



COMISIÓN DE LAS COMUNIDADES EUROPEAS

Bruselas, 19.04.2002
COM(2002)173 final

2002/0086 (CNS)

Propuesta de

DECISIÓN-MARCO DEL CONSEJO

relativa a los ataques de los que son objeto los sistemas de información

(presentada por la Comisión)

EXPOSICIÓN DE MOTIVOS

1. INTRODUCCIÓN

Las redes de comunicación electrónica y los sistemas de información forman actualmente parte integrante de la vida diaria de los ciudadanos de la UE y desempeñan un papel fundamental en el éxito de la economía europea. Cada vez están más interconectadas y es mayor la convergencia de los sistemas de información y las redes. Esta tendencia implica sin duda numerosas y evidentes ventajas, pero va acompañada también de un riesgo inquietante de ataques malintencionados contra los sistemas de información. Estos ataques pueden adoptar formas muy distintas, incluido el acceso ilegal, la difusión de programas perjudiciales y ataques por denegación de servicio. Es posible lanzar estos ataques desde cualquier lugar del mundo hacia el resto del mundo y ello, además, en cualquier momento. En el futuro podrían producirse nuevas formas de ataques inesperados.

Los ataques contra los sistemas de información constituyen una amenaza para la creación de una sociedad de la información más segura y de un espacio de libertad, seguridad y justicia y conviene, pues, que la Unión Europea dé una respuesta. La presente propuesta de Decisión marco sobre la armonización del derecho penal relativo a los ataques de los que son objeto los sistemas de información constituye una parte de la respuesta de la Comisión.

1.1. Tipos de ataques contra los sistemas de información

La expresión "sistema de información" se utiliza deliberadamente aquí en su sentido más amplio habida cuenta de la convergencia entre las redes de comunicación electrónica y los distintos sistemas que conectan. A efectos de la presente propuesta, los sistemas de información cubren, pues, los ordenadores personales autónomos, las agendas electrónicas personales, los teléfonos móviles, los intranets, los extranets y, naturalmente, las redes, servidores y otras infraestructuras de Internet.

En su Comunicación "Seguridad de las redes y de la información - Propuesta para un enfoque político europeo"¹, la Comisión propuso la descripción siguiente de las amenazas contra los sistemas informáticos:

- a) **Acceso no autorizado a sistemas de información.** Esto incluye el concepto de "piratería informática". La piratería consiste en tener acceso de manera no autorizada a un ordenador o a una red de ordenadores. Puede tomar distintas formas que van desde el mero uso de informaciones internas a ataques directos y la interceptación de contraseñas. Se realiza generalmente –pero no siempre– con una intención dolosa de copiar, modificar o destruir datos. La corrupción deliberada de sitios Internet o el acceso sin previo pago a servicios restringidos puede constituir uno de los objetivos del acceso no autorizado.
- b) **La perturbación de los sistemas de información.** Existen distintas maneras de perturbar los sistemas de información mediante ataques malintencionados. Uno de los medios más conocidos de denegar o deteriorar los servicios ofrecidos por Internet

¹ Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de Regiones "Seguridad de las redes y de la información - Propuesta para un enfoque político europeo" de 6 de junio de 2001. COM (2001) 298 final.

es el ataque de tipo "**denegación de servicio**" (DdS). Este ataque es en cierta medida similar al hecho de inundar las máquinas de fax con mensajes largos y repetidos. Los ataques del tipo denegación de servicio tienen por objeto sobrecargar los servidores o los proveedores de servicios Internet (PSI) con mensajes generados automáticamente. Otros tipos de ataques pueden consistir en perturbar los servidores que hacen funcionar el sistema de nombres de dominio (DNS) y los ataques contra los "encaminadores". Los ataques destinados a perturbar los sistemas han sido perjudiciales para algunos sitios web prestigiosos como los portales. Según algunos estudios, un reciente ataque causó daños estimados en varios centenares de millones de euros, sin contar el perjuicio no cuantificable en términos de reputación. Las empresas cuentan cada vez más con un sitio Web propio y las que dependen de él para el suministro "justo a tiempo" son especialmente vulnerables.

- c) **Ejecución de programas informáticos perjudiciales que modifican o que destruyen datos.** El tipo más conocido de programa informático malintencionado es el virus. Los virus "I Love You", "Melissa" y "Kournikova" son ejemplos conocidos. Alrededor de 11% de los usuarios europeos se han visto afectados por un virus en su ordenador personal (PC). Existen otros tipos de programas informáticos perjudiciales. Algunos dañan al propio ordenador, mientras que otros utilizan el PC para atacar otros elementos de la red. Algunos programas (llamados "bombas lógicas") pueden permanecer inactivos hasta que se desencadenan por algún motivo como, por ejemplo, una fecha determinada y causan graves daños modificando o destruyendo datos. Otros programas parecen benignos, pero cuando se los lanza, desencadenan un ataque perjudicial (por eso se los llama "Caballos de Troya"). Otros programas (llamados "gusanos") no infectan otros programas como los virus, pero crean réplicas de ellos mismos, estas réplicas crean a su vez nuevas réplicas y de este modo se termina por inundar el sistema.
- d) **Intercepción de las comunicaciones.** La interceptación malintencionada de comunicaciones afecta a los requisitos de confidencialidad e integridad de los usuarios. Se le denomina a menudo "sniffing" (intromisión).
- e) **Declaraciones falsas.** Los sistemas de información ofrecen nuevas posibilidades de declaraciones falsas y de fraude. El hecho de usurpar la identidad de otra persona en Internet y de utilizarla con fines malintencionados se llama "spoofing" (modificación de los datos).

1.2. La naturaleza del riesgo

Existe una necesidad clara de recoger informaciones fiables sobre la amplitud y la naturaleza de los ataques contra los sistemas de información.

Los ataques más graves contra los sistemas de información se dirigen a los operadores de redes de comunicaciones electrónicas y a los servidores de servicios o a las sociedades de comercio electrónico. Los ámbitos más tradicionales pueden también verse afectados seriamente debido al nivel de interconexión cada vez mayor en las comunicaciones modernas: las industrias manufactureras, los servicios, los hospitales, organismos del sector público y Gobiernos. No obstante, las víctimas de los ataques no son sólo organizaciones; los ataques pueden también causar graves daños directos y perjudiciales a los particulares. La carga económica que suponen algunos de estos ataques a los organismos públicos, a las empresas y a las personas privadas es considerable y amenaza con hacer los sistemas de información más costosos y menos asequibles a los usuarios.

Los ataques antes descritos son efectuados a menudo por individuos que actúan por cuenta propia, a veces por menores que no son plenamente conscientes de la gravedad de sus actos. No obstante, el nivel de sofisticación y las ambiciones de los ataques podrían agravarse. Existe una preocupación creciente de que bandas de delincuentes organizadas utilicen las redes de comunicación para lanzar ataques contra los sistemas de información. Los grupos de piratas informáticos especializados en la piratería y la degradación de sitios Internet son cada vez más activos a escala mundial. Ejemplo de ello son los "Brazilian Silver Lords" y "Pakistan Gforce", que intentan extorsionar a sus víctimas proponiéndoles una asistencia especializada tras el pirateo de sus sistemas de información. La detención de importantes grupos de "piratas informáticos o hackers" hace pensar que la piratería podría constituir cada vez más un fenómeno organizado de delincuencia. Recientemente se han producido ataques sofisticados y organizados contra los derechos de propiedad intelectual y tentativas de robo de sumas importantes a servicios bancarios².

Las violaciones en la seguridad de las bases de datos mercantiles del e-comercio electrónico en las que se tiene acceso a información sobre los clientes, incluidos números de tarjeta de crédito, son también una causa de preocupación. Estos ataques suponen cada vez más medios para el fraude en el pago y obligan a la banca a cancelar y a expedir de nuevo miles de tarjetas. Otra consecuencia es el daño no cuantificable a la reputación mercantil y a la confianza del consumidor en el comercio electrónico. Medidas preventivas, tales como requisitos mínimos de seguridad para negociantes en línea que aceptan tarjetas de pago, se están discutiendo conforme al plan de acción para prevenir el fraude y la falsificación de los medios de pago³ no monetarios.

La presente propuesta forma parte asimismo de la contribución de la Comisión a la respuesta a la amenaza de ataque terrorista contra sistemas de información vitales en la Unión Europea y completa las propuestas de la Comisión destinadas a sustituir en el seno de la Unión Europea el procedimiento de extradición mediante una orden de detención europea⁴ y de armonizar las legislaciones en materia de terrorismo⁵, sobre lo cual se ha alcanzado un acuerdo político en el Consejo Europeo de Laeken de los días 14 y 15 de diciembre de 2001. En su conjunto, estos instrumentos permitirán que los Estados miembros de la Unión Europea dispongan de una legislación penal adecuada para luchar contra el ciberterrorismo y reforzarán la cooperación internacional contra el terrorismo.

