satélite en tierra desde el Estado miembro que realiza la interceptación, que no requiere solicitudes individuales.

44 El Convenio también prevé un marco jurídico para las solicitudes de interceptación de las comunicaciones de una persona en el territorio de otro Estado miembro (el Estado miembro requerido). En este caso, tanto el Estado miembro de interceptación como el Estado miembro requerido necesitan obtener mandatos de interceptación en virtud de sus leyes nacionales. Por último, el Convenio establece normas para los casos en que el Estado miembro que realiza la interceptación pueda tener la posibilidad de interceptar las comunicaciones de una persona en el territorio de otro Estado miembro sin necesidad de solicitar la asistencia técnica de dicho Estado miembro.

datos para asegurarse de que las iniciativas pertinentes son eficaces, transparentes y equilibradas.

El uso abusivo e indiscriminado de la capacidad de interceptación, sobre todo a escala internacional, planteará problemas de derechos humanos y socavará la confianza de los ciudadanos en la sociedad de la información. La Comisión ha recibido con preocupación informes sobre supuestos abusos de la capacidad de interceptación[45].

5.2. Retención de datos sobre tráfico

Para investigar y procesar delitos que implican el uso de las redes de comunicaciones, incluida Internet, las autoridades competentes utilizan frecuentemente los datos sobre tráfico cuando éstos son almacenados por los proveedores de servicios a efectos de la facturación. Como el precio de las comunicaciones depende cada vez menos de la distancia y del destino, los proveedores de servicios tienden a facturar tarifas planas, y ya no habrá necesidad de almacenar datos sobre tráfico para la facturación. Las autoridades competentes temen que esto suponga una reducción del material para investigaciones penales, y por tanto abogan por que los proveedores de servicios conserven algunos datos sobre tráfico por lo menos durante un período de tiempo mínimo, a fin de que puedan utilizarse a efectos de la aplicación de la ley[46].

De conformidad con las Directivas de la UE sobre protección de datos personales, tanto los principios generales limitadores de la Directiva 95/46/CE como las disposiciones más específicas de la Directiva 97/66/CE, los datos sobre tráfico deberán destruirse o hacerse anónimos en cuanto termine el servicio de telecomunicación, a menos que sean necesarios a efectos de facturación. En los casos de tarifa plana o de acceso gratuito a los servicios de telecomunicaciones, no se permite en principio a los proveedores de servicios conservar los datos sobre tráfico.

Conforme a las Directivas de la UE sobre protección de datos, los Estados miembros podrán adoptar medidas legales para limitar el alcance de la obligación de destruir los datos sobre tráfico, cuando dichas limitaciones constituyan una medida necesaria para, entre otros, la prevención, la investigación, la detección y la persecución de delitos o la utilización no autorizada del sistema de telecomunicaciones[47].

No obstante, cualquier medida legislativa nacional que pueda prever la retención de datos sobre tráfico a efectos de la aplicación de la ley ha de cumplir determinados requisitos: las medidas propuestas deberán ser adecuadas, necesarias y proporcionadas, de acuerdo con el derecho comunitario y el derecho internacional, así como las Directivas 97/66/CE y 95/46/CE, el Convenio Europeo para la Protección de los Derechos Humanos de 4 de noviembre de 1950 y el Convenio del Consejo de Europa para la protección de las personas en lo que respecta al tratamiento automatizado de los datos personales, de 28 de enero de 1981. Esto es particularmente relevante para las medidas que implican la retención rutinaria de datos sobre gran parte de la población.

---

45 Un amplio informe muy documentado del Sr. Campbell sobre una red de espionaje para la interceptación de comunicaciones llamada ECHELON fue objeto de una audiencia pública del Parlamento Europeo. El informe sostiene que ECHELON fue concebida con fines de seguridad nacional, pero que también se ha utilizado para el espionaje industrial. El Parlamento Europeo ha creado una comisión temporal que estudiará el tema y presentará un informe a la sesión plenaria en el plazo de un año.

46 Aquí se incluirían investigaciones penales en casos no relacionados con las redes informáticas o de comunicaciones, pero donde los datos puedan ayudar a resolver el caso.

47 Artículo 14 de la Directiva 97/66/CE y artículo 13 de la Directiva 95/46/CE.

Algunos Estados miembros están tomando iniciativas legales que requieren o permiten a los proveedores de servicios almacenar algunas categorías de datos sobre tráfico, no necesarias a efectos de facturación, una vez prestado el servicio, pero que se consideran útiles a efectos de investigaciones penales.

El alcance y la forma de estas iniciativas varía considerablemente, pero todas se basan en la idea de que las autoridades competentes deberían disponer de más datos de los que tendrían en caso de que los proveedores de servicios solamente procesasen los datos estrictamente necesarios para la prestación del servicio. La Comisión está examinando estas medidas a la luz del derecho comunitario.

El Parlamento Europeo es sensible a las cuestiones de la intimidad, y se inclina generalmente a favor de una protección fuerte de los datos personales. Sin embargo, en los debates sobre la lucha contra la pornografía infantil en Internet, el Parlamento Europeo se ha expresado en el sentido de favorecer una obligación general de conservar datos sobre tráfico durante un período de tres meses[48].

Esto ilustra la importancia del contexto en el que se discute un tema tan sensible como la retención de los datos sobre tráfico, y el reto para los responsables políticos que intentan buscar un equilibrio adecuado.

La Comisión considera que cualquier solución al complejo problema de la conservación de los datos sobre tráfico deberá tener un buen fundamento, ser proporcionada y lograr un equilibrio justo entre los distintos intereses en juego de las partes implicadas. Sólo un enfoque que aúne los conocimientos y las capacidades del Gobierno, del sector, de las autoridades de control de la protección de datos y de los usuarios, logrará alcanzar estos objetivos. Sería deseable contar con un enfoque coherente en todos los Estados miembros, a fin de alcanzar los objetivos de eficacia y proporcionalidad, y evitar una situación donde tanto las autoridades competentes como la comunidad de Internet tengan que tratar con una diversidad de medios técnicos y jurídicos.

Existen intereses importantes y muy diversos que deben tenerse en cuenta. Por una parte, las autoridades de control de la protección de datos consideran que el medio más eficaz de reducir riesgos inaceptables para la intimidad, reconociendo al mismo tiempo la necesidad de aplicar eficazmente la ley, es que, en principio, los datos sobre tráfico no se conserven solamente a efectos de la aplicación de la ley[49]. Por otra parte, las autoridades competentes han declarado que consideran necesaria la conservación de una cantidad mínima de datos sobre tráfico durante un período de tiempo mínimo necesario para facilitar investigaciones penales.

---

48 Resolución legislativa que contiene el dictamen del Parlamento Europeo sobre el proyecto de Acción común, adoptada por el Consejo en virtud del artículo K.3 del Tratado de la Unión Europea, relativa a la lucha contra la pornografía infantil en Internet, enmienda 17 (DO C 219, 30.7.1999, pág. 68-71).

