PARLAMENTO EUROPEO 2009 - 2014

Comisión de Libertades Civiles, Justicia y Asuntos de Interior

2010/0273(COD)

24.11.2011

***I
PROYECTO DE INFORME

sobre la propuesta de Directiva del Parlamento Europeo y del Consejo relativa a los ataques contra los sistemas de información, por la que se deroga la Decisión marco 2005/222/JAI del Consejo
(COM(2010)0517 – C7-0293/2010 – 2010/0273(COD))

Comisión de Libertades Civiles, Justicia y Asuntos de Interior

Ponente: Monika Hohlmeier

Explicación de los signos utilizados

*	Procedimiento de consulta
***	Procedimiento de aprobación
***I	Procedimiento legislativo ordinario (primera lectura)
***II	Procedimiento legislativo ordinario (segunda lectura)
***III	Procedimiento legislativo ordinario (tercera lectura)

(El procedimiento indicado se basa en el fundamento jurídico propuesto en el proyecto de acto.)

Enmiendas a un proyecto de acto

En las enmiendas del Parlamento las modificaciones introducidas en el proyecto de acto se señalan en ***cursiva negrita***. La utilización de la *cursiva fina* constituye una indicación para los servicios técnicos referente a elementos del proyecto de acto para los que se propone una corrección con miras a la elaboración del texto final (por ejemplo, elementos claramente erróneos u omitidos en alguna versión lingüística). Estas propuestas de corrección están supeditadas al acuerdo de los servicios técnicos interesados.

En las cabeceras de las enmiendas relativas a un acto existente que se quiere modificar con el proyecto de acto, figuran una tercera y cuarta líneas en las que se indican, respectivamente, el acto existente y la disposición en cuestión. Las partes retomadas de una disposición de un acto existente que el Parlamento desee modificar pero que no se hayan modificado en el proyecto de acto se señalarán en **negrita**. Las supresiones que se refieran a dichos pasajes se indicarán de la siguiente manera: **[...]**.

ÍNDICE

Página

PROYECTO DE RESOLUCIÓN LEGISLATIVA DEL PARLAMENTO EUROPEO

sobre la propuesta de Directiva del Parlamento Europeo y del Consejo relativa a los ataques contra los sistemas de información, por la que se deroga la Decisión marco 2005/222/JAI del Consejo
(COM(2010)0517 – C7-0293/2010 – 2010/0273(COD))

(Procedimiento legislativo ordinario: primera lectura)

El Parlamento Europeo,

– Vista la propuesta de la Comisión al Parlamento Europeo y al Consejo (COM(2010)0517),

– Vistos el artículo 294, apartado 2, y el artículo 83, apartado 1, del Tratado de Funcionamiento de la Unión Europea, conforme a los cuales la Comisión le ha presentado su propuesta (C7-0293/2010),

– Visto el artículo 294, apartado 3, del Tratado de Funcionamiento de la Unión Europea,

– Visto el dictamen del Comité Económico y Social Europeo, de 4 de mayo de 2011[1],

– Visto el artículo 55 de su Reglamento,

– Vistos el informe de la Comisión de Libertades Civiles, Justicia y Asuntos de Interior y las opiniones de la Comisión de Asuntos Exteriores y de la Comisión de Industria, Investigación y Energía (A7-0000/2011),

1. Aprueba la posición en primera lectura que figura a continuación;

2. Pide a la Comisión que le consulte de nuevo si se propone modificar sustancialmente su propuesta o sustituirla por otro texto;

3. Encarga a su Presidente que transmita la Posición del Parlamento al Consejo y a la Comisión, así como a los Parlamentos nacionales.

Enmienda 1

Propuesta de Directiva
Considerando 1

Texto de la Comisión	*Enmienda*
(1) El objetivo de la presente Directiva es aproximar las normas de Derecho penal de los Estados miembros en materia de ataques contra los sistemas de información,	(1) El objetivo de la presente Directiva es aproximar las normas de Derecho penal de los Estados miembros en materia de ataques contra los sistemas de información,

[1] DO C 218 de 23.7.2011, p. 130.

y mejorar la cooperación entre las autoridades judiciales y otras autoridades competentes, ***incluida*** la policía y ***los*** demás servicios represivos especializados de los Estados miembros.	y mejorar la cooperación entre las autoridades judiciales y otras autoridades competentes, ***incluyendo a*** la policía y demás servicios represivos especializados de los Estados miembros, ***así como a las agencias especializadas de la Unión***.

Or. en

Justificación

Dada la naturaleza transnacional de los ataques contra los sistemas de información es muy importante intensificar la cooperación entre las autoridades judiciales y policiales tanto de los Estados miembros como de la Unión Europea.