La presente propuesta no cubre solamente los actos dirigidos contra los Estados miembros. Se aplica también a comportamientos que tienen lugar en el territorio de la Unión Europea contra sistemas de información en el territorio de un país tercero. Esto muestra el compromiso asumido por la Comisión de luchar contra los ataques de los que son objeto los sistemas de información tanto en la Unión Europea como a escala mundial.

² Según una investigación publicada por las Asociación de Gestores de Comunicación (CMA), se han perpetrado ataques en forma de "piratería" contra un tercio de las grandes empresas y organismos del sector público del Reino Unido, incluidas las agencias gubernamentales, causando daños que van desde la infiltración en cuentas bancarias de empresas al robo de información. Véase el informe en el sitio: www.cma.org.

³ Comunicación de la Comisión "Prevención del fraude y la falsificación de los medios de pago distintos del efectivo", COM (2001) 11 final. Adoptado por la Comisión el 9.2.2001.

⁴ Propuesta de Decisión marco del Consejo relativa a la orden de detención europea. COM (2001) 522 finales. Adoptada por la Comisión el 19 de septiembre de 2001.

⁵ Propuesta de Decisión marco del Consejo relativa a la lucha contra el terrorismo. COM (2001) 521 final. Adoptada por la Comisión el 19 de septiembre de 2001

En realidad, en los últimos tiempos, las tensiones a escala internacional han supuesto un recrudecimiento de los ataques contra los sistemas de información y, de manera concreta, contra sitios Internet. Unos ataques más graves podrían no solamente tener serias consecuencias financieras, sino además, en algunos casos, implicar la pérdida de vidas humanas (sistemas hospitalarios, sistemas de control del tráfico aéreo, por ejemplo). La importancia que le atribuyen los Estados miembros se refleja en la prioridad concedida a las distintas iniciativas de protección de infraestructuras vitales. Por ejemplo, el programa comunitario sobre tecnología de la sociedad de la información (TSI)⁶ estableció, en conexión con el Ministerio estadounidense de Asuntos Exteriores, un grupo de trabajo conjunto UE/Estados Unidos sobre la protección de las infraestructuras vitales.⁷

1.3. Necesidad de disponer de información y estadísticas precisas

Existen pocas estadísticas fiables sobre el verdadero alcance del fenómeno de la delincuencia informática. El número de intrusiones detectadas y notificadas hasta ahora no refleja probablemente con exactitud todo el alcance del problema. Según una investigación estadounidense⁸, en 1999 solamente el 32% de las empresas que aseguraban haber sido víctimas de una intromisión informática durante el año anterior lo declararon a la policía. Ahora bien, se trataba de una mejora con relación a los años anteriores en los cuales solamente el 17% de las empresas en cuestión recurrieron a la policía. Este silencio estaba justificado por numerosas razones. La toma de conciencia sobre este punto y la experiencia de los administradores de sistemas y usuarios es aún limitada, lo que dificulta detectar las intrusiones. Además, muchas empresas no están dispuestas a indicar los casos de delitos informáticos para evitar una mala publicidad y con el fin de no exponerse al riesgo de nuevos ataques. En su mayoría, los servicios de policía no disponen aún de estadísticas sobre los ordenadores y sistemas de comunicación implicados en este y otros tipos de delincuencia⁹. El personal de los servicios de control no tiene la formación adecuada para detectar y definir las infracciones informáticas e investigar sobre estas infracciones. No obstante, la Unión Europea ha comenzado a estudiar esta cuestión recogiendo datos relativos a los ataques contra los sistemas de información. En un sólo Estado miembro, se estima que en 1999 se cometieron entre 30.000 y 40.000 ataques contra los sistemas de información, mientras que solamente se registraron 105 denuncias oficiales en este ámbito. En 1999, siete Estados miembros registraron en total solamente 1.844 denuncias oficiales de infracciones cometidas contra sistemas de información y datos informáticos. Esto corresponde sin embargo al doble del

⁶ La Comisión Europea gestiona el programa TSI. Forma parte del 5º programa marco que abarca el período 1998-2002. Para más información, consúltese el sitio <http://www.cordis.lu/ist>

⁷ Bajo los auspicios del grupo consultivo mixto instituido en virtud del Acuerdo de cooperación científica y tecnológica Comunidad Europea/Estados Unidos.

⁸ The Computer Security Institute (CSI) and the Federal Bureau of Investigation (FBI) publican a principios de cada año un informe titulado "Computer Crime and Security Survey". Ver el sitio del CSI y otras informaciones relativas al estudio en www.gocsi.com

⁹ El Ministerio italiano de Interior publicó recientemente estadísticas sobre sus actividades operativas en materia de delincuencia informática en 1999 y 2000 (véase el sitio: http://www.mininterno.it/dip_ps/dcpsffp/index.htm). En 2000, se indicaron oficialmente 98 casos de "hacking", lo que representa cuatro veces más que en 1999, en que sólo se denunciaron 21 casos.

número de infracciones indicadas en 1998, en que se registraron oficialmente solamente 972 casos en estos siete Estados miembros¹⁰.

Por otra parte, una reciente investigación¹¹ puso de manifiesto que el 13% de las empresas que eran víctimas de delincuencia económica indicaron que una parte de los delitos sufridos era de naturaleza informática. Esta investigación revela también una inquietud creciente respecto a la delincuencia informática: el 43% de las respuestas mencionaban la ciberdelincuencia como un riesgo futuro. Otro estudio concluyó que los "hackers" o piratas informáticos y los virus suponen el mayor riesgo de ciberdelincuencia contra las organizaciones. Los principales delincuentes informáticos son los hackers o piratas informáticos (45%), antiguos empleados (13%), grupos de delincuencia organizada (13%) y los empleados actuales (11%)¹². Estas cifras seguirán aumentando con la mayor utilización de sistemas de información y la interconexión creciente y a medida que aumente la voluntad de denunciar los ataques. No obstante, deben adoptarse medidas urgentes con el fin de elaborar una herramienta estadística que pueda ser utilizada por todos los Estados miembros y lograr así que la delincuencia informática en la Unión Europea sea controlada cuantitativa y cualitativamente. El punto de partida de este análisis debe ser una definición común a nivel de la Unión Europea de las infracciones relativas a los ataques contra los sistemas de información.

1.4. Contexto político en la Unión Europea

En este contexto, en el Consejo Europeo de Lisboa de marzo de 2000, el Consejo Europeo destacó la importancia que reviste la transición hacia una economía competitiva, dinámica y fundada en el conocimiento e invitó al Consejo y a la Comisión a establecer un Plan global de acción eEuropa para sacar el mayor provecho posible¹³. Este Plan de acción, elaborado por la Comisión y el Consejo y aprobado por el Consejo Europeo de Feira en junio de 2000, incluye acciones destinadas a reforzar la seguridad de las redes y prevé el desarrollo de un enfoque coordinado y coherente de la delincuencia informática para finales de 2002.

En el marco de su contribución a este mandato relativo a la ciberdelincuencia, la Comisión publicó una Comunicación titulada "Creación de una sociedad de la información más segura mediante la mejora de la seguridad de las infraestructuras de información y la lucha contra los delitos informáticos"¹⁴. Propone un enfoque equilibrado para tratar los problemas derivados de los delitos informáticos teniendo en cuenta la postura de todas las partes interesadas incluidos los servicios de control, los servidores de acceso, los operadores de redes, otros grupos industriales, asociaciones de consumidores, autoridades encargadas de la protección de datos y asociaciones de protección de la vida privada. La Comunicación propone una serie de iniciativas legislativas y no legislativas.

¹⁰ Doc. 8123/01 ENFOPOL 38 del Consejo. Disponible en el sitio internet del Consejo <http://db.consilium.eu.int/jai>

¹¹ Informe sobre la delincuencia económica europea 2001, PricewaterhouseCoopers 2001 (<http://www.pwcglobal.com>)

¹² Informe sobre la ciberdelincuencia de 2001 de la "Confederation of British Industry" (véase <http://www.cbi.org.uk>)

¹³ Conclusiones de la Presidencia, Consejo Europeo de Lisboa del 23 y 24 de marzo de 2000, disponibles en el sitio <http://ue.eu.int/en/Info/eurocouncil/index.htm>.

¹⁴ COM (2000) 890 final.

Un ejemplo importante de una acción en curso es en el programa IDA, en el que los Estados miembros y la Comisión ya están trabajando en favor de una política de seguridad común y están ejecutando una red segura para el intercambio de información administrativa.

Una de las cuestiones clave abordadas por la Comunicación era la necesidad de una acción efectiva contra las amenazas para la autenticidad, integridad, confidencialidad y disponibilidad de las redes y los sistemas de información. Se han logrado grandes avances en el Derecho comunitario. Ya existen varias medidas jurídicas vigentes a nivel comunitario con implicaciones específicas para la seguridad de las redes y de la información.