49 "Es imprescindible prohibir la vigilancia exploratoria o general a gran escala... los medios más eficaces para evitar riesgos inaceptables a la intimidad y reconocer simultáneamente la necesidad de una ejecución eficaz de la ley es que, en principio, los datos sobre tráfico no deberán conservarse a efectos exclusivos de control y que las legislaciones nacionales no deberán obligar a los operadores de telecomunicaciones, proveedores de servicios de telecomunicación y proveedores de servicios Internet a conservar los datos sobre tráfico durante un plazo superior al necesario a efectos de facturación."; Recomendación 3/99 de 7 de septiembre de 1999 del Grupo de protección de las personas en lo que respecta al tratamiento de datos personales, creado en virtud del artículo 29, http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm.

El sector tiene interés en cooperar en la lucha contra delitos tales como la piratería y el fraude informático, pero no debería tener que hacer frente a medidas excesivamente costosas. El impacto económico de las medidas debería analizarse cuidadosamente y compararse con la eficacia de las mismas en la lucha contra la delincuencia informática, con el fin de evitar que el uso de Internet sea más costoso y menos asequible para los usuarios. Habría que garantizar una seguridad adecuada de los datos sobre tráfico conservados.

En cualquier caso, el sector desempeñará una función clave al contribuir al proceso de creación de una sociedad de la información más segura. Los usuarios deberían confiar en la seguridad de la sociedad de la información y sentirse protegidos frente a los delitos y frente a la violación de su intimidad.

La Comisión apoya y fomenta plenamente un diálogo constructivo entre las autoridades competentes, el sector, las autoridades responsables de la protección de datos y las organizaciones de consumidores, así como otras partes interesadas. En el foro propuesto de la UE (véase el punto 6.4 de esta Comunicación), la Comisión exhortará a todas las partes implicadas a discutir a fondo, como cuestión prioritaria, el complejo problema de la conservación de los datos sobre tráfico con vistas a encontrar conjuntamente soluciones apropiadas, equilibradas y proporcionadas que respeten plenamente los derechos fundamentales a la intimidad y a la protección de datos[50]. Basándose en los resultados de este trabajo, la Comisión podrá evaluar la necesidad de acciones legislativas o no legislativas a escala de la UE.

5.3. Acceso y uso anónimos

Las autoridades competentes expertas en la materia han expresado su preocupación por que el anonimato pueda dar lugar a la elusión de la responsabilidad y pueda obstaculizar gravemente la posibilidad de detener a los delincuentes. En algunos países, y en otros no, es posible el uso anónimo de la telefonía móvil mediante tarjetas de prepago. Asimismo, los proveedores de servicios y de acceso, incluidos los reexpedidores de correo y los cibercafés, facilitan el acceso anónimo a Internet. También facilita un cierto anonimato el sistema de adjudicación de direcciones provisionales de Internet, donde no se asignan direcciones a los usuarios de forma permanente, sino sólo para la duración de una sesión determinada.

En sus debates con la Comisión, algunos representantes del sector no se han pronunciado a favor del anonimato total, en parte por su propia seguridad, en aras de la integridad de la red y a efectos de la lucha contra el fraude. La London Internet Exchange mencionó unas directrices sobre buenas prácticas publicadas por ella, que han resultado útiles en el Reino Unido[51]. No obstante, otros representantes del sector y expertos en protección de la intimidad han manifestado que sin el anonimato no es posible garantizar los derechos fundamentales.

El Grupo de trabajo sobre protección de datos del artículo 29 ha publicado una recomendación a propósito del uso anónimo de Internet[52]. Este Grupo considera que la cuestión del anonimato en Internet constituye el núcleo de un problema para los Gobiernos y organizaciones internacionales: por una parte, la posibilidad del anonimato es esencial para

---

50 Según figura en el Convenio Europeo de los Derechos Humanos (artículo 8, derecho a la intimidad), en la Carta de la UE sobre los Derechos Fundamentales, en el Tratado de la UE y en las Directivas comunitarias sobre protección de datos.

51 http://www.linx.net/noncore/bcp/.

52 Grupo de protección de las personas en lo que respecta al tratamiento de datos personales. Recomendación 3/97 Anonimato en Internet. Adoptada por el Grupo el 3 de diciembre de 1997. http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm.

mantener en el ciberespacio los derechos fundamentales de intimidad y libertad de expresión. Por otra parte, la posibilidad de participar y comunicarse en línea sin revelar la identidad va en contra de las numerosas iniciativas que se están desarrollando para apoyar otros ámbitos fundamentales del orden público, tales como la lucha contra los contenidos ilícitos y nocivos, el fraude financiero o las violaciones de los derechos de autor. Por supuesto, tal conflicto aparente entre objetivos distintos de orden público no es nuevo. En el contexto de los más tradicionales medios de comunicación fuera de línea, tales como las cartas y paquetes, el teléfono, los periódicos, o la difusión por radio y televisión, se ha alcanzado un equilibrio entre estos objetivos. El reto a que se enfrentan en la actualidad los responsables políticos es garantizar que este enfoque equilibrado, que garantiza los derechos fundamentales permitiendo al mismo tiempo restricciones proporcionadas a estos derechos en circunstancias limitadas y concretas, se mantenga en el nuevo contexto del ciberespacio. Para este equilibrio será vital el grado y los límites a la capacidad de participación en línea de forma anónima.

En la declaración final de la conferencia ministerial de Bonn sobre redes globales de información, celebrada los días 6-8 de julio de 1997, se estableció que el principio debería ser que, en los casos en que el usuario pueda elegir mantenerse anónimo fuera de la red, esta opción debe también poderse dar en la red. Existe pues un claro consenso acerca de que a la actividad en las redes deberán aplicarse los principios jurídicos básicos que se aplican en otros ámbitos. Internet no es un ghetto anárquico donde no se aplican las normas de la sociedad. Asimismo, la capacidad de los Gobiernos y poderes públicos para restringir los derechos individuales y vigilar los comportamientos potencialmente ilícitos no debería ser mayor en las redes públicas que en el mundo exterior, fuera de la red. El requisito de que las restricciones a los derechos y libertades fundamentales deben ser adecuadamente justificadas, necesarias y proporcionadas a la vista de otros objetivos de orden público, debe también aplicarse en el ciberespacio.

En la recomendación del Grupo sobre protección de datos del artículo 29 se indica detalladamente cómo puede lograrse esto en casos específicos (por ejemplo, con respecto al correo electrónico, a los grupos de noticias, etc.)[53]. La Comisión comparte los puntos de vista del Grupo.

5.4. Cooperación práctica a escala internacional

Últimamente, operaciones policiales combinadas a escala internacional, tales como las operaciones Starburst y Cathedral contra redes de pederastas, han puesto de manifiesto el valor de la acción internacional coordinada a cargo de las autoridades policiales y judiciales competentes, tanto en cuanto a intercambio de información en la fase preliminar como para impedir que se produzcan soplos hacia otros miembros de la red cuando se realizan las detenciones y las incautaciones. Internet también ha resultado un instrumento valioso y eficaz para las investigaciones policiales y aduaneras, cuando se utiliza como instrumento para cometer delitos tradicionales, tales como falsificaciones y contrabando. Por otra parte, estas operaciones también han revelado las grandes dificultades jurídicas y operativas a que se enfrentaron las autoridades policiales y judiciales competentes al gestionar esta acción, tales como la preparación de pruebas transfronterizas o comisiones rogatorias, la identificación de víctimas, y la función de las organizaciones intergubernamentales que tratan cuestiones policiales (básicamente, Interpol y Europol).