Enmienda 2

Propuesta de Directiva
Considerando 2

Texto de la Comisión	*Enmienda*
(2) Los ataques contra los sistemas de información, en particular los dirigidos por la delincuencia organizada, son una amenaza creciente, y cada vez preocupa más la posibilidad de atentados terroristas o con motivaciones políticas contra los sistemas de información que forman parte de las infraestructuras críticas de los Estados miembros y la Unión. Esta situación pone en peligro la realización de una sociedad de la información segura y de un espacio de libertad, seguridad y justicia y exige, por tanto, una respuesta por parte de la Unión Europea.	(2) Los ataques contra los sistemas de información, en particular los dirigidos por la delincuencia organizada, son una amenaza creciente, y cada vez preocupa más la posibilidad de atentados terroristas o con motivaciones políticas contra los sistemas de información que forman parte de las infraestructuras críticas de los Estados miembros y la Unión. ***Los atentados contra infraestructuras esenciales de información pueden tener importantes repercusiones transnacionales y perturbar o destruir servicios de vital importancia para la seguridad, la protección, la salud, la movilidad y el bienestar social y económico de los ciudadanos de la Unión, así como para el buen funcionamiento de infraestructuras de servicio público como las centrales energéticas, las redes de transporte y las redes de los órganos de gobernación.*** Esta situación pone en peligro la realización de una sociedad de la información segura y de un espacio de

libertad, seguridad y justicia y exige, por tanto, una respuesta por parte de la Unión Europea.

Or. en

Justificación

Es preciso destacar los posibles efectos y la magnitud de los ciberataques, en particular, cuando van dirigidos contra infraestructuras sensibles.

Enmienda 3

Propuesta de Directiva
Considerando 7 bis (nuevo)

Texto de la Comisión	*Enmienda*
	(7 bis) Teniendo en cuenta que la ocultación de la identidad real del autor de un acto y el prejuicio resultante para el titular legítimo son elementos importantes a la hora de determinar responsabilidades en el ámbito de aplicación de la presente Directiva, la Unión debe desarrollar un instrumento horizontal que abarque estas y otras transgresiones de un modo más detallado, abordando, entre otras cuestiones, la usurpación de identidades, haciendo hincapié, entre otros, en el derecho al propio nombre y en la protección del consumidor.

Or. en

Justificación

El encubrimiento de la identidad real de los infractores y los perjuicios causados al legítimo titular de la identidad usurpada son elementos importantes no solo para la persecución de actos delictivos en el ámbito de aplicación de esta Directiva. A medio plazo, estos y otros delitos afines deberán ser objeto de un instrumento horizontal de un alcance más general que trascienda las intromisiones en los sistemas de información.

Enmienda 4

Propuesta de Directiva
Considerando 8

Texto de la Comisión	*Enmienda*
(8) Las conclusiones del Consejo de 27 y 28 de noviembre indicaron que debía desarrollarse una nueva estrategia con los Estados miembros y la Comisión, teniendo en cuenta el contenido del Convenio del Consejo de Europa de 2001 sobre la ciberdelincuencia. Este Convenio es el marco jurídico de referencia para la lucha contra la ciberdelincuencia, incluidos los ataques contra los sistemas de información. La presente Directiva se basa en dicho Convenio.	(8) Las conclusiones del Consejo de 27 y 28 de noviembre indicaron que debía desarrollarse una nueva estrategia con los Estados miembros y la Comisión, teniendo en cuenta el contenido del Convenio del Consejo de Europa de 2001 sobre la ciberdelincuencia. Este Convenio es el marco jurídico de referencia para la lucha contra la ciberdelincuencia, incluidos los ataques contra los sistemas de información. La presente Directiva se basa en dicho Convenio. ***Por consiguiente es muy importante que los Estados miembros que no hayan ratificado aún el Convenio del Consejo de Europa sobre la ciberdelincuencia lo hagan tan pronto como sea posible.***

Or. en

Justificación

Habida cuenta de que el Convenio sobre la ciberdelincuencia es un instrumento básico del derecho internacional con relación a estos delitos, es conveniente pedir a los Estados miembros que, por razones de coherencia y como señal política, ratifiquen el Convenio, si no lo han hecho aún.

Enmienda 5

Propuesta de Directiva
Considerando 9

Texto de la Comisión	*Enmienda*
(9) Dadas las diferentes formas en que pueden realizarse los ataques y la rápida evolución de los programas y equipos informáticos, la presente Directiva se refiere a los «instrumentos» que pueden utilizarse para cometer las infracciones	(9) Dadas las diferentes formas en que pueden realizarse los ataques y la rápida evolución de los programas y equipos informáticos, la presente Directiva se refiere a los «instrumentos» que pueden utilizarse para cometer las infracciones

penales enumeradas en la presente Directiva. Estos instrumentos pueden ser, por ejemplo, programas informáticos nocivos, incluidos los botnets, que se utilizan para cometer ataques informáticos.	penales enumeradas en la presente Directiva. Estos instrumentos pueden ser, por ejemplo, programas informáticos nocivos, incluidos los botnets, que se utilizan para cometer ataques informáticos. ***Estas son solo algunas de las maneras de atacar sistemas de información. Sobre este telón de fondo es menester proseguir e intensificar el trabajo para una estrategia de la UE en materia de arquitecturas TI, en particular, la computación en nube, promoviendo la normalización técnica y el establecimiento de un marco legal común.***

Or. en

Justificación

Teniendo en cuenta el progreso tecnológico parece oportuno incluir una referencia a la computación en nube. Se requiere una mayor normalización técnica y un marco legal común europeo sobre computación en nube. De este modo se reforzará asimismo la posición de la UE como proveedor y como usuario de estructuras TI seguras y modernas.