La presente Decisión marco complementa lo que se ha logrado ya en el campo del Derecho comunitario para proteger los sistemas de información, como por ejemplo las Directivas 95/46/CE, la Directiva 97/66/CE y la Directiva 98/84/CE relativas a la protección legal de los servicios basados o consistentes en un acceso restringido. En particular, el marco europeo de telecomunicación y protección de datos (Directivas 95/46/CE y 97/66/CE¹⁵) contiene disposiciones destinadas a garantizar que los prestatarios de servicios de telecomunicación accesibles al público adopten las medidas técnicas y organizativas convenientes para garantizar la seguridad y confidencialidad de sus servicios y que estas medidas ofrezcan un nivel de seguridad correspondiente al riesgo existente.

La prevención y la educación constituyen los medios más importantes y eficaces de tratar estos problemas. La Comunicación destaca la importancia de la disponibilidad, la aplicación, el suministro y la utilización eficaz de tecnologías preventivas. Destaca que es necesario sensibilizar al público ante los riesgos vinculados a la delincuencia informática, promover las mejores prácticas en materia de seguridad de las tecnologías de la información, definir herramientas y procedimientos eficaces con el fin de luchar contra la delincuencia informática, y fomentar el desarrollo de las medidas en materia de mecanismos de alerta rápida y gestión de las crisis. El programa comunitario sobre la tecnología de la sociedad de la información (TSI)¹⁶ proporciona un marco para el desarrollo de las capacidades y técnicas necesarias para incluir y afrontar los retos que comienza a plantear la delincuencia informática.

Más recientemente, el Consejo Europeo de Estocolmo del 23 y 24 de marzo reconoció la necesidad de acciones complementarias en el ámbito de la seguridad de las redes y de los sistemas de información y concluyó que *"el Consejo, en concertación con la Comisión, pondrá a punto una extensa estrategia en materia de seguridad de las redes electrónicas, estableciendo medidas de aplicación práctica. Esta estrategia debería estar lista a tiempo para el Consejo Europeo de Gotemburgo"*. La Comisión respondió a esta propuesta mediante la Comunicación "Seguridad en las redes y la información - Propuesta para una perspectiva política europea"¹⁷. Esta Comunicación analiza los problemas actuales en materia de seguridad de las redes y define un marco estratégico de acción en este ámbito. A ella le siguió una Resolución del Consejo del 6 de diciembre de 2001 relativa a un planteamiento común y unas acciones específicas en el ámbito de la seguridad en las redes y la información.

Estas iniciativas no bastan por sí solas para proporcionar todas las respuestas necesarias ante los graves ataques de los que son objeto los sistemas de información. Las dos

¹⁵ DO L 281 de 23 de noviembre de 1995, p 31 a 50, DO L 24 de 30 de enero de 1998, p 1 a 8.

¹⁶ El programa IST es gestionado por la Comisión Europea. Forma parte del 5º Programa Marco de 1998 2002. Se puede obtener más información en el sitio: <http://www.cordis.lu/ist>

¹⁷ COM(2001) 298, adoptado el 6 de junio de 2001

Comunicaciones de la Comisión reconocen también que era urgente armonizar a nivel de la Unión Europea el derecho positivo penal relativo a los ataques contra los sistemas de información, teniendo en cuenta así las conclusiones del Consejo Europeo de Tampere de octubre de 1999¹⁸ que incluyó la delincuencia que utiliza tecnologías avanzadas en una lista limitada de sectores en los cuales debe hacerse todo lo posible para alcanzar un acuerdo sobre definiciones, tipificación y sanciones comunes y que figura también en la recomendación n° 7 de la estrategia de la Unión Europea sobre la prevención y la represión de la delincuencia organizada para el próximo milenio, adoptada por el Consejo JAI en marzo de 2000.¹⁹ La presente propuesta de Decisión marco forma también parte del programa de trabajo de la Comisión para el año 2001²⁰ y del Marcador para el establecimiento de un espacio de libertad, seguridad y justicia, realizado por la Comisión y analizado por el Consejo de Justicia y Asuntos de Interior del día 30 de octubre de 2001²¹.

1.5. La necesidad de armonizar el derecho penal de los Estados miembros

En este ámbito, el derecho penal de los Estados miembros contiene vacíos jurídicos y diferencias importantes susceptibles de obstaculizar la lucha contra la delincuencia organizada y el terrorismo, así como los graves ataques contra los sistemas de información perpetrados por particulares. La aproximación del derecho positivo en materia de delincuencia informática contribuirá a que las legislaciones nacionales sean lo suficientemente completas para que todas las graves formas de ataques contra los sistemas de información puedan ser objeto de investigaciones mediante las técnicas y los métodos disponibles en derecho penal. Los autores de estos delitos deben ser identificados y llevados a juicio y los tribunales deben disponer de sanciones adecuadas y proporcionadas. Se enviará así un claro mensaje disuasorio a los autores potenciales de ataques contra los sistemas de información.

Además, los vacíos jurídicos y las diferencias pueden impedir una cooperación policial y judicial eficaz en caso de ataques contra sistemas de información. Estos ataques son a menudo transnacionales por su propia naturaleza y requieren una cooperación internacional policial y judicial. La aproximación de las legislaciones mejorará pues esta cooperación garantizando que se cumple la exigencia de doble incriminación (según la cual una actividad debe constituir un delito en los dos países en cuestión para que estos colaboren a nivel judicial en el marco de una investigación penal). Será útil para los Estados miembros de la UE con el fin de cooperar entre ellos, así como para reforzar la cooperación entre los Estados miembros de la UE y los terceros países (en los casos en que se haya celebrado un acuerdo de asistencia judicial mutua adecuado).

Existe también una necesidad de complementar los instrumentos existentes a nivel de la Unión Europea. La Decisión marco sobre la orden de detención europea²², el Anexo del Convenio Europol²³ y la Decisión del Consejo por la que se crea Eurojust²⁴ contienen

¹⁸ <http://db.consilium.eu.int/en/Info/eurocouncil/index.htm>.

¹⁹ La prevención y control de la delincuencia organizada: Una estrategia de la Unión Europea ante el nuevo Milenio (DO 2000 C124, 3.5.2000).

²⁰ http://europa.eu.int/comm/off/work_programme/index_en.htm

²¹ http://europa.eu.int/comm/dgs/justice_home. COM (2001) 628 final, 30.10.2001

²² DO C. . p

²³ Acto del Consejo, de 26 de julio de 1995, relativo al establecimiento del Convenio, basado en el artículo K.3 del Tratado de la Unión Europea, por el que se crea una Oficina Europea de Policía (Convenio Europol) DO C 316 de 27.11.1995 p. 0001 - 0001

²⁴ DO C. . p

referencias a los delitos informáticos que deben definirse con mayor precisión. A efectos de tales instrumentos, en el delito informático debería incluirse los ataques contra los sistemas de información de acuerdo con la definición que se hace en la presente Decisión marco, que establecerá un nivel mucho mayor de aproximación de los elementos constitutivos de tales delitos. La presente Decisión marco complementa asimismo la Decisión marco relativa a la lucha contra el terrorismo²⁵, que cubre las acciones terroristas que causan la destrucción de una instalación de infraestructuras, incluido un sistema de información, al poner en peligro vidas humanas o provocar importantes pérdidas económicas.

1.6. Ámbito de aplicación y objeto de la Decisión marco

Los objetivos de la presente Decisión marco del Consejo consisten pues en armonizar el derecho penal de los Estados miembros relativo a los ataques contra los sistemas de información y garantizar de la mejor manera posible la cooperación policial y judicial respecto a las infracciones penales en respuesta a los ataques contra los sistemas de información. Por otra parte, esta propuesta contribuye a los esfuerzos de la Unión Europea en la lucha contra el terrorismo y la delincuencia organizada. No se pretende que los Estados miembros penalicen comportamientos de escasa relevancia o poco importantes.

Del artículo 47 del Tratado de la Unión Europea se deriva claramente que la presente Decisión marco se aplicará sin perjuicio de lo dispuesto en el Derecho comunitario. En particular, no afecta a los derechos a la vida privada o a la protección de datos ni a las obligaciones previstas por el Derecho comunitario (Directivas 95/46 y 97/66, por ejemplo). La Decisión marco no exige a los Estados miembros que penalicen las infracciones que tienen por objeto el acceso /la revelación de datos de carácter personal, el secreto de las comunicaciones, la seguridad del tratamiento de los datos de carácter personal, las firmas electrónicas²⁶ o las violaciones de los derechos de propiedad intelectual y se aplica sin perjuicio de la Directiva 98/84 CE relativa a la protección jurídica de los servicios de acceso condicional basados en dicho acceso²⁷. Son cuestiones importantes, pero ya cubiertas por el Derecho comunitario en vigor. Toda aproximación del derecho penal en estos ámbitos con el fin de llegar a objetivos legislativos comunitarios como la protección de los datos de carácter personal, la remuneración de los proveedores de servicios de acceso condicional o la propiedad intelectual debe pues preverse en el marco del Derecho comunitario y en el del Título VI del TUE. Por lo tanto, la presente Decisión marco cubre solamente los comportamientos descritos en las letras a) a c) de la sección 1.1.