---

53 http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm

En el ámbito de las medidas prácticas de cooperación internacional, las redes internacionales para el intercambio de información son cada vez más importantes para las autoridades policiales y aduaneras.

Dentro del G8, se ha creado una red de información permanente de puntos de contacto de las autoridades competentes, que ya está operativa. Su propósito principal es recibir y responder a las solicitudes urgentes de cooperación en casos donde intervengan pruebas electrónicas. La red se ha utilizado con éxito en varios casos. El Consejo JAI de la UE de 19 de marzo de 1998 aprobó los 10 principios para luchar contra la delincuencia de alta tecnología adoptados por el G8, e invitó a los Estados miembros de la UE no pertenecientes al G8 a adherirse a la red[54]. Estos puntos de contacto deberán cooperar directamente, complementando las estructuras existentes de ayuda mutua y de canales de comunicaciones[55].

La creación de esta red también está prevista en el proyecto de Convenio del Consejo de Europa. La referencia a una red permanente de puntos de contacto existe también en la Decisión del Consejo relativa a la lucha contra la pornografía infantil en Internet, en la Posición Común de la UE relativa al proyecto de Convenio del Consejo de Europa sobre delincuencia en el ciberespacio[56] y en la Decisión del Consejo por la que se aprueba el plan de acción del G8[57], pero aún no se han tomado iniciativas concretas específicas para la UE.

La Comisión considera que, dada la necesidad de una experiencia adecuada y una acción acelerada en este ámbito, las intenciones del Consejo deberían ejecutarse sin demora. Sin embargo, para que tal red tenga éxito necesitará personal competente tanto en el plano jurídico como técnico, lo que implica una formación apropiada.

Existe una necesidad similar de intensificar la cooperación y el intercambio de información entre las autoridades aduaneras. Será necesario reforzar las actuales formas de cooperación, y desarrollar nuevos medios para la gestión de las operaciones conjuntas y el intercambio de información. Teniendo en cuenta los requisitos para la protección de datos, existe un creciente consenso entre las autoridades aduaneras en el sentido de que deben crearse redes internacionales de información con objeto de facilitar el intercambio de información. También es necesario invertir mayores recursos en este ámbito, tanto por lo que se refiere a la mejora de los sistemas informáticos como a la formación del personal, a fin de que las autoridades aduaneras puedan cumplir su cometido con mayor eficacia.

5.5. Competencias de derecho procesal y jurisdicción

A escala nacional, y una vez cumplidas las condiciones jurídicas necesarias, las autoridades competentes necesitan poder investigar e incautar datos almacenados en ordenadores con la rapidez suficiente para impedir la destrucción de pruebas delictivas. Las autoridades

---

54 Hasta ahora, aparte de los miembros del G8, cinco Estados miembros de la UE se han adherido a la red permanente del G8.

55 En la Conferencia mundial contra la explotación sexual comercial de los niños, celebrada en Estocolmo el 28 de agosto de 1996, se presentaron propuestas tendentes a incluir a INTERPOL en las redes mencionadas. La Decisión del Consejo de la UE relativa a la lucha contra la pornografía infantil en Internet prevé asimismo la participación de Europol en este ámbito.

56 Artículo 1.4 de la Posición Común: "Los Estados miembros deberán apoyar en la mayor medida posible el establecimiento de disposiciones que faciliten la cooperación internacional, con inclusión de disposiciones relativas a la asistencia judicial. El Convenio habrá de facilitar la cooperación rápida en relación con los delitos cometidos total o parcialmente por medios informáticos. Esta forma de cooperación podrá incluir la creación de puntos de contacto para la aplicación de la ley que funcionen 24 horas al día, que complementarán las estructuras de asistencia judicial existentes."

57 Disponible en el sitio web de la Red Judicial Europea http://ue.eu.int/ejn/index.htm.

competentes consideran que deberían tener suficientes poderes coercitivos, en su jurisdicción, para investigar los sistemas informáticos e incautar datos, ordenar la entrega de datos informáticos concretos, y ordenar u obtener con celeridad la conservación de datos específicos de conformidad con las salvaguardias y procedimientos jurídicos normales. Sin embargo, de momento las salvaguardias y los procedimientos no están aproximados.

Pueden surgir problemas en los casos en que, al acceder a un ordenador, las autoridades competentes encuentren que están implicados varios ordenadores y redes situados por todo el país. La cuestión se complica considerablemente si, mientras se registra un ordenador o simplemente se realiza una investigación, la autoridad competente se encuentra que está accediendo, o que necesita acceder, a datos localizados en uno o más países distintos. Hay en juego importantes intereses en materia de soberanía, derechos humanos y aplicación de la ley, y es necesario equilibrarlos.

Los instrumentos jurídicos existentes para la cooperación internacional en asuntos de derecho penal, tales como la asistencia judicial mutua, pueden no ser apropiados o suficientes, puesto que su aplicación suele tardar varios días, semanas o meses. Se necesita un mecanismo por el cual los países puedan investigar delitos y obtener pruebas de manera rápida y eficaz, o al menos no perder pruebas importantes en los procedimientos transfronterizos de aplicación de la ley, de manera consistente con los principios de soberanía nacional y de derechos humanos y constitucionales, incluida la protección de la intimidad y de los datos.

Entre las nuevas propuestas que se están estudiando en el proyecto de Convenio del Consejo de Europa sobre delincuencia informática con objeto de abordar estos problemas, figuran órdenes para la conservación de datos, a fin de asistir en investigaciones específicas. Sin embargo, otras cuestiones tales como la búsqueda y la incautación transnacionales presentan problemas difíciles y aún no resueltos. Serán necesarios nuevos debates entre las partes interesadas antes de que puedan preverse iniciativas concretas.

El subgrupo sobre delincuencia de alta tecnología del G8 ha discutido largamente la cuestión de la búsqueda y la incautación transnacionales y, anticipándose a un acuerdo posterior más permanente, ha alcanzado un consenso sobre principios provisionales[58]. Las cuestiones importantes, sin embargo, tratan en particular de cuándo es posible la investigación e incautación aceleradas en situaciones especiales, antes de informar al Estado objeto de la investigación, y de la necesidad de establecer salvaguardias adecuadas para el respecto de los derechos fundamentales. En la posición común de la UE relativa al proyecto de Convenio del Consejo de Europa sobre delincuencia en el ciberespacio, los ministros adoptaron una posición abierta[59].

En el caso de los delitos informáticos transfronterizos, es importante que existan normas claras respecto a qué país tiene jurisdicción para el procesamiento. Debe evitarse

---

58 Comunicado de la Conferencia Ministerial de los países del G8 sobre la lucha contra la delincuencia transnacional organizada - Moscú, 19-20 de octubre de 1999 (véase http://www.usdoj.gov/criminal/cybercrime/action.htm y también http://www.usdoj.gov/criminal/cybercrime/principles.htm).