Enmienda 6

Propuesta de Directiva
Considerando 9 bis (nuevo)

Texto de la Comisión	*Enmienda*
	(9 bis) El uso intencional no autorizado de un programa de ordenador concebido para eliminar pruebas de un delito con arreglo a la presente Directiva debe considerarse como un acto de connivencia o un delito penal independiente.

Or. en

Justificación

Considerando que aunque un programa de ordenador concebido para eliminar rastros de actividades delictivas no sea un instrumento con arreglo al artículo 7 de esta Directiva, su aplicación en la práctica favorece la realización de atentados cibernéticos. Por

consiguiente, los Estados miembros deben velar por que la utilización de tales programas se considere bien como un acto encubridor o como un delito penal independiente (por ejemplo, como obstrucción de una instrucción penal).

Enmienda 7

Propuesta de Directiva
Considerando 10

Texto de la Comisión	*Enmienda*
(10) La presente Directiva no pretende exigir responsabilidad penal cuando las infracciones se cometen de forma no intencionada, como en el caso de las pruebas ***autorizadas*** o la protección de los sistemas de información	(10) La presente Directiva no pretende exigir responsabilidad penal cuando las infracciones se cometen de forma no intencionada, pero el acto se cometa sin propósito delictivo, como en el caso de las pruebas ***acordes con la ley*** o la protección de los sistemas de información, ***o cuando la denegación de la autorización de acceso a un sistema constituiría un acto abusivo***.

Or. en

Justificación

El concepto de «prueba autorizada» podría interpretarse en el sentido de que fuera necesaria una autorización formal para poder efectuar una prueba de seguridad en sistemas de información propios. Con ello se socavaría la eficacia y viabilidad de tales pruebas sin propósito delictivo. Por otra parte, no debería haber presunción de delito cuando la limitación de acceso a un sistema contraviniere a su vez un precepto ilegal.

Enmienda 8

Propuesta de Directiva
Considerando 12 bis (nuevo)

Text proposed by the Commission	*Enmienda*
	(12a) Sobre el telón de fondo del establecimiento de una política de la Unión para la lucha contra la ciberdelincuencia, las conclusiones de los Consejos de 24 de octubre de 2008, de 27/28 de noviembre de 2008 y de 26 de abril de 2010 otorgaron a Europol el

cometido específico de contribuir al logro de este objetivo. A este fin, Europol debe crear y mantener una plataforma europea que sirva de punto de convergencia para las plataformas nacionales, con la misión, entre otras, de recoger y centralizar información sobre infracciones comprobadas por Internet. En ella se ha de incluir información sobre los infractores y su forma de operar. De conformidad con la Decisión del Consejo2009/371/JAI de 6 de abril de 2009 por la que se establece la Oficina Europea de Policía (Europol), concretamente las disposiciones sobre protección de datos personales del Capítulo V, y de conformidad también con la Decisión Marco del Consejo 2008/977/JAI de 27 de noviembre de 2008 relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal, la presente Directiva tiene en cuenta las tareas encomendadas a Europol.

_____

[1] DO L 121, 15.5.2009, p. 37.

[2] DO L 350, 30.12.2008, p. 60.

Or. en

Justification

Dada la naturaleza transnacional de los atentados contra los sistemas de información y habida cuenta de la misión de coordinación de Europol, conviene precisar el cometido de la agencia con respecto a los ataques cibernéticos. A este efecto, el Consejo Europeo ya ha proporcionado orientaciones útiles que se deberían tener en cuenta en el marco de esta Directiva.

Enmienda 9

Propuesta de Directiva
Considerando 12 ter (nuevo)

Texto de la Comisión	*Enmienda*
	(12 ter) Para combatir eficazmente la ciberdelincuencia es preciso incrementar la estabilidad de los sistemas informáticos protegiéndolos mejor contra los atentados. Particular importancia reviste en este contexto el establecimiento de normas mínimas para una adecuada protección de los sistemas de información. Los esfuerzos de la Unión y de sus Estados miembros contra la ciberdelicuencia solo podrán surtir efectos si la presente Directiva va asociada a medidas preventivas contra tales delitos, de conformidad con el artículo 67, apartado 3, y el artículo 84 del Tratado de Funcionamiento de la Unión Europea.