Las disposiciones legales en la Unión Europea deben también tener en cuenta la situación en otros foros europeos. Por lo que se refiere a la aproximación del derecho positivo penal relativo a los ataques contra los sistemas de información, es el Consejo de Europa quien más ha avanzado en esta materia, desde que comenzó a preparar un Convenio internacional sobre la ciberdelincuencia a partir de febrero de 1997 y el Convenio fue adoptado formalmente y abierto a la firma en noviembre de 2001²⁸. El Convenio tiene por objeto armonizar una serie de infracciones penales en las que se incluyen infracciones contra la confidencialidad, la

²⁵ DO C. . p

²⁶ Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica, DO L 13 de 19 de enero de 2000.

²⁷ DO L 320 de 28.11.1998, p. 54-57

²⁸ El texto está disponible en Internet en dos lenguas, en francés: <http://conventions.coe.int/treaty/fr/projets/cybercrime.htm>. y en inglés: <http://conventions.coe.int/treaty/en/projets/cybercrime.htm>.

integridad y la disponibilidad de sistemas y datos informáticos. La presente Decisión marco respeta el enfoque seguido en el Convenio del Consejo de Europa para estas infracciones.

En los debates del G8 acerca de la delincuencia vinculada a la alta tecnología, se han definido dos categorías principales de riesgos. En primer lugar, los riesgos que pesan sobre las infraestructuras informáticas y cuyo objetivo es interrumpir, denegar, deteriorar o borrar información albergada en ordenadores y redes informáticas o en los ordenadores y las propias redes y, en segundo lugar, las amenazas a través del ordenador, es decir, las actividades perjudiciales, como fraudes, blanqueo de dinero, pornografía infantil, violación de derechos de propiedad intelectual y tráfico de drogas, realizados gracias al ordenador. La presente propuesta se refiere a la primera categoría de amenazas.

La armonización de la UE debería tener en cuenta la situación en los foros internacionales y debería ajustarse a las actuales políticas comunitarias. La presente propuesta tiene también por objetivo llegar a una mayor aproximación de las legislaciones en el seno de la UE de lo que ha sido posible en otros foros internacionales.

2. FUNDAMENTO JURÍDICO

El objetivo de la creación de un espacio de libertad, seguridad y justicia debe ser alcanzado mediante la prevención y la lucha contra la delincuencia, organizada o no, incluido el terrorismo, mediante una cooperación más estrecha entre los servicios represivos y las autoridades judiciales de los Estados miembros y mediante la aproximación de las disposiciones penales en los Estados miembros. La presente propuesta de Decisión marco tiene por objeto armonizar las legislaciones y las normativas de los Estados miembros en materia de cooperación policial y judicial penal. Prevé "normas mínimas relativas a los elementos constitutivos de los actos criminales", en gran parte en materia de delincuencia organizada y terrorismo. Tiene por objeto asimismo "garantizar la compatibilidad de las normas aplicables en los Estados miembros" con el fin de facilitar y de acelerar la cooperación entre las autoridades judiciales. La base jurídica indicada en el preámbulo de la propuesta es pues el artículo 29, la letra a) del artículo 30, el artículo 31 y la letra b) del apartado 2 del artículo 34 del Tratado de la Unión Europea. La presente propuesta no tendrá una incidencia financiera en el presupuesto de las Comunidades Europeas.

3. LA DECISIÓN MARCO: ARTÍCULADO

Artículo 1 - Ámbito de Aplicación y objetivo de la Decisión marco

Este artículo indica expresamente que la Decisión marco tiene como objetivos armonizar el derecho penal de los Estados miembros en relación con los graves ataques contra los sistemas de información y contribuir de manera particular a la lucha contra la delincuencia organizada y el terrorismo y, de este modo, procurar que la cooperación judicial sea lo más estrecha posible respecto a las infracciones penales relacionadas con los ataques contra los sistemas de información. De conformidad con lo dispuesto en el artículo 47 del Tratado de la Unión Europea, la presente Decisión marco se aplicará también sin perjuicio de lo dispuesto en el Derecho comunitario. En particular, en lo relativo al derecho a la vida privada y a la protección de los datos de carácter personal, así como las obligaciones previstas por las Directivas 95/46 y 97/66. La Decisión marco no tiene por objeto exigir a los Estados miembros que penalicen las infracciones en materia de acceso/revelación de datos de carácter

personal, de confidencialidad de las comunicaciones, seguridad en el tratamiento de los datos de carácter personal, firmas electrónicas²⁹ o violaciones de los derechos de propiedad intelectual, y se aplica sin perjuicio de la Directiva 98/84/CE relativa a la protección jurídica de los servicios de acceso condicional o basados en dicho acceso³⁰.

La presente Decisión marco no exige a los Estados miembros que penalicen comportamientos menores o de escasa trascendencia. Sus artículos 3 y 4 definen los criterios que deben cumplirse para que la acción sea considerada delito. Estos criterios respetan las posibilidades de derogación y reserva previstas en el proyecto de Convenio relativo a la ciberdelincuencia del Consejo de Europa.

Todas las infracciones penales cubiertas por la Decisión marco deben haber sido cometidas de manera intencionada. El término "intencionado" se utiliza expresamente en los artículos 3, 4 y 5. Conviene interpretarlo de acuerdo con los principios normales de derecho penal de los Estados miembros que regulan la intencionalidad. Así pues, la presente Decisión marco no exige la tipificación penal de acciones en caso de falta grave u otra imprudencia, en las que no existe intencionalidad. La intención de acceder a sistemas de información o de perturbarlos de manera ilícita debería bastar y no debería ser necesario probar que el acto intencional contemplaba un sistema de información específico.

Artículo 2 - Definiciones

La Decisión marco del Consejo propuesta contiene las definiciones siguientes:

- a) "*Red de comunicaciones electrónicas*". Esta definición es la misma que la adoptada por el Consejo y el parlamento Europeo el 14 de febrero de 2002 en la Directiva relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas³¹.
- b) "*Ordenador*". Esta definición se basa en el artículo 1 del proyecto de Convenio del Consejo de Europa relativo a la ciberdelincuencia. La definición cubre también, por ejemplo, los ordenadores personales autónomos, las agendas electrónicas personales, aparatos digitales que integran convertidor y codificador, grabadores de vídeo personales y teléfonos móviles (si tienen funciones de tratamiento de datos, por ejemplo, WAP y tercera generación), que no estarían cubiertos solamente por la definición de las redes de comunicaciones electrónicas.
- c) "*Datos informáticos*". Esta definición está basada en la definición de datos de la ISO³². No cubre un libro almacenado en forma de datos informáticos (por ejemplo, preservado en formato electrónico como fichero de tratamiento de texto) o convertido en datos informáticos mediante escaneo. Por lo tanto, la definición precisa que los datos informáticos deben "haber sido creados o formateados" de manera que

²⁹ Directiva 1999/93/CE del Parlamento Europeo y el Consejo, de 13 de diciembre de 1999, sobre un marco comunitario para las firmas electrónicas, DO L 13 de 19 de enero de 2000.

³⁰ DO L 320 de 28.11.1998, p. 54-57

³¹ Para el texto final véase

³² http://europa.eu.int/information_society/topics/telecoms/regulatory/new_rf/index_en.htm#reg
La Organización internacional de normalización (ISO) es una federación mundial de organismos nacionales de normalización a la que pertenecen aproximadamente cien países.

puedan ser procesados en un sistema de información o permitan desarrollar una función en un sistema de información.

- d) "*Sistema de información*". La definición de los sistemas de información se toma originalmente de la adoptada por la OCDE en 1992 en sus Directrices para la Seguridad de los Sistemas de Información y de las definiciones previas en referencia a las redes de comunicaciones electrónicas, a los ordenadores y a los datos informáticos. Estos términos se habían utilizado también en instrumentos de Derecho comunitario previos, como la Decisión del Consejo, de 31 de marzo de 1992, "en materia de seguridad de los sistemas de información" y la Recomendación del Consejo, de 7 abril de 1995, "acerca de los criterios comunes destinados a evaluar el grado de confianza de los sistemas de información". Deben ser tecnológicamente neutros y reflejar con precisión la idea de redes y sistemas que contienen datos interconectados. Cubren tanto el material como los programas informáticos del sistema, pero no el contenido de la propia información. Cubren asimismo los sistemas autónomos. La Comisión considera que es deseable extender la protección concedida por el derecho penal a los ordenadores autónomos y no limitarla a los sistemas interconectados.
- e) "*Persona jurídica*". Se trata de una definición habitual de las anteriores Decisiones marco del Consejo.
- f) "*Persona autorizada*". Se refiere a toda persona que tenga el derecho por ley o por contrato o bien autorización legal para utilizar, administrar, controlar, probar o efectuar investigaciones científicas permitidas por la ley o de utilizar de cualquier otra manera un sistema de información, y que actúa de acuerdo con este derecho o esta autorización. Puede tratarse de personas que actúan de acuerdo con la autorización legal de otra persona que le concedió una autorización expresa. Es importante que las categorías siguientes de personas y actividades legales (dentro de los límites de los derechos, autorizaciones y responsabilidades de las personas y de acuerdo con las normas comunitarias que regulan la protección de datos y la confidencialidad de las comunicaciones) no sean penalizadas una vez que la presente Decisión marco se incorpore al Derecho nacional:
- Los actos de los usuarios habituales, ya se trate de particulares o sociedades, incluido el uso del código secreto para proteger sus propias comunicaciones y datos;
 - Descompilación de programas informáticos dentro de los límites previstos en la Directiva 91/250 de 14 de mayo de 1991 relativa a la protección jurídica de programas de ordenador³³;
 - Los actos de los administradores, inspectores y operadores de redes y sistemas;
 - Los actos de personas autorizadas que controlan un sistema en el marco de una empresa o en el caso de personas externas autorizadas a controlar la seguridad de un sistema;
 - Investigación científica permitida legalmente.