59 DO L 142/2: "Sin perjuicio de los principios constitucionales y de las salvaguardias específicas para respetar adecuadamente la soberanía, seguridad, orden público u otros intereses fundamentales de otros Estados, en casos excepcionales, en particular en situación de urgencia (por ejemplo, en la medida en que resulte necesario para impedir la destrucción o alteración de pruebas de un delito grave o para impedir la comisión de un delito del que pueda seguirse con probabilidad la muerte o una lesión física grave de una persona), podrá estudiarse la posibilidad de una búsqueda informática transfronteriza, a efectos de investigación de un delito penal grave, que se definirá con más detalle en el Convenio."

especialmente el que ningún país tenga jurisdicción. Las principales normas propuestas por el proyecto de Convenio del Consejo de Europa son que la jurisdicción corresponderá a un Estado cuando el delito sea cometido en su territorio o por uno de sus nacionales. Cuando más de un Estado reivindique la jurisdicción, los Estados en cuestión deberán hacer consultas con objeto de determinar la jurisdicción más apropiada. No obstante, mucho dependerá de que se realice efectivamente la consulta bilateral o multilateral. La Comisión seguirá estudiando esta cuestión con objeto de ver si es necesaria cualquier otra acción a escala de la UE.

La Comisión, que ha participado tanto en los debates del Consejo de Europa como del G8, reconoce la complejidad y las dificultades asociadas con las cuestiones de derecho procesal. Pero una cooperación eficaz en la UE para luchar contra la delincuencia cibernética es un elemento esencial para una sociedad de la información más segura y para la creación de un espacio de libertad, seguridad y justicia.

La Comisión se propone continuar sus consultas con todas las partes interesadas durante los próximos meses, con objeto de desarrollar estos trabajos. Esta cuestión también se estudiará en el contexto más amplio del trabajo sobre la aplicación de las conclusiones del Consejo Europeo de Tampere de octubre de 1999. En especial, la Cumbre de Tampere pidió al Consejo y a la Comisión que adoptasen, en diciembre de 2000, un programa de medidas destinado a aplicar el principio de reconocimiento mutuo de resoluciones judiciales. La Comisión ya ha publicado una Comunicación sobre el reconocimiento mutuo de resoluciones firmes en materia penal[60]. Como parte de su contribución a la aplicación de la parte del programa de medidas relativa a la ejecución de los autos anteriores al juicio, la Comisión considerará las opciones para el reconocimiento mutuo de autos anteriores al juicio asociados con investigaciones relativas a la delincuencia cibernética, con vistas a la presentación de una propuesta legislativa en virtud del Título VI del TUE.

5.6. Valor probatorio de los datos informáticos

Incluso en los casos en que las autoridades competentes accedan a datos informáticos que parezcan ser pruebas delictivas, necesitan poder recuperarlos y autenticarlos para poder utilizarlos en investigaciones y procesamientos penales. No es una tarea fácil, dada la naturaleza volátil y la facilidad de manipulación, falsificación, protección tecnológica o eliminación de los datos electrónicos, y la realizan forenses informáticos, desarrollando y utilizando protocolos científicos y procedimientos para investigar ordenadores y para analizar y mantener la autenticidad de los datos recuperados.

A petición de los expertos del G8, la Organización Internacional de Prueba Informática (OIPI) ha acordado elaborar recomendaciones sobre normas, incluida la definición de métodos, técnicas de identificación y términos comunes que deben utilizarse, y el establecimiento de un formato común para las peticiones forenses. La UE debería asociarse a este trabajo, tanto en el nivel de los organismos de investigación de los Estados miembros especializados en delincuencia informática, como a través de la I+D apoyada por el 5º Programa Marco (Programa TSI).

6. MEDIDAS NO LEGISLATIVAS

Se necesita una legislación adecuada tanto a escala nacional como internacional, pero no basta por sí misma para luchar eficazmente contra el uso delictivo de las redes y la delincuencia

---

60 COM (2000) 495, Bruselas 26.7.2000.

informática. Se necesitan también varias condiciones suplementarias no legislativas como complemento a las medidas legislativas. La mayoría se han incluido en las recomendaciones del estudio COMCRIME, el G8 las ha incluido en su plan de acción de 10 puntos, y han recibido un gran apoyo en el proceso informal de consulta que precedió a la elaboración de esta Comunicación. Entre ellas figuran:

- la creación de unidades de policía especializadas en delincuencia informática a escala nacional, en los casos en que aún no existan;

- una mayor cooperación entre las autoridades competentes, el sector, las organizaciones de consumidores y las autoridades responsables de la protección de datos;

- fomentar iniciativas adecuadas dirigidas por el sector y la UE, incluidas iniciativas sobre productos de seguridad.

El problema del cifrado conservará su importancia en este contexto. El cifrado es una herramienta esencial para facilitar la aplicación y la adopción de nuevos servicios, incluido el comercio electrónico, y puede contribuir considerablemente a la prevención de la delincuencia en Internet. La política de la Comisión sobre cifrado se estableció en su Comunicación sobre el fomento de la seguridad y la confianza en la comunicación electrónica de 1997[61], donde la Comisión indica que tratará de suprimir todas las restricciones a la libre circulación de productos de cifrado en la Comunidad Europea. Además, la Comunicación establece que las restricciones nacionales a la libre circulación de productos de cifrado deberán ser compatibles con el derecho comunitario y que examinará si dichas restricciones son justificadas y proporcionadas, especialmente con respecto a las disposiciones del Tratado sobre libre circulación, la jurisprudencia del Tribunal de Justicia y los requisitos de las Directivas sobre protección de datos. Sin embargo, la Comisión reconoce que el cifrado también presenta retos nuevos y difíciles para las autoridades competentes.

La Comisión, por tanto, acoge con satisfacción el reglamento revisado sobre productos de doble uso, recientemente adoptado, que ha contribuido considerablemente a liberalizar la disponibilidad de productos de cifrado, reconociendo al mismo tiempo que ello debe ir acompañado de un mejor diálogo entre los usuarios, el sector y las autoridades competentes. Por su parte, la Comisión se propone fomentar este diálogo a escala de la UE a través del propuesto Foro de la UE. La disponibilidad a escala comunitaria de productos de seguridad, incluidos los productos de cifrado reforzado, certificados en su caso mediante criterios de evaluación acordados, mejoraría las posibilidades de prevención de la delincuencia y la confianza de los usuarios en los procesos de la sociedad de la información.

6.1. Unidades especializadas a escala nacional

Dada la complejidad técnica y jurídica de algunos delitos informáticos, es importante crear unidades especializadas a escala nacional. Tales unidades especializadas, compuestas por personal pluridisciplinar (policial y judicial) y con grandes conocimientos, deberían contar con instalaciones técnicas adecuadas y funcionar como puntos de contacto rápidos con los siguientes fines:

- responder rápidamente a las solicitudes de información sobre presuntos delitos. Será necesario definir formatos comunes para el intercambio de tal información, aunque los

---

61 COM(97)503.

debates de los expertos del G8 han puesto de manifiesto que esto puede no ser tarea fácil, dadas las diferencias entre las culturas jurídicas nacionales;

- actuar como interfaz de las autoridades competentes, nacional e internacionalmente, para las líneas directas[62], recibiendo denuncias de los usuarios de Internet sobre contenidos ilícitos;

- mejorar o desarrollar técnicas especializadas de investigación informática con el fin de detectar, investigar y procesar delitos informáticos;

- actuar como centro de excelencia en cuestiones relacionadas con la delincuencia cibernética, con el fin de compartir experiencias y mejores prácticas.