Or. en

Justificación

Aunque la legislación penal sea un importante elemento en la lucha contra la ciberdelincuencia, no deja de ser un último recurso, que entra en acción una vez se haya producido ya el atentado. Por este motivo, la UE debería incrementar sus esfuerzos por proteger sus sistemas en primer lugar, por ejemplo, mediante el establecimiento de estándares mínimos de protección de los sistemas de información.

Enmienda 10

Propuesta de Directiva
Considerando 12 quater (nuevo)

Texto de la Comisión	*Enmienda*
	(12 quater) Los Estados miembros deben entender la protección de sus sistemas de información y datos asociados como parte de su respectivo deber de protección. Se debe garantizar niveles razonables de protección frente a amenazas

razonablemente identificables. El coste y la servidumbre de esa protección deben ser proporcionales al riesgo de perjuicio para los afectados.

Or. en

Justificación

Los propios Estados miembros gestionan datos importantes y sensibles, como la información fiscal o los datos que obran en poder de los seguros de enfermedad. Su deber es proteger estos datos adecuadamente contra las intromisiones.

Enmienda 11

Propuesta de Directiva
Considerando 12 quinquies (nuevo)

Texto de la Comisión	*Enmienda*
	(12 quinquies) Los Estados miembros también deben adoptar las medidas oportunas para que las personas jurídicas tengan la obligación, en el ámbito de sus responsabilidades, de proteger datos de carácter personal encomendados a su custodia frente a las intromisiones a las que se refiere la presente Directiva. Se debe aplicar niveles razonables de protección frente a amenazas razonablemente identificables. El coste y la servidumbre de esa protección deben ser proporcionales a la magnitud del riesgo para los afectados. Cuando una persona jurídica no ha proporcionado los niveles adecuados de protección, y el perjuicio causado a raíz de esa ausencia de protección sea considerable, los Estados miembros deben garantizar que se puedan pedir responsabilidades a esta persona.

Or. en

Justificación

Cuando gestionen datos personales, las personas jurídicas tienen la responsabilidad de protegerlos adecuadamente contra riesgos razonablemente identificables. Si no proporcionaran ese nivel de protección, los Estados miembros deberían garantizar que se puedan exigir responsabilidades a dichas personas.

Enmienda 12

Propuesta de Directiva
Considerando 12 sexies (nuevo)

Texto de la Comisión	*Enmienda*
	(12 sexies) También es necesario consolidar e intensificar la cooperación entre proveedores de servicios, fabricantes, fuerzas del orden y autoridades judiciales, en el pleno respeto de la legalidad, a fin de afianzar, en particular, la seguridad jurídica y la previsibilidad y de garantizar la debida protección de personas bajo sospecha y personas inculpadas, sobre la base de la presunción de inocencia y el derecho de pedir resarcimiento por vía judicial. En este contexto se incluye, por ejemplo, la labor de asistencia de los proveedores de servicios en la desarticulación de sistemas o funciones ilegales.

Or. en

Justificación

La cooperación entre los servicios de los sectores privado y público es fundamental para combatir eficazmente los ciberataques.

Enmienda 13

Propuesta de Directiva
Considerando 12 septies (nuevo)

Texto de la Comisión	*Enmienda*
	(12 septies) Sin perjuicio de la cooperación voluntaria entre personas jurídicas, como los proveedores de servicios y los fabricantes, por una parte, y las autoridades judiciales por otra, los Estados miembros deben definir en qué casos la abstención de tomar medidas puede constituir en sí una conducta incriminable.

Or. en

Justificación

La falta de cooperación o la obstrucción de investigaciones penales por personas jurídicas son una cuestión muy conflictiva, en la medida en que pueden ser interpretadas como complicidad o connivencia con actos delictivos como los abarcados por la presente Directiva.

Enmienda 14

Propuesta de Directiva
Considerando 13

Texto de la Comisión	*Enmienda*
(13) Las diferencias y divergencias significativas que existen entre las legislaciones de los Estados miembros en este ámbito pueden dificultar la lucha contra la delincuencia organizada y el terrorismo y complicar la 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 los modernos sistemas de información significa que los ataques suelen revestir un carácter transfronterizo, lo que plantea la necesidad urgente de proseguir la aproximación de las	(13) Las diferencias y divergencias significativas que existen entre las legislaciones de los Estados miembros en este ámbito pueden dificultar la lucha contra la delincuencia organizada y el terrorismo y complicar la 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 los modernos sistemas de información significa que los ataques suelen revestir un carácter transfronterizo, lo que plantea la necesidad urgente de proseguir la aproximación de las

legislaciones penales en este ámbito. Por otra parte, la coordinación del enjuiciamiento de los casos de ataques contra los sistemas de información debe facilitarse con la adopción de la Decisión marco 2009/948/JAI del Consejo sobre la prevención y resolución de conflictos de ejercicio de jurisdicción en los procesos penales.	legislaciones penales en este ámbito. Por otra parte, la coordinación del enjuiciamiento de los casos de ataques contra los sistemas de información debe facilitarse ***mediante la adecuada transposición y aplicación*** de la Decisión marco 2009/948/JAI del Consejo sobre la prevención y resolución de conflictos de ejercicio de jurisdicción en los procesos penales.