³³ DO L 122 de 17 de mayo de 1991, págs. 42 a 46.

- g) "*Sin autorización*". Este concepto es amplio y deja una cierta libertad a los Estados miembros para definir de manera concreta el delito. No obstante, con el fin de facilitar la aplicación de la Decisión marco del Consejo en las legislaciones nacionales, la Comisión juzga necesario indicar que algunas actividades no deberían constituir infracciones. No es posible, y probablemente tampoco deseable, hacer una lista de exenciones completa y restrictiva en el marco de la Unión Europea. Los términos "sin autorización" completan las definiciones previas para excluir los comportamientos de personas autorizadas. Excluyen también cualquier otra conducta cuyo carácter legal sea reconocido por el Derecho nacional, incluidos los argumentos jurídicos habituales y otros tipos de derechos reconocidos en el Derecho nacional.

Artículo 3 - Ataque mediante el acceso ilegal a sistemas de información

Este delito cubre el acceso ilícito a sistemas de información. Ello incluye el concepto de piratería informática o "hacking". Los Estados miembros son libres de excluir los casos menores o poco importantes de la tipificación del delito en el momento de la transposición de la Decisión marco al Derecho nacional.

El delito sólo debe tipificarse en el Derecho nacional de los Estados miembros en la medida en que se cometió

- (i) contra una parte cualquiera de un sistema de información que es objeto de medidas de protección especiales, o
- (ii) con la intención de causar un daño a una persona física o jurídica ; o
- (iii) con la intención de obtener un beneficio económico.

La Comisión no desea de ninguna manera cuestionar la importancia que concede a la utilización de medidas técnicas eficaces para proteger los sistemas de información. Es sin embargo deplorable que una gran parte de los usuarios se expongan a ataques sin disponer de protección técnica adecuada (o incluso de ninguna protección). Con el fin de evitar los ataques a estos usuarios, el derecho penal debe cubrir el acceso no autorizado a sus sistemas aunque estos sistemas no se beneficien de una protección técnica adecuada. Por esta razón, y siempre que exista una intención de dañar o la intención de obtener un beneficio económico, no es requisito que se hayan burlado las medidas de seguridad para considerar como cometido el delito.

Artículo 4 - Interferencia ilegal con los sistemas de información

Este delito cubre la realización intencional ilegal de una de las siguientes acciones:

- a) el hecho de obstaculizar o interrumpir de manera significativa sin autorización el funcionamiento de un sistema de información introduciendo, transmitiendo, perjudicando, borrando, deteriorando, alterando o suprimiendo datos informáticos. El hecho de introducir o transmitir datos informáticos se refiere especialmente al problema de los "ataques por denegación de servicios" que consiste en intentar deliberadamente saturar un sistema de información. La infracción cubre también la "interrupción" del funcionamiento de un sistema de información, algo que podría deducirse del término "obstaculizar", pero que se menciona expresamente a efectos de una mayor claridad. Los otros elementos del delito (dañar, borrar, deteriorar, alterar o suprimir datos informáticos) se refieren específicamente al problema de los virus y

otros tipos de ataques dirigidos a impedir o interrumpir las funciones del propio sistema de información.

- b) el hecho de borrar, deteriorar, alterar, suprimir o hacer inaccesibles los datos informáticos en un sistema de información cuando es cometido con la intención de causar un daño a una persona física o jurídica. Ello cubre los ataques mediante virus contra el contenido (datos informáticos) del sistema de información, así como el deterioro de sitios de Internet.

La letra a) contiene los términos "obstaculizar o interrumpir de manera significativa" como elemento constitutivo de la infracción con el fin de describir los efectos de tal ataque. No se define el significado de la palabra "obstaculizar de manera significativa" ya que un obstáculo puede tener distintas formas y su nivel puede variar según el tipo de ataque y las capacidades técnicas del sistema de información atacado. Cada Estado miembro determina separadamente qué criterios deben cumplirse para que un sistema de información sea considerado como "obstaculizado de manera significativa". No obstante, anomalías o perturbaciones menores del funcionamiento de los servicios no deberían considerarse como incluidas en el requisito de gravedad.

Como se ha apuntado más arriba, los Estados miembros pueden excluir casos menores o poco importantes del alcance del delito a efectos de la transposición de la presente Decisión marco al Derecho nacional.

Artículo 5 - Instigación, complicidad y tentativa

El apartado 1 del artículo 5, obliga a los Estados miembros a tomar las medidas necesarias para que se castigue judicialmente el hecho de incitar a cometer el delito contra los sistemas de información previsto en los artículos 3 y 4, de ser cómplice o de intentar cometerlo.

El apartado 2 del artículo 5, se refiere específicamente a la tentativa. En virtud de esta disposición, los Estados miembros tomarán las medidas necesarias para que las tentativas de cometer uno de los delitos contra los sistemas de información descritos en los artículos 3 y 4 sean punibles por ley.

Artículo 6 - Sanciones

El apartado 1 exige a los Estados miembros que adopten las medidas necesarias para que los delitos previstos en los artículos 3 a 5 lleven aparejadas sanciones efectivas, proporcionadas y disuasorias³⁴.

En virtud de este apartado, los Estados miembros deben prever sanciones proporcionadas a la gravedad del delito, incluyendo penas privativas de libertad por un período máximo que no será inferior a un año en los casos graves. Se excluyen de dichos casos aquellos en los que la conducta no dio lugar a daño o beneficio económico alguno.

La pena máxima consistente en un año de cárcel en los casos graves sitúa estos delitos en el ámbito de la Orden Europea de detención así como en el ámbito de otros instrumentos tales como la Decisión marco del Consejo de 26 de junio de 2001³⁵ relativa al blanqueo de

³⁴ La frase procede de la sentencia del Tribunal de Justicia de 21 de septiembre 1989 en el Asunto 68/88 [1989] ECR 2965.

³⁵ DO L 182 de 5.7.2001, p.1

capitales, la identificación, seguimiento, embargo, incautación y decomiso de los instrumentos y productos del delito.

De conformidad con la naturaleza de todas las Decisiones marco que vinculan a los Estados miembros respecto al resultado que debe obtenerse pero que les deja la elección de la forma y los medios para alcanzarlo, los Estados miembros conservan un determinado grado de flexibilidad para adaptar su legislación a estas normas y determinar la severidad de las sanciones aplicables dentro de los límites fijados por la Decisión marco y, en particular, las circunstancias agravantes del artículo 7. La Comisión destaca que corresponde a los Estados miembros establecer los criterios para determinar el grado de gravedad de una infracción de acuerdo con sus sistemas jurídicos respectivos.

Las sanciones no deben necesariamente constituir penas privativas de libertad. El apartado 2 prevé la posibilidad de que los Estados miembros puedan imponer multas complementarias o alternativas a las penas de encarcelamiento, de acuerdo con sus tradiciones y sistemas jurídicos respectivos.

Artículo 7 - Circunstancias agravantes

Este artículo prevé la posibilidad de que los Estados miembros aumenten las penas definidas en el artículo 6 en determinadas circunstancias. La Comisión subraya que la lista de circunstancias agravantes prevista en este artículo se aplica sin perjuicio de otras circunstancias consideradas como agravantes en la legislación de los Estados miembros. Esta lista tiene en cuenta las circunstancias agravantes previstas en las disposiciones nacionales en los Estados miembros y lo fijado en las propuestas de la Comisión previas a las Decisiones del marco.

La pena de encarcelamiento podrá no ser inferior a los cuatro años si se cumple una de las siguientes condiciones enumeradas en el apartado 1:

- (a) el delito fue cometido en el marco de una organización criminal según lo previsto por la Acción común 98/733/JHA, con independencia del grado de la pena al que se hace mención en dicha Acción;
- (b) el delito provocó o tuvo como consecuencia una pérdida económica directa o indirecta sustancial, el daño físico a una persona física o un daño sustancial a parte de las infraestructuras vitales del Estado miembro; o
- (c) el delito dio lugar a unos ingresos cuantiosos.