En la UE, algunos Estados miembros ya han creado estas unidades especializadas que tratan específicamente los delitos informáticos. La Comisión considera que la creación de tales unidades especializadas es una prerrogativa de los Estados miembros y anima a éstos a que tomen medidas en esa dirección. La compra del hardware y software más avanzado para estas unidades, así como la formación del personal, supone grandes costes y presupone prioridades y decisiones políticas en los niveles gubernamentales correspondientes[63]. La experiencia de unidades ya existentes en los Estados miembros puede ser particularmente valiosa. La Comisión fomentará el intercambio de estas experiencias.

La Comisión también opina que Europol puede proporcionar mayor valor añadido a escala de la UE mediante la coordinación, el análisis y otras ayudas a las unidades nacionales especializadas. Por tanto, la Comisión apoyará la ampliación del mandato de Europol para cubrir la delincuencia cibernética.

6.2. Formación especializada

Se requiere un considerable esfuerzo en el ámbito de la formación continua y especializada del personal policial y judicial. Las técnicas y las capacidades de la delincuencia informática evolucionan con más rapidez que las correspondientes a áreas más tradicionales de actividad delictiva.

Algunos Estados miembros han llevado a cabo iniciativas sobre formación en alta tecnología del personal responsable de la aplicación de la ley. Estos Estados podrían proporcionar asesoramiento y orientación a los Estados miembros que aún no han tomado medidas similares.

---

62 Hasta ahora, sólo existen líneas directas en unos pocos países. Los ejemplos son Cybertipline en EE.UU. e Internet Watch Foundation (IWF) en el Reino Unido, que desde diciembre de 1996, gestiona una línea directa de teléfono y de correo electrónico para que el público informe acerca del material encontrado en Internet que consideren ilícito. La IWF juzga si el material es ilícito, informa a los PSI y a la policía. También existen otros organismos de supervisión en Noruega (Redd Barna), Países Bajos (Meldpunt), Alemania (Newswatch, FSM y Jugendschutz), Austria (ISPAA) e Irlanda (ISPAI). En el marco del programa comunitario Daphne, Childnet International ha iniciado recientemente un proyecto relacionado directamente con esta cuestión ("Foro internacional de proveedores de líneas directas en Europa"). La reunión de expertos de la UNESCO en París en enero de 1999 apoya y fomenta también las líneas directas nacionales y la creación de redes de líneas directas, o de una "atalaya electrónica" internacional.

63 Acerca de la experiencia de EE.UU. en esta cuestión, véase Michael A. Sussmann “The Critical Challenges from International High-Tech and Computer-Related Crime at the Millennium”, Duke Journal of Comparative and International Law, Vol. 9 Primavera de 1999, p. 464.

Se han lanzado proyectos individuales tendentes a este fin, en forma de intercambio de experiencias y seminarios sobre los retos comunes a que se enfrentan los profesionales en cuestión, con el apoyo de programas gestionados por la Comisión (en especial STOP, FALCONE y GROTIUS). La Comisión propondrá más actividades en este campo, incluida la formación informática y en línea.

Europol ha tomado la iniciativa de organizar una sesión de formación de una semana para el personal de los Estados miembros responsable de la aplicación de la ley, en noviembre de 2000, con especial referencia al problema de la pornografía infantil. El alcance de la sesión podría ampliarse para incluir la delincuencia informática en general. Interpol también permanece activa en este ámbito desde hace varios años. Sus iniciativas podrían ampliarse para incluir un mayor número de personal.

El G8 ha organizado iniciativas tendentes al intercambio de experiencias entre las autoridades competentes, y al establecimiento de técnicas comunes de investigación, basándose en casos concretos. Se espera que se adopte otra iniciativa en el ámbito de la formación en la segunda mitad de 2001. Los Estados miembros de la UE pertenecientes al G8 podrían compartir estas experiencias con los otros Estados miembros.

En el ámbito específico de la lucha contra la pornografía infantil en Internet, la creación y el mantenimiento de una biblioteca central digital de imágenes de pornografía infantil a escala internacional (que estaría disponible en Internet para las unidades nacionales especializadas de policía, con las condiciones y limitaciones necesarias por lo que respecta al acceso y la protección de la intimidad) ayudaría a la búsqueda de víctimas y delincuentes, y contribuiría a determinar la naturaleza de los delitos y a formar a los funcionarios de policía especializados[64].

6.3. Mejor información y normas comunes sobre mantenimiento de archivos

La creación de un conjunto armonizado de normas sobre mantenimiento de archivos policiales y judiciales, y de instrumentos adecuados para el análisis estadístico de la delincuencia informática, ayudaría a las autoridades policiales y judiciales competentes a almacenar, analizar, y evaluar mejor la información recogida en este área cambiante.

Asimismo, desde el punto de vista del sector privado, estas estadísticas son necesarias para la correcta evaluación de los riesgos y el análisis de costes y beneficios de su gestión. Esto es importante no sólo por razones operativas (como las decisiones acerca de las medidas de seguridad que deben tomarse), sino también a efectos del seguro.

Se está actualizando y haciendo accesible para la Comisión una base de datos sobre el estatuto de la delincuencia informática, que se presentó como parte del estudio COMCRIME. La Comisión estudiará la posibilidad de mejorar el contenido (inclusión de leyes y jurisprudencia) y la utilidad de la base de datos.

---

64 En este contexto, el proyecto "Excalibur", elaborado por la división nacional sueca de inteligencia sobre delincuencia y copatrocinado por la Comisión Europea bajo el programa STOP, ha sido una iniciativa muy acertada. Este proyecto se ha creado con la cooperación de las fuerzas de policía de Alemania, el Reino Unido, los Países Bajos y Bélgica, así como Europol e Interpol. También hay que considerar otros proyectos realizados por el BKA alemán ("Perkeo") y el Ministerio de interior francés (proyecto "Surfimage", también copatrocinado por el programa STOP).

6.4. Cooperación entre los diversos actores: El foro de la UE

La cooperación efectiva entre el Gobierno y el sector dentro del marco jurídico se considera un elemento esencial de toda política destinada a abordar la delincuencia informática[65]. Los representantes de las autoridades competentes han admitido que no han sido siempre suficientemente claros y precisos acerca de lo que necesitan de los proveedores de servicios. Los representantes del sector han expresado una actitud generalmente positiva hacia una mayor cooperación con las autoridades competentes, subrayando la necesidad de un equilibrio adecuado entre la protección de los derechos y libertades fundamentales de los ciudadanos, en especial su derecho a la intimidad[66]; la necesidad de luchar contra la delincuencia; y la carga económica para los proveedores.

El sector y las autoridades competentes, conjuntamente, pueden aumentar la conciencia pública acerca de los riesgos que plantean los delincuentes en Internet, promover las mejores prácticas para la seguridad, y desarrollar instrumentos y procedimientos eficaces para luchar contra la delincuencia. Ya ha habido iniciativas en este sentido en varios Estados miembros, de las cuales el Foro británico sobre la delincuencia en Internet es probablemente el más antiguo y de mayor envergadura[67].

