



PARLAMENTO EUROPEO

2009 - 2014

Comisión de Libertades Civiles, Justicia y Asuntos de Interior

2013/0027(COD)

15.1.2014

OPINIÓN

de la Comisión de Libertades Civiles, Justicia y Asuntos de Interior

para la Comisión de Mercado Interior y Protección del Consumidor

sobre la propuesta de Directiva del Parlamento Europeo y del Consejo relativa a medidas para garantizar un elevado nivel común de seguridad de las redes y de la información en la Unión
(COM(2013)0048 – C7-0035/2013 – 2013/0027(COD))

Ponente (de opinión): Carl Schlyter

PA_Legam

BREVE JUSTIFICACIÓN

El objetivo de la propuesta es garantizar un elevado nivel común de seguridad de las redes y de la información. El ponente apoya los objetivos de la propuesta, recomendando enmiendas que mejorarán la seguridad jurídica y reforzarán las salvaguardias y protecciones de los ciudadanos y de su intimidad para garantizar que estos asuman el control de sus datos personales y confíen en el entorno digital, y para crear una cultura de gestión del riesgo y de mejora de la información compartida entre los sectores privado y público.

Las enmiendas propuestas se refieren al refuerzo de la referencia a la legislación sobre protección de datos, aclarando que «las infraestructuras críticas» no deben incluir las redes sociales ni las tiendas de aplicaciones (véase la lista del anexo II modificada) y asegurándose de que se respete la proporcionalidad subrayando el aspecto civil de la empresa: la mayor parte de los problemas y causas comunes de los fallos sistémicos no son ataques cibernéticos intencionales causados por terroristas, delincuentes o espías extranjeros, sino errores humanos y causas naturales no premeditados. Es de suma importancia que la UE distinga entre la aplicación de la legislación propuesta y cualquier militarización del asunto, excluyendo los objetivos de seguridad y vigilancia de la industria, teniendo en cuenta el contexto de un mercado digital globalizado.

Siguen constituyendo un importante motivo de preocupación la relación entre el sistema propuesto y el sistema de notificación propuesto con arreglo al Reglamento general sobre protección de datos, y su coexistencia efectiva, que es una de las razones que destacan el hecho de que toda legislación de la UE en materia de seguridad cibernética debe seguir a la aprobación del Reglamento general sobre protección de datos y no precederla. Además, deben tenerse en cuenta las verdaderas implicaciones financieras y administrativas, incluidos los costes sociales totales y no solo los costes de una notificación. Las empresas de programas informáticos que elaboran programas descuidados para ahorrar dinero, exponiendo así a sus clientes a riesgos, no pueden estar protegidas en todos los casos por la norma que figura en las condiciones de uso y que excluye su responsabilidad en caso de funcionamiento defectuoso de sus programas. Hay que incentivarlas para asegurarse de que sus programas son razonablemente seguros. Por último deben aclararse conceptos fundamentales para no dejarlos a la libre interpretación de los Estados miembros (como el significado de «administraciones públicas» y de «efecto significativo» y una definición concreta de «ciberdelincuencia»).

ENMIENDAS

La Comisión de Libertades Civiles, Justicia y Asuntos de Interior pide a la Comisión de Mercado Interior y Protección del Consumidor, competente para el fondo, que incorpore en su informe las siguientes enmiendas:

Enmienda 1

Propuesta de Directiva

Considerando 1

Texto de la Comisión

(1) Las redes y los sistemas y servicios de información desempeñan un papel crucial en la sociedad. Su fiabilidad y seguridad son esenciales para la actividad económica y el bienestar social y, ***en particular, para el funcionamiento del mercado interior.***

Enmienda

(1) Las redes y los sistemas y servicios de información desempeñan un papel crucial en la sociedad. Su fiabilidad y seguridad son esenciales para la actividad económica, el bienestar social y ***las comunicaciones y los intercambios entre personas, organizaciones de la sociedad civil y empresas, así como para la protección y el respeto de la intimidad y los datos personales.***

Enmienda 2

Propuesta de Directiva **Considerando 2**

Texto de la Comisión

(2) La magnitud y la frecuencia de los incidentes de seguridad, ya sean deliberados o accidentales, se están incrementando y representan una grave amenaza para el funcionamiento de las redes y los sistemas de información. Tales incidentes pueden interrumpir las actividades económicas, generar considerables pérdidas financieras, minar la confianza del usuario y causar grandes daños a la economía de la Unión.

