Propuesta de Decisión marco del Consejo relativa a los ataques de los que son objeto los sistemas de información

(2002/C 203 E/16)

COM(2002) 173 final — 2002/0086(CNS)

(Presentada por la Comisión el 19 de abril de 2002)

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 Comisión,

Visto el dictamen del Parlamento Europeo,

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 *e*Europa la Comunicación de la Comisión titulada «Seguridad de las redes y de la información: Propuesta para una perspectiva política europea» [1] 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 de 2001 [2], 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 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 justicia [3], 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 Comisión [4] y la Resolución del Parlamento Europeo de 19 de mayo de 2000 [5] 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» [6].

(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 el terrorismo y el crimen organizado.

---

[1] COM(2001) 298.

[2] [2001/2098(INI)].

[3] DO C 19 de 23.1.1999, p. 1.

[4] COM(2001) 278 final.

[5] A5-0127/2000.

[6] COM(2000) 890.

(8) La Decisión marco sobre la orden de detención europea, 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 terrorismo 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 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/JAI [1] 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 tengan 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 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.

[1] DO L 351 de 29.12.1998, p. 1.

Artículo 2

Definiciones

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 los siguientes actos intencionales sin autorización sean tipificodas 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 los 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. El Estado miembro 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 cuando 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*.