Or. en

Justificación

Corrección lingüística.

Enmienda 15

Propuesta de Directiva
Considerando 13 bis (nuevo)

Texto de la Comisión	*Enmienda*
	(13 bis) Una mayor cooperación a escala de los órganos de ejecución de la ley y las autoridades judiciales en la Unión es fundamental para combatir eficazmente la ciberdelincuencia. A este respecto, la Comisión y los Estados miembros deben incrementar sus esfuerzos en pos de la adecuada formación de los cuerpos de ejecución de la ley y de las autoridades judiciales, con miras a elevar el nivel de comprensión de la naturaleza de la ciberdelincuencia y sus repercusiones, consolidar la cooperación y el intercambio de buenas prácticas, por ejemplo, en el marco de la Red Judicial Europea, con la coadyuvación de Europol, Eurojust y la Agencia Europea de Seguridad de las Redes y de la Información.

Or. en

Justificación

La adecuada formación de las personas encargadas de perseguir a autores de actos de ciberdelincuencia es fundamental para luchar contra estos delitos. Además, a escala de la UE existen cauces para mejorar esta cooperación e incrementar el nivel de preparación. Estos aspectos cobran más importancia, si cabe, en la medida en que los órganos policiales y judiciales se debaten entre sistemas legales que definen y tipifican estos delitos de maneras distintas. La mutua comprensión es fundamental, por lo tanto.

Enmienda 16

Propuesta de Directiva
Considerando 13 ter (nuevo)

Texto de la Comisión	*Enmienda*
	(13 ter) Esta formación y el intercambio de información contribuirán a agudizar la percepción de las diferencias entre los sistemas legales nacionales y de los problemas que se plantean en la instrucción penal a resultas de las distintas apreciaciones que hacen los sistemas nacionales con respecto a la gravedad del delito, como la gravedad del perjuicio, o el reparto de competencias entre los órganos nacionales de ejecución de la ley.

Or. en

Justificación

En la persecución de los ciberataques, los órganos policiales y judiciales se ven confrontados con sistemas legales que definen y tipifican los delitos de maneras distintas. La mutua comprensión es fundamental, por lo tanto.

Enmienda 17

Propuesta de Directiva
Artículo 2 – letra d

Texto de la Comisión	*Enmienda*
d) «sin autorización»: el acceso o la intromisión no autorizados por el	d) «sin autorización»: el acceso, ***la utilización*** o la intromisión no autorizados

propietario o titular de otro tipo de derecho sobre el sistema o parte del mismo o no permitidos por la legislación nacional.	por el propietario, o titular de otro tipo de derecho sobre el sistema o parte del mismo ***(en la medida en que la denegación de la autorización no constituya por sí misma un abuso de derecho),*** o no permitidos por la legislación nacional.

Or. en

Justificación

No deberá restringirse el libre flujo de información cuando su desaprobación vulneraría derechos reconocidos, como el derecho a la libertad de información. Por consiguiente, una desaprobación puede constituir una vulneración de derechos.

Enmienda 18

Propuesta de Directiva
Artículo 2 – letra d bis (nueva)

Texto de la Comisión	*Enmienda*
	d bis) «casos de menor gravedad» pueden ser aquellos, por ejemplo, en que el perjuicio y/o riesgo para intereses públicos o privados, tales como la integridad de un sistema de información o de datos informáticos, o para la integridad, derechos e intereses de un individuo, o bien sean de menor importancia o de naturaleza tal que no sea preciso, en función de los parámetros legales aplicables, imponer una sanción penal ni establecer responsabilidades penales;

Or. en

Justificación

El concepto de «casos de menor gravedad» es un elemento importante de esta Directiva, a la hora de determinar la gravedad de una infracción. Por motivos de seguridad jurídica es oportuno dar una definición del concepto.

Enmienda 19

Propuesta de Directiva
Artículo 2 – letra d ter (nueva)

Texto de la Comisión	*Enmienda*
	d ter) «sistema de una infraestructura crítica de información»: el sistema de información de una infraestructura esencial para funciones sociales vitales en los ámbitos de la salud, la protección, la seguridad y el bienestar social y económico de la población, y cuya inoperancia o anulación afectaría gravemente a un Estado miembro, por privarle de la posibilidad de mantener esas funciones;

Or. en

Justificación

En interés de la seguridad jurídica conviene aclarar qué se entiende por «sistema de una infraestructura crítica de información». El Libro Verde de la Comisión COM(2005)576, así como las Comunicaciones COM(2011)163 y COM(2009)149 sobre protección de infraestructuras críticas de información ofrecen indicaciones válidas a este respecto.