La Comisión acoge con satisfacción estas iniciativas y considera que deben fomentarse en todos los Estados miembros. La Comisión se propone crear un foro de la UE que reúna a organismos responsables de la aplicación de la ley, proveedores de servicios de Internet, operadores de telecomunicaciones, organizaciones de libertades civiles, representantes de los consumidores, autoridades responsables de la protección de datos y otras partes interesadas, con el objetivo de mejorar la cooperación a escala de la UE. En una primera fase, participarán funcionarios públicos nombrados por los Estados miembros, expertos en tecnología, expertos en cuestiones de intimidad que serán designados por el Grupo sobre protección de datos del art. 29, y representantes del sector y de los consumidores, que serán seleccionados previa consulta con asociaciones del sector y de los consumidores. En una fase posterior, este foro incluirá a representantes de iniciativas nacionales pertinentes.

El foro de la UE se gestionará de forma abierta y transparente, y los documentos pertinentes se publicarán en una página web. Asimismo, se invitará a todas las partes interesadas a que formulen comentarios.

---

65 En el comunicado oficial adoptado en Washington los días 9 y 10 de diciembre de 1997 sobre principios y un plan de acción de 10 puntos para luchar contra la delincuencia de alta tecnología, los Ministros de Justicia e Interior del G8 declararon lo siguiente: "es el sector industrial el que diseña, despliega y mantiene estas redes globales, y él es el responsable principal de la elaboración de normas técnicas. Así pues, corresponde al sector industrial desempeñar su parte en el desarrollo y la distribución de sistemas seguros diseñados para ayudar a detectar el abuso informático, conservar las pruebas electrónicas y contribuir a determinar la situación e identidad de los delincuentes". La decisión del Consejo de la UE de luchar contra la pornografía infantil en Internet subraya la necesidad de que los Estados miembros mantengan un diálogo constructivo con el sector, y en contacto con él, cooperaren compartiendo sus experiencias.

66 Según lo establecido en las Directivas de la UE sobre protección de datos, el Convenio del Consejo de Europa sobre Derechos Humanos, el Convenio n° 108 del Consejo de Europa para la protección de las personas en lo que respecta al tratamiento automatizado de los datos personales y el derecho nacional pertinente.

67 Creado en 1997, el Foro sobre la delincuencia en Internet está compuesto por agentes de policía, funcionarios del Ministerio de Interior y funcionarios responsables de la protección de datos, y representantes del sector de Internet; celebra reuniones plenarias 3 o 4 veces al año y cuenta con varios grupos de trabajo permanentes.

Se invitará al foro de la UE a que estudie en particular los siguientes aspectos:

- Desarrollo, cuando proceda, de puntos de contacto permanentes entre el Gobierno y el sector;

- Desarrollo de un formato adecuado para las peticiones de información de las autoridades competentes al sector, aumentando el uso de Internet por parte de las autoridades competentes al comunicarse con los proveedores de servicios;

- Fomento del desarrollo y/o de la aplicación de códigos de conducta y mejores prácticas, y distribución de dichos códigos entre el sector y los Gobiernos[68];

- Fomento del intercambio de información sobre tendencias en la delincuencia de alta tecnología entre diversas partes, particularmente el sector y los organismos responsables de la aplicación de la ley;

- Exploración de los intereses de las autoridades competentes en cuanto al desarrollo de nuevas tecnologías;

- Fomento del desarrollo de mecanismos de detección temprana y gestión de crisis con el fin de prevenir, identificar y manejar amenazas o eventos perjudiciales para las infraestructuras de información;

- Aportación, donde se requiera, de la contribución de expertos que trabajen en el Consejo y en otros foros internacionales, como el Consejo de Europa y el G8;

- Fomento de la cooperación entre las partes interesadas, incluyendo principios compartidos por las autoridades competentes, el sector y los usuarios (por ejemplo, memorándum de acuerdo, códigos de prácticas acordes con el marco jurídico, etc.).

6.5. Acciones directas del sector

En gran parte, la lucha contra la delincuencia informática interesa a la propia comunidad en el sentido más amplio. Para que los consumidores confíen en el comercio electrónico, las medidas de prevención de la delincuencia informática deben constituir un elemento aceptado de las buenas prácticas comerciales. Muchos sectores, por ejemplo la banca, las comunicaciones electrónicas, las tarjetas de crédito y los derechos de autor, y sus clientes, son víctimas potenciales de la delincuencia informática. Las empresas protegen, evidentemente, sus propios nombres y marcas registradas, y desempeñan por tanto una función en la prevención del fraude. Las organizaciones que representan a los sectores del software y de audio (por ejemplo, la industria fonográfica británica - BPI) cuentan con equipos de investigación de la piratería (incluida la piratería relacionada con Internet). Los proveedores de servicios de Internet en varios Estados miembros han creado líneas directas para la comunicación de contenidos ilícitos y nocivos.

---

[68] Por lo que respecta a los códigos de conducta en el sentido del artículo 27 de la Directiva 95/46/CE (podrían cubrir, por ejemplo, cuestiones correspondientes al ámbito de la Directiva 97/66/CE tales como las interceptaciones), participan el Grupo de trabajo sobre protección de datos del artículo 29 y las autoridades nacionales de control de la protección de datos.

La Comisión ha apoyado algunas de estas iniciativas, fomentando su participación en el programa marco de I+D de la UE, en el plan de acción de Internet[69] y en los programas del título VI tales como STOP y DAPHNE.

En el foro de la UE se intercambiarán las mejores prácticas en estos ámbitos.

6.6. Proyectos de IDT apoyados por la UE

En el Programa de Tecnologías de la Sociedad de la Información, que forma parte del 5º programa marco 1998-2002, se hace hincapié en el desarrollo y despliegue de tecnologías destinadas a crear confianza. Como tales, las tecnologías destinadas a crear confianza abarcan tanto las tecnologías sobre seguridad de redes y de información, como los métodos e instrumentos técnicos destinados a la protección contra el abuso del derecho fundamental a la protección de datos y de la intimidad y otros derechos personales, y la lucha contra la delincuencia informática.

El Programa TSI, y en especial los trabajos relacionados con la *seguridad de la información y de las redes y otras tecnologías de fomento de la confianza,* de la Acción clave 2 - *Nuevos métodos de trabajo y comercio electrónico,* proporcionan el marco para desarrollar la capacidad y las tecnologías destinadas a comprender y abordar los nuevos retos tecnológicos relacionados con la prevención y la lucha contra la delincuencia informática y garantizar el cumplimiento de los requisitos de seguridad e intimidad a escala de la UE, de las comunidades virtuales y de los individuos.

Asimismo, para tratar correctamente los retos relacionados con la confianza y la seguridad, incluyendo la prevención y la investigación de la delincuencia informática, también se ha puesto en marcha una iniciativa sobre confianza en el contexto del Programa TSI. El papel de esta iniciativa es contribuir a aumentar la seguridad y la confianza en infraestructuras de información muy interconectadas y en sistemas de alta integración en redes, promoviendo la toma de conciencia respecto a la seguridad y las tecnologías que proporcionan seguridad. Parte integrante de esta iniciativa es la cooperación internacional. El Programa TSI ha desarrollado relaciones de trabajo con DARPA y NSF, y ha establecido, en colaboración con el Departamento de Estado de EE.UU., un grupo de trabajo conjunto sobre protección de infraestructuras críticas bajo los auspicios del Grupo consultivo conjunto CE/EE.UU. sobre el Acuerdo de Cooperación de C+T[70].