Es necesario asimismo que los Estados miembros se aseguren que los delitos mencionados en los artículos 3, 4 y 5 sean punibles mediante penas privativas de libertad mayores que las previstas en el artículo 6, cuando el delincuente haya sido condenado por tal delito mediante una sentencia firme en un Estado miembro.

Artículo 8 - Circunstancias particulares

Este artículo establece las circunstancias en base a las cuales un Estado miembro puede reducir las penas mencionadas en los artículos 6 y 7 cuando, según la opinión de la autoridad judicial competente, el delincuente causó solamente un daño menor.

Artículo 9 - Responsabilidad de las personas jurídicas

Conforme al planteamiento adoptado en varios instrumentos jurídicos adoptados por la UE para combatir diversos tipos de delincuencia, es necesario también incluir los casos en los que las personas jurídicas participan en ataques contra sistemas de información. En este sentido, el artículo 9 contiene disposiciones para imputar a una persona jurídica por los delitos previstos en los artículos 3, 4 y 5, cometidos en su beneficio por cualquier persona con un cargo de responsabilidad que actúa individualmente o como parte del órgano de la persona jurídica. El término responsabilidad deberá interpretarse a fin de incluir la responsabilidad penal o civil.

Además, según la práctica habitual, el apartado 2 establece que una persona jurídica puede también ser considerada responsable cuando la ausencia de supervisión o control por una persona con poder para ejercer ese control ha hecho posible la comisión de los delitos en su beneficio. El apartado 3 indica que las acciones legales contra una persona jurídica no impide que éstas se realicen paralelamente contra una persona física.

Artículo 10 – Sanciones aplicables a las personas jurídicas

El artículo 10 establece un requisito para las sanciones que se aplican a las personas jurídicas responsables de los delitos mencionadas en los artículos 3, 4 y 5. Prevé sanciones efectivas, proporcionadas y disuasorias, incluidas multas de carácter penal o administrativo. También se indican otras sanciones específicas aplicables a las personas jurídicas.

Artículo 11 - Competencia

La naturaleza internacional de los delitos consistentes en ataques contra sistemas de información supone que cualquier respuesta legal efectiva necesitará de disposiciones procesales sobre la competencia y la extradición claras y ambiciosas a nivel de la Unión Europea, para asegurarse que los delincuentes no puedan evitar su procesamiento.

El apartado 1 establece una serie de criterios a efectos de la atribución de competencias con el fin de procesar e investigar los actos delictivos mencionados en la presente Decisión marco. Un Estado miembro será competente en las tres situaciones siguientes:

- a) cuando el delito se cometa total o parcialmente en su territorio, independientemente de la condición de la persona jurídica o la nacionalidad de la persona física implicada (principio de territorialidad), o
- b) cuando el delincuente sea nacional de ese Estado miembro (principio de personalidad activo) y la conducta delictiva afecta a individuos o grupos de dicho Estado. Los Estados miembros que no prevean la extradición serán responsables de juzgar a sus propios nacionales que hayan cometido delitos en el extranjero; o
- c) cuando el delito se cometa en nombre de una persona jurídica establecida en el territorio de ese Estado miembro.

El apartado 2 prevé que al establecer su competencia sobre los delitos de acuerdo con el principio de territorialidad de la letra a) del apartado 1, cada Estado miembro será competente en los casos en los que:

- a) el delito es cometido por el delincuente cuando éste se encuentra físicamente presente en su territorio, independientemente de si el delito se comete contra un sistema de información en su territorio. Por ejemplo, una persona que logra un acceso no

autorizado (piratería informática) en un sistema de información en un país tercero desde el territorio del Estado miembro; o

- b) el delito implica material racista recibido en un sistema de información en su territorio, independientemente de si el delincuente comete el acto delictivo estando físicamente presente en su territorio. Por ejemplo, una persona que logra un acceso no autorizado (piratería informática) en un sistema de información en el territorio de un Estado miembro desde el territorio de un país tercero.

Dado que no todas las tradiciones jurídicas de todos los Estados miembros reconocen la competencia extraterritorial para todos los tipos de delitos, el apartado 3 les permite no aplicar las normas sobre competencia establecidas en el apartado 1 en relación con las situaciones cubiertas por las letras (b) y (c) del apartado 1.

El apartado 4 establece que cada Estado miembro tome las medidas necesarias para establecer su jurisdicción sobre los delitos mencionadas en los artículos 3 a 5 en caso de que se niegue a entregar o conceder la extradición de una persona sospechosa o condenada por tal delito a otro Estado miembro o a un tercer país.

El apartado 5 cubre los casos de conflicto de jurisdicciones, y aspira a garantizar la cooperación completa entre los Estados miembros para centralizar los procedimientos en un solo Estado miembro, si ello fuera posible. Con este fin, se recuerda que los Estados miembros pueden recurrir a cualquier organismo o mecanismo establecido en la Unión Europea para facilitar la cooperación entre sus autoridades judiciales y la coordinación de su acción. Esto incluiría Eurojust y la red judicial europea.

El apartado 6 establece que los Estados miembros informarán a la Secretaría General del Consejo y de la Comisión sobre los casos en los que opten por aplicar el apartado 3.

Artículo 12– Intercambio de información

El propósito del artículo 12 es facilitar el intercambio de información mediante puntos de contacto. Esto es importante para una cooperación eficaz de la policía. Más concretamente, la necesidad de que todos los Estados miembros se incorporen a la red de puntos de contacto del G8 fue reconocido por el Consejo de Justicia e Interior de 19 de marzo de 1998 y, más recientemente, con la adopción de una Recomendación del Consejo sobre puntos de contacto accesibles de manera ininterrumpida para la lucha contra la delincuencia de alta tecnología³⁶.

Artículo 13 - Aplicación

El artículo 13 se refiere a la aplicación y al seguimiento de la presente Decisión marco.

Se insta a los Estados miembros a que adopten las medidas necesarias para adaptarse a la Decisión marco a más tardar el 31 de diciembre de 2003.

Los Estados miembros comunicarán a la Secretaría general del Consejo y a la Comisión las medidas tomadas para la transposición a su Derecho nacional de las obligaciones que les impone la Decisión marco. Al cabo de un año, el Consejo evaluará, de acuerdo con la información remitida por los Estados miembros y un informe escrito de la Comisión, en qué

³⁶ DO C 187 de 3.7.2001, p. 5

medida los Estados miembros se han ajustado a las obligaciones impuestas por la Decisión marco.

Artículo 14 – Entrada en vigor

El artículo 14 establece que la Decisión marco entrará en vigor el vigésimo día siguiente al de su publicación en *el Diario Oficial de las Comunidades Europeas*.

Propuesta de

DECISIÓN-MARCO DEL CONSEJO

relativa a los ataques de los que son objeto los sistemas de información

EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de la Unión Europea y, en particular, el artículo 29, la letra a) del artículo 30, el artículo 31 y la letra b) del apartado 2 del artículo 34,

Vista la propuesta de la Comisión¹,

Visto el dictamen del Parlamento Europeo²,

Considerando lo siguiente:

(1) La existencia de ataques lanzados contra los sistemas de información como consecuencia de la amenaza de la delincuencia organizada y la inquietud creciente ante la posibilidad de ataques terroristas contra sistemas de información que forman parte de las infraestructuras vitales de los Estados miembros. Esta situación corre el riesgo de comprometer la realización de una sociedad de la información segura y de un espacio de libertad, seguridad y justicia y por tanto requiere una respuesta por parte de la Unión Europea.

(2) Una respuesta eficaz a esas amenazas requiere un planteamiento global en materia de seguridad de las redes y de la información, como se puso de manifiesto en el Plan de acción eEuropa la Comunicación de la Comisión titulada "Seguridad de las redes y de la información: Propuesta para una perspectiva política europea"³ y en la Resolución del Consejo de 6 de diciembre de 2001 sobre un planteamiento común y acciones específicas en el ámbito de la seguridad en la red y en la información.

(3) En la resolución del Parlamento Europeo de 5 de septiembre 2001⁴, se destaca la necesidad de un incremento mayor de la concienciación respecto a los problemas relacionados con la seguridad de la información y la conveniencia de proporcionar asistencia práctica.

(4) Las divergencias y la distancia significativa que existen entre las legislaciones de los Estados miembros en este ámbito dificultan la lucha contra la delincuencia organizada y el terrorismo, y suponen un obstáculo a una cooperación eficaz de los servicios de policía y las administraciones de justicia en materia de ataques contra los

¹ DO C. . p.

² DO C.. p

³ COM(2001) 298.