Enmienda 20

Propuesta de Directiva
Artículo 3

Texto de la Comisión	*Enmienda*
Los Estados miembros adoptarán las medidas necesarias para que el acceso intencionado, sin autorización, ***al*** conjunto o a una parte de un sistema de información sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad.	Los Estados miembros adoptarán las medidas necesarias para que el acceso intencionado, sin autorización, ***en el sentido de intromisión en el*** conjunto o a una parte de un sistema de información sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad. ***Cada Estado miembro podrá establecer que un acto mencionado en el apartado 1 solo sea objeto de acciones judiciales cuando la infracción se cometa***

transgrediendo medidas de seguridad.

Or. en

Justificación

En aras de la seguridad jurídica es oportuno incluir esta precisión del alcance de la palabra «acceso». Asimismo, el concepto del acceso ilegal debería implicar la transgresión de medidas de seguridad. En caso contrario, el acceso no autorizado a una red WiFi abierta tendría que considerarse una infracción.

Enmienda 21

Propuesta de Directiva
Artículo 6

Texto de la Comisión	*Enmienda*
Los Estados miembros adoptarán las medidas necesarias para garantizar que la interceptación intencionada, por medios técnicos, de transmisiones no públicas de datos informáticos hacia, desde o dentro de un sistema de información, incluidas las emisiones electromagnéticas de un sistema de información que contenga dichos datos informáticos, se castigue como una infracción penal cuando se cometa sin autorización.	Los Estados miembros adoptarán las medidas necesarias para garantizar que la interceptación intencionada, por medios técnicos, de transmisiones no públicas de datos informáticos hacia, desde o dentro de un sistema de información, incluidas las emisiones electromagnéticas de un sistema de información que contenga dichos datos informáticos, se castigue como una infracción penal cuando se cometa sin autorización, ***al menos cuando se trate de casos de menor gravedad***. ***La interceptación por medios técnicos abarca la escucha, el seguimiento y el análisis del contenido de comunicaciones con el propósito de apoderarse del contenido de los datos bien directamente, mediante el acceso y recurso a ese sistema de información, o indirectamente, por medio de sistemas de interceptación y grabación electrónicos. La interceptación podrá estar unida a la grabación.*** ***Entre los medios técnicos se incluyen sistemas conectados a las líneas de transmisión, así como sistemas que permiten obtener y grabar comunicaciones inalámbricas, incluso mediante el uso de programas informáticos y de claves y códigos de***

acceso.

Or. en

Justificación

Por coherencia con lo precisado en los artículos 3 a 5, tampoco este artículo debería incluir entre las infracciones penales los casos de menor gravedad. Asimismo parece oportuno definir la palabra «interceptación». El informe explicativo del Convenio sobre la ciberdelincuencia ofrece elementos útiles a este respecto en su apartado 53. En aras de la seguridad jurídica conviene aclarar qué se entiende por una «medida técnica». El informe explicativo del Convenio sobre la ciberdelincuencia ofrece una definición útil a este respecto en la segunda parte de su apartado 53.

Enmienda 22

Propuesta de Directiva
Artículo 7

Texto de la Comisión	*Enmienda*
Los Estados miembros adoptarán las medidas necesarias para garantizar que la producción, venta, adquisición para el uso, importación, ***posesión,*** distribución u otra forma de puesta a disposición de los siguientes elementos se castiguen como infracciones penales cuando sean intencionadas y se realicen sin autorización con ***el fin*** de cometer cualquiera de las infracciones mencionadas en los artículos 3 a 6:	Los Estados miembros adoptarán las medidas necesarias para garantizar que la producción, venta, adquisición para el uso, importación, distribución u otra forma de puesta a disposición de los siguientes elementos se castiguen como infracciones penales cuando sean intencionadas y se realicen sin autorización con ***la intención clara*** de cometer cualquiera de las infracciones mencionadas en los artículos 3 a 6:

Or. en

Justificación

Dada la posibilidad de utilizar programas de doble uso, con fines legales y fines no legales, la posesión en si de tales herramientas no debería considerarse como punible. Además, el propósito de las acciones a las que se refiere este artículo solo es punible si la acción se lleva a efecto con el claro propósito de cometer una infracción.

Enmienda 23

Propuesta de Directiva
Artículo 7 – letra a

Texto de la Comisión	*Enmienda*
a) ***un dispositivo, incluido*** un programa informático, concebido o adaptado ***principalmente para*** cometer una infracción de las mencionadas en los artículos 3 a 6;	a) un programa informático, concebido o adaptado ***con el claro propósito de*** cometer una infracción de las mencionadas en los artículos 3 a 6;

Or. en

Justificación

La palabra «dispositivo» puede resultar equívoca, puesto que se podría referirse sencillamente a un producto de hardware, como un ordenador o una cámara. Por consiguiente parece aconsejable no usarla. La expresión «principalmente», por otra parte, no es suficientemente explícita; se propone precisarla haciendo referencia al «claro propósito» perseguido.