El Centro Común de Investigación de la Comisión (CCI), que ha apoyado la iniciativa de seguridad del Programa TSI, centrará sus esfuerzos en desarrollar estadísticas, indicadores y medidas adecuadas y armonizadas en consulta con otras partes interesadas, incluida Europol. El objetivo será desarrollar una clasificación y comprensión adecuadas de las actividades ilegales, su distribución geográfica, el índice de aumento y la eficacia de las medidas tomadas para contrarrestarlas. Cuando proceda, el CCI incluirá a otros grupos de investigación e integrará sus esfuerzos y resultados. Asimismo, mantendrá un sitio web sobre este tema e informará al Foro de la UE acerca de su progreso.

---

69 Para más información sobre el plan de acción de Internet, consúltese el Plan de acción para propiciar una mayor seguridad en la utilización de Internet en http://158.169.50.95:10080/iap/.

70 Para más información sobre el Programa TSI, consúltese http://www.cordis.lu/ist.

7. CONCLUSIONES Y PROPUESTAS

La prevención y la lucha eficaz contra la delincuencia informática exige la existencia de varias condiciones:

- La disponibilidad de tecnologías preventivas. Esto exige un marco normativo adecuado que proporcione margen e incentivos para la innovación y la investigación. La financiación pública puede justificarse para apoyar el desarrollo y despliegue de tecnologías de seguridad adecuadas.

- La conciencia de los posibles riesgos para la seguridad y la forma de combatirlos.

- Disposiciones legislativas sustantivas y procesales adecuadas, tanto por lo que se refiere a las actividades delictivas nacionales como transnacionales. Los derechos penales sustantivos nacionales deberían ser suficientemente completos y eficaces en la tipificación del abuso informático grave y prever sanciones disuasorias, ayudando a superar los problemas de doble tipicidad[71] y facilitando la cooperación internacional. Cuando se justifique debidamente una acción por parte de las autoridades responsables de la aplicación de la ley para investigar de forma acelerada los sistemas informáticos e incautar o copiar con seguridad datos informáticos en su territorio nacional, con el fin de investigar un delito relacionado con la informática, las normas procesales deberán permitirlo, de conformidad con los principios y excepciones previstos en el derecho comunitario y de acuerdo con el Convenio Europeo sobre Derechos Humanos. La Comisión opina que el acuerdo alcanzado sobre disposiciones de interceptación en el Convenio sobre asistencia judicial en materia penal constituye el grado máximo posible en la fase actual. La Comisión seguirá revisando su aplicación con los Estados miembros, los responsables del sector y los usuarios para asegurarse de que las iniciativas pertinentes son eficaces, transparentes y equilibradas.

- La disponibilidad de un número suficiente de personal responsable de la aplicación de la ley bien formado y equipado. Se fomentará una estrecha colaboración con proveedores de servicios de Internet y operadores de telecomunicaciones en el ámbito de la formación.

- Mayor cooperación entre todos los participantes: usuarios y consumidores, responsables del sector, autoridades competentes y autoridades responsables del control de la protección de datos. Esto es esencial para la investigación de los delitos informáticos y la protección de la seguridad pública. El sector debe actuar en el marco de normas y obligaciones claras. Los Gobiernos deberían reconocer que las necesidades de las autoridades competentes pueden suponer cargas al sector, y tomar por tanto medidas razonables para minimizar tales cargas. Al mismo tiempo, el sector debería incluir consideraciones de seguridad pública en sus prácticas empresariales. Cada vez más, ello necesitará la cooperación y el apoyo activos de los usuarios y consumidores individuales.

- Iniciativas continuas dirigidas por el sector y la UE. Las líneas directas, que ya funcionan para la comunicación de los contenidos ilícitos y nocivos, pueden ampliarse a otros tipos de abusos. La autorregulación sectorial y un memorándum de acuerdo multidisciplinar podrían abarcar el mayor número posible de partes interesadas y desempeñar un papel

---

[71] En los casos en que las investigaciones penales necesiten la asistencia de autoridades de otros países, muchos ordenamientos jurídicos requieren que el delito sea punible en ambos países como requisito previo para determinados tipos de ayuda judicial mutua y para la extradición.

múltiple en la ayuda a la prevención y la lucha contra la delincuencia informática, y una mayor confianza y toma de conciencia.

- Los logros y el potencial de la I+D deberían aprovecharse en la medida de lo posible. El foco estratégico consistirá en reunir avances tecnológicos e iniciativas políticas de la UE asequibles y eficaces, y otros tendentes a crear mayor seguridad.

No obstante, cualquier medida que deba contar con el acuerdo de la UE, deberá tener en cuenta la necesidad de acercar poco a poco a estos países candidatos al ámbito de la UE y de la cooperación internacional en este sector, y evitar que se utilicen como paraísos para la delincuencia informática. Debería estudiarse la participación de representantes de estos países en alguna o en todas las reuniones pertinentes de la UE.

Las propuestas de la Comisión pueden dividirse en las siguientes áreas:

7.1. Propuestas legislativas

La Comisión presentará propuestas legislativas con arreglo al Título VI del TUE:

- Aproximación de las legislaciones de los Estados miembros en el ámbito de los delitos relacionados con la pornografía infantil. Esta iniciativa formará parte de un paquete de propuestas que cubrirá asimismo cuestiones más amplias asociadas con la explotación sexual de los niños y la trata de seres humanos, según se anunció en la Comunicación de la Comisión sobre la trata de seres humanos de diciembre de 1998. Tal propuesta coincidirá plenamente con el intento del Parlamento Europeo de convertir la iniciativa austríaca de una decisión del Consejo sobre pornografía infantil en una decisión marco que requerirá la aproximación de las legislaciones. Esto coincide asimismo con las conclusiones de Tampere y la estrategia de la UE para el nuevo milenio de lucha contra la delincuencia organizada, y ya forma parte del calendario para el establecimiento de un espacio de libertad, seguridad y justicia.

- Mayor aproximación del derecho penal sustantivo en el ámbito de la delincuencia de alta tecnología. Esto incluirá los delitos relacionados con la piratería y la denegación de servicio. La Comisión examinará asimismo el alcance de las medidas contra el racismo y la xenofobia en Internet, con vistas a presentar una propuesta para una decisión marco del Consejo, en virtud del Título VI del TUE, que cubra las actividades racistas y xenófobas en línea y fuera de línea. También se examinará el problema de las drogas ilegales en Internet.

- Aplicación del principio de reconocimiento mutuo de los autos anteriores al juicio asociados con las investigaciones de delitos informáticos, y mayor facilidad para las investigaciones penales de delitos relacionados con la informática que impliquen a más de un Estado miembro, con las salvaguardias adecuadas por lo que respecta a los derechos fundamentales. Esta propuesta es coherente con el programa global de medidas para el reconocimiento mutuo, que hace referencia a la necesidad de considerar propuestas sobre la presentación y congelación de pruebas.

La necesidad de adoptar medidas, en particular de naturaleza legislativa, sobre la cuestión de la retención de datos sobre tráfico, será evaluada por la Comisión, entre otras consultas, con arreglo al resultado del trabajo que realice el propuesto Foro de la UE en este ámbito.