⁴ [2001/2098 (INI)]

sistemas de información. La naturaleza transnacional y transfronteriza de las redes de telecomunicación electrónicas modernas supone que los ataques suelen revestir un carácter internacional, lo que plantea la necesidad urgente de proseguir la aproximación de los derechos penales en este ámbito.

(5) El Plan de acción del Consejo y la Comisión sobre la mejor manera de aplicar las disposiciones del Tratado de Amsterdam relativas a la creación de un espacio de libertad, seguridad y justicia⁵, las conclusiones del Consejo Europeo de Tampere del 15 y 16 de octubre 1999, el Consejo Europeo de Santa Maria da Feira de 19 y 20 de junio de 2000, el Marcador de la Comisión⁶ y la Resolución del Parlamento Europeo de 19 de mayo de 2000⁷ muestran o invitan a una acción legislativa contra la ciberdelincuencia, incluidas definiciones, tipificación y sanciones comunes.

(6) Es necesario completar los trabajos realizados por las organizaciones internacionales, más concretamente los del Consejo de Europa sobre la armonización del derecho penal y los trabajos del G8 sobre la cooperación transnacional en el ámbito de la delincuencia de alta tecnología, proponiendo un enfoque común de la Unión Europea en este ámbito. Esta invitación se desarrolló más ampliamente en la Comunicación que la Comisión envió al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité Regiones, titulada "Creación de una sociedad de la información más segura mediante la mejora de la seguridad de las infraestructuras de información y la lucha contra los delitos informáticos".⁸

(7) Debe armonizarse la legislación penal en materia de ataques contra los sistemas de información con el fin de conseguir la mejor cooperación policial y judicial posible por lo que se refiere a las infracciones vinculadas a ataques contra los sistemas de información y contribuir a la lucha contra terrorismo y el crimen organizado.

(8) La Decisión marco sobre la orden de detención europea⁹, el Anexo del Convenio Europol y la Decisión del Consejo por la que se crea el euro sólo contienen referencias a los delitos informáticos (ciberdelincuencia) que necesitan definirse con mayor precisión. A efectos de tales instrumentos, se debe entender como incluidos entre los delitos informáticos los ataques contra los sistemas de información según lo definido en la presente Decisión marco que establece un nivel mucho mayor de aproximación de los elementos constitutivos de tales delitos. La presente Decisión marco, también complementa la Decisión marco relativa a la lucha contra el terrorismo¹⁰ que cubre acciones terroristas capaces de causar daños significativos en una instalación de infraestructuras, incluido un sistema de información, poniendo en peligro la vida humana o provocando una pérdida económica importante.

(9) Todos los Estados miembros han ratificado el Convenio del Consejo de Europa de 28 de enero para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. Los datos personales tratados en el

⁵ DO C19 de 23.01.1999, p.1.

⁶ COM (2001) 278 final

⁷ A5-0127/2000

⁸ COM (2000) 890.

⁹ DO C. . p

¹⁰ DO C. . p

contexto de la aplicación de la presente Decisión marco se protegerán de conformidad con los principios de dicho Convenio.

(10) Unas definiciones comunes en este ámbito, más concretamente para los sistemas de información y los datos informáticos, son indispensables para garantizar la aplicación coherente de la presente Decisión marco en los Estados miembros.

(11) Es necesario llegar a un enfoque común para los elementos constitutivos de las infracciones penales, estableciendo un delito común de acceso ilícito a un sistema de información y de intromisión ilegal dentro de tal sistema.

(12) Es necesario evitar la penalización de comportamientos intrascendentes o irrelevantes, así como la inculpación de detentadores de derechos y personas autorizadas tales como los usuarios privados o profesionales autorizados, los gestores, los controladores y explotadores de redes y sistemas, los investigadores científicos autorizados y las personas autorizadas encargadas de probar un sistema, independientemente de que la persona trabaje en la sociedad o esté contratada exteriormente y obtenga el permiso para supervisar la seguridad de un sistema.

(13) Es necesario que los Estados miembros prevean sanciones eficaces, proporcionadas y disuasorias para reprimir los ataques contra los sistemas de información, incluidas las penas de prisión en los casos más graves.

(14) Es necesario prever penas más severas cuando determinadas circunstancias que concurren en un ataque contra un sistema de información suponen una mayor amenaza para la sociedad. En estos casos, las sanciones contra los autores deben ser suficientes para que los ataques contra los sistemas de información se incluyan en el ámbito de la aplicación de los instrumentos jurídicos ya adoptados con el fin de luchar contra la delincuencia organizada, como la Acción común 98/733/JAI¹¹ de 21 de diciembre de 1998 adoptada por el Consejo sobre la base del artículo K.3 del Tratado de la Unión Europea relativa a la tipificación penal de la participación en una organización delictiva en los Estados miembros de la Unión Europea.

(15) Deben adoptarse medidas para que las personas jurídicas puedan ser consideradas responsables de las infracciones penales mencionadas en el presente instrumento en los casos en que se cometan en su beneficio y para que los Estados miembros tenga competencia sobre los delitos cometidos contra los sistemas de información en los casos en que el autor está físicamente presente en su territorio o el sistema de información se encuentra asimismo en dicho territorio.

(16) Deben también preverse medidas de cooperación entre los Estados miembros con el fin de garantizar una acción eficaz contra los ataques de los que son objeto los sistemas de información. Deben establecerse puntos de contacto operativos para el intercambio de información.

(17) Puesto que los objetivos de garantizar que los ataques contra los sistemas de información sean sancionados en todos los Estados miembros mediante penas efectivas, proporcionadas y disuasorias y de mejorar y reforzar la cooperación judicial superando los obstáculos potenciales, no pueden alcanzarse enteramente de manera

¹¹ DO L 351 de 29.12.1998, p. 1

individual por los Estados miembros, pues las normas tienen que ser comunes y compatibles, y pueden por lo tanto lograrse mejor a nivel de la Unión, ésta podrá adoptar medidas, de conformidad con el principio de subsidiariedad recogido en el artículo 2 del Tratado de la UE y según lo establecido en el artículo 5 del Tratado CE. De acuerdo con el principio de proporcionalidad, establecido en el artículo anterior, la presente Decisión marco del Consejo no va más allá del mínimo necesario para la realización de esos objetivos.

(18) La presente Decisión marco se aplicará sin perjuicio de las competencias de la Comunidad Europea.

(19) La presente Decisión marco respeta los derechos fundamentales y los principios reconocidos por la Carta de los Derechos Fundamentales de la Unión Europea y, en particular, sus Capítulos II y VI.

HA ADOPTADO LA PRESENTE DECISIÓN:

Artículo 1

Ámbito de aplicación y objeto de la Decisión marco

La presente Decisión marco tiene por objeto reforzar la cooperación entre las autoridades judiciales y las otras autoridades competentes, incluida la policía y los otros servicios especializados encargados de la aplicación de la ley en los Estados miembros, mediante la aproximación de su legislación penal en materia de ataques contra los sistemas de información.

Artículo 2

Definiciones

1. A los efectos de la presente Decisión marco, se entenderá por:
 - (a) "*Red de comunicaciones electrónicas*": los sistemas de transmisión y, cuando proceda, los equipos de conmutación y encaminamiento de redes así como otros medios que permitan el transporte de señales por cable, por radio, por soporte óptico o por cualquier otro medio electromagnético, incluidas las redes por satélite, redes terrestres móviles y fijas (conmutación por paquetes o por circuitos, incluido Internet), y sistemas de cable eléctrico en la medida en que sean utilizados con el fin de transmitir señales, así como las redes utilizadas para la emisión de radio y televisión, y las redes de televisión por cable, cualquiera que sea la naturaleza de las informaciones transmitidas o la técnica utilizada.
 - (b) "*Ordenador*": todo aparato o grupo de aparatos interconectados o relacionados entre sí, uno o varios de los cuales realizan, mediante un programa, el tratamiento automático de datos informáticos.
 - (c) "*Datos informáticos*": cualquier representación de hechos, informaciones o conceptos creada o dispuesta de tal forma que permite su tratamiento por un sistema de información, incluido un programa gracias al cual se permite a dicho sistema de información realizar una función.

- (d) *"Sistema de información"*: los ordenadores y redes de comunicación electrónicas, así como los datos informáticos almacenados, tratados, recuperados o transmitidos por estos últimos para su funcionamiento, utilización, protección y mantenimiento.
- (e) *"Persona jurídica"*: toda entidad a la cual el derecho vigente reconoce este estatuto, a excepción de los Estados y otros organismos públicos que ejercen prerrogativas estatales y organizaciones internacionales de derecho público.
- (f) *"Persona autorizada"*: toda persona física o jurídica que tenga el derecho por ley o contrato o bien la autorización legal para utilizar, administrar, controlar, probar o efectuar investigaciones científicas permitidas por la ley o utilizar de cualquier otra manera un sistema de información, y que actúa de acuerdo con este derecho o autorización.
- (g) *"Sin autorización"*: se excluyen los actos de las personas autorizadas y otros actos cuyo carácter legal es reconocido por el Derecho nacional.