Enmienda

(2) La magnitud y la frecuencia de los incidentes de seguridad, ya sean deliberados o accidentales, se están incrementando y representan una grave amenaza para el funcionamiento de las redes y los sistemas de información. Tales incidentes pueden interrumpir las actividades económicas, generar considerables pérdidas financieras, minar la confianza del usuario y causar grandes daños a la economía de la Unión. ***Se reconoce cada vez más que los sistemas de control son vulnerables a los ataques cibernéticos procedentes de numerosas fuentes, incluidos gobiernos hostiles, grupos terroristas y otros intrusos malintencionados. Los ataques inteligentes y los ataques coordinados podrían tener graves repercusiones para la estabilidad, el rendimiento y los aspectos económicos de la infraestructura.***

Enmienda 3

Propuesta de Directiva Considerando 3

Texto de la Comisión

(3) Al ser instrumentos de comunicación sin fronteras, los sistemas de información digitales —y sobre todo Internet— contribuyen decisivamente a facilitar la circulación transfronteriza de bienes, servicios y personas. Dado su carácter transnacional, una perturbación grave de esos sistemas en un Estado miembro puede afectar también a otros Estados miembros y a la Unión en su conjunto. Por consiguiente, la resiliencia y la estabilidad de las redes y los sistemas de información son fundamentales para el correcto funcionamiento del mercado interior.

Enmienda

(3) Al ser instrumentos de comunicación sin fronteras, los sistemas de información digitales —y sobre todo Internet— contribuyen decisivamente a facilitar la circulación transfronteriza de bienes, servicios y personas. Dado su carácter transnacional, una perturbación grave de esos sistemas en un Estado miembro puede afectar también a otros Estados miembros y a la Unión en su conjunto. Por consiguiente, la resiliencia y la estabilidad de las redes y los sistemas de información son fundamentales para el correcto funcionamiento del mercado interior **y para las comunicaciones y los intercambios entre personas, organizaciones de la sociedad civil y empresas.**

Enmienda 4

Propuesta de Directiva Considerando 3 bis (nuevo)

Texto de la Comisión

Enmienda

(3 bis) Puesto que las causas más comunes de los fallos sistémicos siguen siendo involuntarias, como las causas naturales o los errores humanos, las infraestructuras deben poder resistir tanto a perturbaciones intencionales como no intencionales, y los operadores de infraestructuras críticas deben diseñar sistemas basados en la resistencia que sean operativos incluso cuando fallen otros sistemas que estén fuera de su control.

Enmienda 5

Propuesta de Directiva Considerando 6 bis (nuevo)

Texto de la Comisión

Enmienda

(6 bis) Es vital reconocer la incertidumbre inherente a los complejos sistemas que nos mantienen. Ello exige una mejor comprensión común de lo que es crítico, entre quienes protegen una organización y quienes fijan su dirección estratégica.

Enmienda 6

Propuesta de Directiva Considerando 8

Texto de la Comisión

Enmienda

(8) Las disposiciones de la presente Directiva no han de obstar para que los Estados miembros adopten las medidas necesarias para asegurar la protección de sus intereses esenciales en materia de seguridad, salvaguardar el orden público y la seguridad pública, y permitir la investigación, detección y represión de delitos. De conformidad con el artículo 346 del TFUE, ningún Estado miembro debe estar obligado a facilitar información cuya divulgación considere contraria a los intereses esenciales de su seguridad.

(8) Las disposiciones de la presente Directiva no han de obstar para que los Estados miembros adopten las medidas necesarias para asegurar la protección de sus intereses esenciales en materia de seguridad, salvaguardar el orden público y la seguridad pública, y permitir la investigación, detección y represión de delitos, ***a condición de que ello no les sirva de pretexto para no cumplir sus obligaciones más generales en materia de respeto de la protección de la intimidad y los datos personales.*** De conformidad con el artículo 346 del TFUE, ningún Estado miembro debe estar obligado a facilitar información cuya divulgación considere contraria a los intereses esenciales de su seguridad.

Enmienda 7

Propuesta de Directiva Considerando 9

Texto de la Comisión

(9) A fin de alcanzar y mantener un elevado nivel común de seguridad de las redes y los sistemas de información, los Estados miembros deben disponer de sendas estrategias nacionales de SRI que fijen los objetivos estratégicos y las medidas concretas que haya que aplicar. Deben elaborarse a escala nacional planes de cooperación en el ámbito de la SRI que cumplan los requisitos esenciales para así lograr niveles de capacidad de respuesta que hagan posible una cooperación efectiva y eficaz a escala nacional y de la Unión ante los incidentes que se produzcan.