7.2. Propuestas no legislativas

Se proponen medidas en varias áreas:

- La Comisión creará y presidirá un foro de la UE que reunirá a organismos responsables de la aplicación de la ley, a proveedores de servicios, a operadores de redes, a grupos de consumidores y a autoridades responsables de la protección de datos, con el objetivo de aumentar la cooperación en la UE incrementando la conciencia pública sobre los riesgos que plantean los delincuentes en Internet, promoviendo las mejores prácticas para la seguridad de la TI, desarrollando procedimientos e instrumentos eficaces de lucha contra la delincuencia para combatir la delincuencia informática, y fomentando el desarrollo de mecanismos de detección temprana y gestión de crisis. Ésta sería una versión para la UE de foros similares existentes en algunos Estados miembros y que tienen gran éxito. En los casos en que no existan tales foros, la Comisión animará a los Estados miembros a que los creen. La cooperación entre estos foros se fomentará y se facilitará a través del foro de la UE.

- La Comisión continuará promoviendo la seguridad y la confianza en el contexto de la iniciativa *e*Europa, el Plan de Acción de Internet, el Programa TSI y el próximo programa marco de IDT. Éstos incluirán el fomento de la disponibilidad de productos y servicios con un nivel apropiado de seguridad, y el estímulo de un uso más liberalizado del cifrado reforzado a través del diálogo entre las partes interesadas.

- La Comisión promoverá otros proyectos al amparo de los programas existentes, con el fin de apoyar la formación del personal responsable de la aplicación de la ley en cuestiones relacionadas con la delincuencia de alta tecnología, y para apoyar la investigación en informática forense.

- La Comisión estudiará la posibilidad de financiar la mejora del contenido y la utilidad de la base de datos de legislaciones nacionales de los Estados miembros proporcionada por el estudio COMCRIME, y lanzará un estudio para obtener un mejor panorama de la naturaleza y el grado de la delincuencia informática en los Estados miembros.

7.3. Acciones en otros foros internacionales

La Comisión continuará desempeñando una importante función en la coordinación entre los Estados miembros en otros foros internacionales donde se discute la delincuencia informática, tales como el Consejo de Europa y el G8. Las iniciativas de la Comisión a escala de la UE tendrán plenamente en cuenta el progreso en otros foros internacionales, buscando simultáneamente la aproximación en el seno de la UE.

* * * * *

FICHA FINANCIERA

1. DENOMINACIÓN DE LA ACCIÓN

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.

2. LÍNEAS PRESUPUESTARIAS IMPLICADAS

B5 302
B5 820
B6 1110, B6 2111, B6 1210

3. BASE JURÍDICA

Artículos 95, 154 y 155 del Tratado CE, y artículos 29 y 34 del Tratado de la UE.

4. DESCRIPCIÓN DE LA OPERACIÓN

4.1. Objetivo general

La Comisión creará y presidirá un foro de la UE donde se reunirán los organismos responsables de la aplicación de la ley, los prestadores de servicios de Internet, los operadores de telecomunicaciones, las organizaciones de libertades civiles, los representantes de los consumidores, las autoridades responsables de la protección de datos y otras partes interesadas, con el objetivo de reforzar la comprensión y la cooperación mutuas a escala de la UE. El foro intentará aumentar la conciencia pública acerca de los riesgos que plantean los delincuentes en Internet, promover las mejores prácticas para la seguridad, establecer herramientas efectivas y procedimientos de lucha contra la delincuencia informática y fomentar el desarrollo futuro de mecanismos de detección temprana y gestión de crisis. Los documentos pertinentes se publicarán en un sitio de Internet.

4.2 Período cubierto y disposiciones para la renovación

2001-2002. En 2002, se evaluará si procede continuar con el foro.

5. CLASIFICACIÓN DE LOS GASTOS O INGRESOS

5.1. Gastos no obligatorios

5.2. Créditos disociados

6. TIPO DE GASTOS O INGRESOS

Reuniones : reembolso de gastos de desplazamiento para expertos			
B5 302A	2001		27.000 €
B5 302A	2002		40.500 €
Funcionamiento del foro, mantenimiento de un sitio Internet			
B6 1110	2001	Misiones del CCI	10.000 €
B6 2111	2001	Créditos específicos del CCI (varios)	15.000 €
B6 1210	2001	Recursos para gastos generales del CCI	50.000 €
B6 1110	2002	Misiones del CCI	10.300 €
B6 2111	2002	Créditos específicos del CCI (varios)	15.450 €
B6 1210	2002	Recursos para gastos generales del CCI	51.500 €
Estudios sobre cuestiones específicas			
B6 2111	2001	Créditos específicos del CCI (estudios)	25.000 €
B6 2111	2002	Créditos específicos del CCI (estudios)	25.750 €
Total	2001 + 2002		270.500 €

7. IMPACTO FINANCIERO

Método para calcular el coste total de la operación (relación entre costes individuales y totales):

Reembolso de gastos de desplazamiento para los participantes en las reuniones. Calculamos celebrar 2 reuniones en 2001 y 3 reuniones en 2002. Se reembolsará a 15 expertos por reunión. El coste medio de reembolso por persona se calcula en 900 €.

Los costes, tanto de personal como de créditos específicos, infraestructura y apoyo administrativo y técnico, se asignan en proporción al número de personal asignado a las actividades en cuestión. El presupuesto para estudios se calcula sobre la base de 2 estudios por año, de aproximadamente 1 persona/mes por cada uno.

8. MEDIDAS DE PREVENCIÓN DEL FRAUDE

Controles rutinarios. No se ha previsto ninguna medida adicional de prevención del fraude.

9. ELEMENTOS DEL ANÁLISIS DE LA RENTABILIDAD

9.1. Objetivos específicos y cuantificados; población objetivo

Refuerzo de la comprensión y la cooperación mutuas a escala de la UE por parte de los distintos grupos de interés. Participantes a quienes va dirigido: organismos responsables de la aplicación de la ley, prestadores de servicios de Internet, operadores de telecomunicaciones, organizaciones de libertades civiles, representantes de los consumidores, autoridades responsables de la protección de datos y otras partes interesadas.

9.2. Bases para el funcionamiento

El foro se ha creado con el objetivo de reforzar la comprensión y la cooperación mutuas de diversos grupos de interés a escala de la UE. El foro intentará aumentar la conciencia pública acerca de los riesgos que plantean los delincuentes en Internet, promover las mejores prácticas para la seguridad, establecer herramientas efectivas y procedimientos de lucha contra la delincuencia informática y fomentar el desarrollo futuro de mecanismos de detección temprana y gestión de crisis.

9.3. Control y evaluación del funcionamiento

La Comisión organizará y presidirá las reuniones del foro y participará en las discusiones. La Comisión gestionará el sitio Internet asociado. En 2002 se evaluará la necesidad de continuar el foro en 2003 y posteriormente.

10. GASTOS ADMINISTRATIVOS

Los requisitos en términos de recursos humanos se cubrirán con el personal existente.

10.1. Efecto en el número de puestos

Tipo de puesto	Personal que se asignará a la gestión de la operación		Procedencia		Duración
	Puestos permanentes	Puestos temporales	Recursos existentes en la DG	Recursos adicionales	
Funcionarios o agentes temporales A B C	 0.05	 1,75 0,15	 1,75 0,15 0,05		Por año más de 2 años
Otros recursos					
Total	0.05	1.9	1.95		

10.2.Impacto financiero global de los recursos humanos

	Cantidades	Método de cálculo (2001 - 2002)
Funcionarios	421 200 €	2 años x 108.000 € x 1.95 personas