Enmienda 24

Propuesta de Directiva
Artículo 8 – título

Texto de la Comisión	*Enmienda*
Inducción, complicidad y tentativa	***Incitación***, ***connivencia y*** complicidad, y tentativa

Or. en

Justificación

Corrección lingüística.

Enmienda 25

Propuesta de Directiva
Artículo 8 – apartado 1

Texto de la Comisión	*Enmienda*
1. Los Estados miembros garantizarán que la ***inducción y la*** complicidad en relación con las infracciones mencionadas en los artículos 3 a 7 sean punibles como infracciones penales.	1. Los Estados miembros garantizarán que la ***incitación, connivencia o*** complicidad en relación con las infracciones mencionadas en los artículos 3 a 7 sean punibles como infracciones penales.

Or. en

Justificación

Corrección lingüística.

Enmienda 26

Propuesta de Directiva
Artículo 9 – apartado 1

Texto de la Comisión	*Enmienda*
1. Los Estados miembros adoptarán las medidas necesarias para garantizar que las infracciones mencionadas en los artículos 3 a 8 se castiguen con sanciones penales eficaces, ***proporcionadas*** y disuasorias.	1. Los Estados miembros adoptarán las medidas necesarias para garantizar que las infracciones mencionadas en los artículos 3 a 8 se castiguen con sanciones penales eficaces, ***proporcionales*** y disuasorias.

Or. en

Justificación

Corrección lingüística.

Enmienda 27

Propuesta de Directiva
Artículo 10 – apartado 1

Texto de la Comisión	*Enmienda*
1. Los Estados miembros adoptarán las medidas necesarias para garantizar que las infracciones mencionadas en los ***artículos 3 a 7*** se castiguen con sanciones penales privativas de libertad de una duración máxima de al menos cinco años cuando se cometan en el contexto de una organización delictiva tal como se define en la Directiva marco 2008/841/JAI.	1. Los Estados miembros adoptarán las medidas necesarias para garantizar que las infracciones mencionadas en los ***artículos 4 a 7*** se castiguen con sanciones penales privativas de libertad de una duración máxima de al menos cinco años cuando se cometan en el contexto de una organización delictiva tal como se define en la Directiva marco 2008/841/JAI. ***En ese caso no serán aplicables las sanciones penales con arreglo a la Decisión marco.***

Or. en

Justificación

El artículo 3 de la Decisión marco 2008/841/JAI prevé penas entre dos y cinco años de privación de libertad por delitos cometidos en colaboración con una organización delictiva, mientras que el artículo 10 de la propuesta prevé penas de una duración máxima de al menos cinco años de cárcel. En aras de la seguridad jurídica conviene aclarar qué niveles penales se aplican en caso de delitos cometidos en colaboración con una organización criminal.

Enmienda 28

Propuesta de Directiva
Artículo 10 – apartado 2

Texto de la Comisión	*Enmienda*
2. Los Estados miembros adoptarán las medidas necesarias para garantizar que las infracciones mencionadas en los ***artículos 3 a 6*** se castiguen con sanciones penales privativas de libertad de una duración máxima de al menos cinco años cuando se cometan utilizando un instrumento concebido para lanzar ataques que afecten a un número significativo de sistemas de información o ataques que causen ***daños considerables*** como la interrupción de los	2. Los Estados miembros adoptarán las medidas necesarias para garantizar que las infracciones mencionadas en los ***artículos 4 a 6*** se castiguen con sanciones penales privativas de libertad de una duración máxima de al menos cinco años cuando se cometan utilizando un instrumento concebido para lanzar ataques que afecten a un número significativo de sistemas de información o ataques que causen ***daños graves*** como la interrupción de los

servicios del sistema, costes económicos o pérdida de datos personales.	servicios del sistema, costes económicos o pérdida de datos personales, ***o estén dirigidos contra una infraestructura crítica de información.***

Or. en

Justificación

Los artículos 4 a 6 se refieren a delitos que se consideran particularmente graves cuando se cometen a gran escala y provocan serios daños, o cuando se dirigen contra una infraestructura esencial de información.

Enmienda 29

Propuesta de Directiva
Artículo 14 – título

Texto de la Comisión	*Enmienda*
Intercambio de información	Intercambio de información ***y cooperación***

Or. en

Justificación

En virtud de las enmiendas que siguen, el ámbito de aplicación de este artículo se hace extensivo a la cooperación. Por consiguiente, el título de este epígrafe deberá modificarse.