Enmienda

(9) A fin de alcanzar y mantener un elevado nivel común de seguridad de las redes y los sistemas de información, los Estados miembros deben disponer de sendas estrategias nacionales de SRI que fijen los objetivos estratégicos y las medidas concretas que haya que aplicar. Deben elaborarse a escala nacional planes de cooperación en el ámbito de la SRI que cumplan los requisitos esenciales para así lograr niveles de capacidad de respuesta que hagan posible una cooperación efectiva y eficaz a escala nacional y de la Unión ante los incidentes que se produzcan, ***respetando y protegiendo la intimidad y los datos personales.***

Enmienda 8

**Propuesta de Directiva
Considerando 10**

Texto de la Comisión

(10) Con miras a una aplicación efectiva de las disposiciones adoptadas de conformidad con la presente Directiva, procede crear o designar en cada uno de los Estados miembros ***un organismo*** que coordine las cuestiones relacionadas con la SRI y actúe como centro de referencia nacional a efectos de cooperación transfronteriza a escala de la Unión. Estos organismos deben disponer de recursos técnicos, financieros y humanos suficientes para poder desempeñar efectiva y eficazmente las tareas que se les encomienden y alcanzar de este modo los objetivos de la presente Directiva.

Enmienda

(10) Con miras a una aplicación efectiva de las disposiciones adoptadas de conformidad con la presente Directiva, procede crear o designar en cada uno de los Estados miembros ***una autoridad nacional competente bajo control civil con pleno control democrático y transparencia en sus operaciones*** que coordine las cuestiones relacionadas con la SRI y actúe como centro de referencia nacional a efectos de cooperación transfronteriza a escala de la Unión. Estos organismos deben disponer de recursos técnicos, financieros y humanos suficientes para poder desempeñar efectiva y eficazmente las tareas que se les encomienden y alcanzar de este modo los objetivos de la presente Directiva.

Enmienda 9

Propuesta de Directiva Considerando 14 bis (nuevo)

Texto de la Comisión

Enmienda

(14 bis) Aumenta el número de sectores que adoptan servicios en la nube en su entorno informático, como los servicios informáticos que utilizan infraestructuras críticas. Hay que prever medidas de seguridad suficientes para garantizar la confidencialidad, la integridad y la disponibilidad de los datos en la nube. El alojamiento de servicios de infraestructuras y el almacenamiento de datos sensibles en la nube implican requisitos de seguridad y resistencia que los actuales servicios en la nube no pueden abordar. Por ello, es necesaria una garantía de que el entorno de computación en nube pueda ofrecer una protección completa de los datos sobre infraestructuras críticas sensibles.

Enmienda 10

Propuesta de Directiva Considerando 15

Texto de la Comisión

Enmienda

(15) La cooperación entre los sectores público y privado reviste importancia esencial por cuanto la mayor parte de las redes y sistemas de información es de titularidad privada. Conviene alentar a los operadores del mercado a crear sus propios mecanismos de cooperación informal para garantizar la SRI. Asimismo, los operadores deben cooperar con el sector público e intercambiar información y mejores prácticas **a cambio de obtener** apoyo operativo en caso de que se produzcan incidentes.

(15) La cooperación entre los sectores público y privado reviste importancia esencial por cuanto la mayor parte de las redes y sistemas de información es de titularidad privada. Conviene alentar a los operadores del mercado a crear sus propios mecanismos de cooperación informal para garantizar la SRI. Asimismo, los operadores deben cooperar con el sector público e intercambiar **mutuamente** información y mejores prácticas **así como** apoyo operativo **recíproco cuando sea necesario** en caso de que se produzcan incidentes.

Enmienda 11

Propuesta de Directiva Considerando 15 bis (nuevo)

Texto de la Comisión

Enmienda

(15 bis) Los actuales mecanismos nacionales de cooperación entre operadores privados y públicos deben respetarse plenamente, en la medida de lo posible y de conformidad con la Directiva 95/46/CE, y las disposiciones estipuladas en la presente Directiva no deben socavar este tipo de acuerdos de cooperación establecidos.

Enmienda 12

Propuesta de Directiva Considerando 16

Texto de la Comisión

Enmienda

(16) Para garantizar la transparencia e informar debidamente a los ciudadanos y operadores del mercado de la UE, conviene que las autoridades competentes creen un sitio web común para publicar información no confidencial sobre incidentes y riesgos.

(16) Para garantizar la transparencia e informar debidamente a los ciudadanos y operadores del mercado de la UE, conviene que las autoridades competentes creen un sitio web común para publicar **rápidamente** información no confidencial **integral** sobre incidentes y riesgos.