Artículo 3

Acceso ilegal a los sistemas de información

Los Estados miembros dispondrán que el acceso intencionado sin autorización al conjunto o a una parte de un sistema de información sea tipificado como delito cuando sea cometido:

- (i) contra una parte cualquiera de un sistema de información que es objeto de medidas de protección especiales, o
- (ii) con la intención de causar un daño a una persona física o jurídica ; o
- (iii) con la intención de obtener un beneficio económico.

Artículo 4

Intromisión ilegal en los sistemas de información

Los Estados miembros dispondrán que la comisión de las siguientes actos intencionales sin autorización sean tipificadas como delito:

- (a) obstaculizar o interrumpir de manera significativa sin autorización el funcionamiento de un sistema de información introduciendo, transmitiendo, perjudicando, borrando, deteriorando, alterando o suprimiendo datos informáticos.
- (b) borrar, deteriorar, alterar, suprimir o hacer inaccesibles los datos informáticos en un sistema de información cuando es cometido con la intención de causar un daño a una persona física o jurídica.

Artículo 5

Inducción, complicidad y tentativa

1. Los Estados miembros garantizarán la punibilidad de la inducción intencionada y la complicidad en la comisión de los delitos contemplados en los artículos 3 y 4.

2. Los Estados miembros garantizarán la punibilidad de la tentativa de cometer los delitos mencionados en los artículos 3 y 4.

Artículo 6

Sanciones

1. Los Estados miembros dispondrán que los delitos mencionados en los artículos 3, 4 y 5 sean objeto de sanciones efectivas, proporcionadas y disuasorias incluidas las penas privativas de libertad cuyo máximo no puede ser inferior a un año en los casos graves. Se excluyen de dichos casos aquellos en los que la conducta no tuvo como resultado un daño o beneficio económico.
2. Los Estados miembros deberán garantizar la posibilidad de imponer multas además o como alternativa de las penas privativas de libertad.

Artículo 7

Circunstancias agravantes

1. Los Estados miembros dispondrán que los delitos a los que se hace mención en los artículos 3, 4 y 5 sean punibles mediante una pena privativa de libertad durante al menos cuatro años de prisión cuando los delitos se cometieron en una de las siguientes circunstancias:
 - (a) el delito se ha cometido en el marco de una organización criminal en el sentido definido por la Acción común 98/733/JAI de 21 de diciembre de 1998 relativa a la tipificación penal de la participación en una organización delictiva en los Estados miembros de la Unión Europea con independencia del grado de la pena al que se hace mención en dicha Acción;
 - (b) el delito causó o tuvo como resultado una pérdida económica importante directa o indirecta, daños corporales a una persona física o un daño importante a una parte de la infraestructura sensible del Estado miembro;
 - (c) el delito tuvo como resultado beneficios económicos importantes.
2. Los Estados miembros dispondrán que los delitos mencionadas en los artículos 3 y 4 sean punibles mediante penas privativas de libertad superiores a las previstas de conformidad con el artículo 6, cuando el delincuente haya sido condenado por tal delito mediante sentencia firme en un Estado miembro.

Artículo 8

Circunstancias particulares

Sin perjuicio de lo dispuesto en los artículos 6 y 7, los Estados miembros dispondrán que las sanciones mencionadas en dichos artículos puedan reducirse en los casos en los que la autoridad judicial competente considere que el autor del delito sólo causó daños menores.

Artículo 9

Responsabilidad de las personas jurídicas

1. Los Estados miembros dispondrán que las personas jurídicas puedan ser consideradas responsables de los actos previstos en los artículos 3, 4 y 5 cometidos en su beneficio por cualquier persona, individualmente o como miembro de un órgano de la persona jurídica, y ejerciendo un poder de dirección en el mismo en virtud:
 - (a) de un mandato de representación de la persona jurídica, o
 - (b) de un poder para tomar decisiones en nombre de la persona jurídica, o
 - (c) de un poder para efectuar un control en la persona jurídica.
2. Además de los casos previstos en el apartado 1, los Estados miembros tomarán las medidas necesarias para garantizar que una persona jurídica sea considerada responsable cuando una falta de vigilancia o de control por una de las personas citadas en el apartado 1 haga posible la comisión de los delitos mencionados en artículos 3, 4 y 5 en favor de dicha persona jurídica por una persona que se encuentra bajo su autoridad.
3. La responsabilidad de una persona jurídica en virtud de los apartados 1 y 2 no excluye las diligencias penales contra las personas físicas culpables de los delitos o conductas mencionados en los artículos 3, 4 y 5.

Artículo 10

Sanciones penales de las personas jurídicas

1. Los Estados miembros dispondrán que una persona jurídica considerada responsable en virtud del apartado 1 del artículo 9 sea objeto de penas efectivas, proporcionadas y disuasorias incluyendo multas penales o no penales y eventualmente otras sanciones como:
 - (a) exclusión de prestaciones o ayudas públicas;
 - (b) prohibición temporal o permanente del desempeño de actividades comerciales,
 - (c) sometimiento a vigilancia judicial,
 - (d) medida judicial de liquidación.
2. Los Estados miembros dispondrán que una persona jurídica considerada responsable con arreglo al apartado 2 del artículo 9 sea objeto de sanciones o medidas efectivas, proporcionadas o disuasorias.

Artículo 11

Competencia

1. Los Estados miembros serán competentes respecto a los delitos previstos en los artículos 3, 4 y 5 cuando el delito se cometió:
 - (a) total o parcialmente en su territorio; o
 - (b) por uno de sus nacionales y el acto afecta a individuos o grupos del Estado de que se trate, o
 - (c) en nombre de una persona jurídica que tiene su domicilio social en el territorio de dicho Estado miembro.
2. Al delimitar su competencia de acuerdo con la letra a) del apartado 1, los Estados miembros tomarán todas las medidas necesarias para que su competencia incluya los casos en los que:
 - (a) el autor del delito comete éste estando físicamente presente en su territorio, independientemente de que el delito sea o no contra un sistema de información en su territorio;
 - (b) el delito se realiza contra un sistema de información situado en su territorio, independientemente de que el delincuente cometa el delito o no estando físicamente presente en su territorio.
3. Un Estado miembro podrá decidir no aplicar, o aplicar sólo en casos o circunstancias específicas, el criterio de competencia contemplado en las letras b) y c) del apartado 1.
4. Los Estados miembros tomará las medidas necesarias para establecer su jurisdicción sobre los delitos mencionados en los artículos 3 a 5 en caso de que rechace entregar o conceder la extradición de una persona sospechosa o condenada por tal delito a otro Estado miembro o a un tercer país.
5. Cuando el delito corresponda a la jurisdicción de varios Estados miembros y cuándo cualquier Estado concernido pueda válidamente enjuiciar sobre la base de los mismos hechos, los Estados miembros concernidos cooperarán para decidir cuál de ellos procesará a los delincuentes con el objetivo, si fuera posible, de la centralización de los juicios en un solo Estado miembro. Con este fin, los Estados miembros podrán recurrir a cualquier organismo o mecanismo establecido en la Unión Europea para facilitar la cooperación entre sus autoridades judiciales y la coordinación de su acción.
6. Los Estados miembros informarán a la Secretaría general del Consejo y la Comisión de su decisión de aplicar el apartado 3, indicando, si fuera necesario, los casos o circunstancias específicos en los cuales se aplica.

Artículo 12

Intercambio de información

1. A efectos del intercambio de información respecto a los delitos mencionados en los artículos 3, 4 y 5, y de acuerdo con las normas que regulan la protección de datos, los Estados miembros velarán por establecer puntos de contacto operativos disponibles ininterrumpidamente las 24 horas del día todos los días de la semana.
2. Los Estados miembros comunicarán a la Secretaría General del Consejo y a la Comisión los puntos de contacto designados para el intercambio de información respecto a los delitos relativos a los ataques contra los sistemas de información. La Secretaría General remitirá esta información a los otros Estados miembros.

Artículo 13

Aplicación

1. Los Estados miembros adoptarán las medidas necesarias para dar cumplimiento a la presente Decisión marco a más tardar el 31 de diciembre de 2003.
2. Comunicarán a la Secretaría General del Consejo y a la Comisión el texto de las disposiciones que adopten y la información relativa a las medidas adoptadas para cumplir con la presente Decisión marco.
3. Sobre esa base, la Comisión presentará, antes del 31 de diciembre de 2004, un informe al Parlamento Europeo y al Consejo sobre la aplicación de la presente Decisión marco, acompañada, en su caso, de propuestas legislativas.
4. El Consejo evaluará en qué medida los Estados miembros han cumplido con la presente Decisión marco.

Artículo 14

Entrada en vigor

La presente Decisión entrará en vigor el vigésimo día siguiente al de su publicación en el *Diario Oficial de las Comunidades Europeas*.

Hecho en Bruselas,

Por el Consejo
El Presidente