Enmienda 30

Propuesta de Directiva
Artículo 14 – apartado 1

Texto de la Comisión	*Enmienda*
1. A efectos del intercambio de información sobre las infracciones mencionadas en los artículos 3 a 8, y de acuerdo con las normas de protección de datos, los Estados miembros harán uso de la red existente de puntos de contacto operativos disponibles las 24 horas del día los 7, días de la semana. Los Estados miembros también se asegurarán de que	1. A efectos del intercambio de información sobre las infracciones mencionadas en los artículos 3 a 8, y de acuerdo con las normas de protección de datos, los Estados miembros harán uso de la red existente de puntos de contacto operativos disponibles las 24 horas del día los 7, días de la semana. Los Estados miembros también se asegurarán de que

existan procedimientos disponibles para responder a solicitudes urgentes en un plazo máximo de ocho horas. La respuesta deberá indicar al menos si se atenderá la solicitud de ayuda, así como la forma y el plazo en que se hará.	existan procedimientos disponibles para responder a solicitudes urgentes en un plazo máximo de ocho horas ***indicando*** si se atenderá la solicitud de ayuda, así como la forma y el plazo en que se hará. ***Ese intercambio de información no supondrá menoscabo para las normas nacionales de los Estados miembros sobre recopilación y admisibilidad de pruebas por cuanto concierne al uso de tales informaciones en procedimientos penales posteriores.***

Or. en

Justificación

Aunque el rápido intercambio de información y la mutua asistencia sean elementos fundamentales en la lucha común contra los ciberataques transnacionales, estas disposiciones no afectan a la cuestión de la admisibilidad de pruebas en procedimientos penales posteriores.

Enmienda 31

Propuesta de Directiva
Artículo 14 – apartado 2 bis (nuevo)

Texto de la Comisión	*Enmienda*
	2 bis. Para el intercambio de la información relativa a los delitos enunciados en los artículos 3 a 8, los Estados miembros, de conformidad con las normas sobre protección de datos, establecerán redes de cooperación y colaboración con proveedores de servicios y fabricantes.

Or. en

Justificación

Además de la cooperación entre las autoridades, a fin de poder combatir eficazmente los ciberataques e incrementar la estabilidad de las redes, bien sean públicas o privadas, es muy importante incrementar la cooperación entre el sector privado y las autoridades públicas.

Enmienda 32

Propuesta de Directiva
Artículo 15 – apartado 3

Texto de la Comisión	*Enmienda*
3. Los Estados miembros transmitirán a la Comisión los datos recogidos con arreglo al presente artículo. ***También garantizarán*** la publicación de una revisión consolidada de sus informes estadísticos.	3. Los Estados miembros transmitirán a la Comisión ***y a la Agencia Europea de Seguridad de las Redes y de la Información*** los datos recogidos con arreglo al presente artículo***, con miras a evaluar la situación con respecto a la seguridad de las redes y de la información de conformidad con el Reglamento (CE) n° 468/2004 del Parlamento Europeo y del Consejo de 10 de marzo de 2004 por el que se crea la Agencia Europea de Seguridad de las Redes y de la Información.*** ***Los Estados miembros también transmitirán a Europol datos estadísticos y otros datos útiles relativos al modo de actuación de los autores de los delitos, a efectos de evaluaciones de amenazas y de análisis estratégicos de la ciberdelincuencia, de conformidad con la Decisión del Consejo 2009/371/JAI.*** ***La Comisión, en colaboración con los Estados miembros, garantizará*** la publicación de una revisión consolidada de sus informes estadísticos. **_____** ***[1] DO L 77 de 13.3.2004, p. 1.***

Or. en

Justificación

Habida cuenta de la naturaleza transnacional de los ataques de que son objeto los sistemas de información y de sus posibles efectos a escala de la Unión, será preciso hacer partícipes en mayor medida a la Agencia Europea de Seguridad de las Redes y de la Información y a Europol en la evaluación de los datos relevantes. De conformidad con las orientaciones fijadas por el Consejo Europeo, para poder cumplir con sus cometidos, Europol debe recibir datos, en particular, sobre el modo de actuación de los infractores.

Enmienda 33

Propuesta de Directiva
Artículo 18 – apartado 1

Texto de la Comisión	*Enmienda*
1. Antes del [CUATRO AÑOS DESDE SU ADOPCIÓN] y, a continuación, cada tres años, la Comisión presentará al Parlamento Europeo y al Consejo un informe sobre la aplicación de la presente Directiva en los Estados miembros que incluirá las propuestas necesarias.	1. Antes del [CUATRO AÑOS DESDE SU ADOPCIÓN] y, a continuación, cada tres años, la Comisión presentará al Parlamento Europeo y al Consejo un informe sobre la aplicación de la presente Directiva en los Estados miembros que incluirá las propuestas necesarias. ***En el marco de dicho informe de revisión, la Comisión deberá tener en cuenta el progreso técnico y legal en el ámbito de la ciberdelincuencia, en particular, con respecto al ámbito de aplicación de la presente Directiva.***

Or. en

Justificación

Teniendo en cuenta el rápido progreso de las tecnologías cibernéticas parece obligado verificar regularmente si el contenido reglamentario de la presente Directiva aún cubre las posibilidades técnicas del momento, y también, si cambios en el ordenamiento jurídico, inclusive a escala de la UE, repercuten sobre el ámbito cubierto por la Directiva, por ejemplo, con relación a una futura política de la UE sobre la computación en nube.