Enmienda 13

Propuesta de Directiva Considerando 21

Texto de la Comisión

Enmienda

(21) El alcance mundial de los problemas de SRI hace necesaria una mayor cooperación internacional con miras a mejorar las normas de seguridad y el intercambio de información, y promover

(21) El alcance mundial de los problemas de SRI hace necesaria una mayor cooperación internacional con miras a mejorar las normas de seguridad y el intercambio de información, y promover

un planteamiento mundial común con respecto a las cuestiones de SRI.

un planteamiento mundial común con respecto a las cuestiones de SRI, **a condición de que los Estados con los que se prevé esta cooperación estén dotados de instrumentos de control y de protección de datos que garanticen la misma seguridad que los de la UE.**

Enmienda 14

Propuesta de Directiva Considerando 22

Texto de la Comisión

(22) La responsabilidad de velar por la SRI recae en gran medida en las administraciones públicas y **los operadores del mercado**. Debe fomentarse una cultura de gestión de riesgos que entrañe una evaluación del riesgo y la aplicación de medidas de seguridad **proporcionales a los riesgos existentes** y que habrá de desarrollarse a través de requisitos reglamentarios adecuados y prácticas voluntarias del sector. Asimismo, son necesarias condiciones uniformes para garantizar el funcionamiento efectivo de la red de cooperación y, por ende, una colaboración eficaz de todos los Estados miembros.

Enmienda

(22) La responsabilidad de velar por la SRI recae en gran medida en las administraciones públicas y **las empresas**. Debe fomentarse una cultura de gestión de riesgos que entrañe una evaluación del riesgo y la aplicación de medidas de seguridad **dirigidas a prevenir los incidentes de seguridad, ya sean deliberados o accidentales**, y que habrá de desarrollarse a través de requisitos reglamentarios adecuados y prácticas voluntarias del sector. **Si ya existe tal cultura de gestión de riesgos y, en particular, si se basa en prácticas voluntarias, debe apoyarse, reforzarse y compartirse**. Asimismo, son necesarias condiciones uniformes para garantizar el funcionamiento efectivo de la red de cooperación y, por ende, una colaboración eficaz de todos los Estados miembros.

Enmienda 15

Propuesta de Directiva Considerando 22 bis (nuevo)

Texto de la Comisión

Enmienda

(22 bis) Las administraciones públicas y las empresas privadas, incluidos los proveedores de servicios de redes y de

información y programas, deben considerar la protección de sus sistemas de información y de los datos que contengan como parte de su obligación de diligencia. Es menester garantizar niveles adaptados de protección frente a amenazas y sectores vulnerables razonablemente identificables. Los costes y las cargas de esa protección deben reflejar el posible riesgo de ciberataque para los afectados.

Enmienda 16

Propuesta de Directiva Considerando 26 bis (nuevo)

Texto de la Comisión

Enmienda

(26 bis) Los niños están expuestos a Internet y otras tecnologías modernas, así como a las amenazas que proceden de ellas, desde muy jóvenes. Una buena gestión de un espacio en línea favorable a los niños es crucial para mitigar los daños y garantizar que no se comprometan la protección de los niños y sus derechos.

Enmienda 17

Propuesta de Directiva Considerando 28

Texto de la Comisión

Enmienda

(28) Las autoridades competentes deben procurar que se mantengan los canales de intercambio de información informales y de confianza entre los operadores del mercado y entre los sectores público y privado. **Antes de dar publicidad a** los incidentes notificados a las autoridades competentes, **es preciso sopesar debidamente el** interés de los ciudadanos en ser informados sobre las amenazas existentes **y los perjuicios que en términos**

(28) Las autoridades competentes deben procurar que se mantengan los canales de intercambio de información informales y de confianza entre los operadores del mercado y entre los sectores público y privado. **En la publicidad de** los incidentes notificados a las autoridades competentes **debe darse prioridad, por encima de las consideraciones económicas a corto plazo,** al interés de los ciudadanos en ser

comerciales y de reputación puedan sufrir las administraciones públicas y los operadores del mercado que notifican los incidentes. A la hora de cumplir sus obligaciones de notificación, las autoridades competentes han de tener muy en cuenta la necesidad de mantener estrictamente confidencial la información sobre los puntos vulnerables del producto antes de dar a conocer las soluciones de seguridad adecuadas.

informados sobre las amenazas existentes.

Enmienda 18

Propuesta de Directiva Considerando 29 bis (nuevo)

Texto de la Comisión

Enmienda

(29 bis) Un uso fraudulento de Internet permite a la delincuencia organizada ampliar sus actividades en línea para el blanqueo de dinero, la falsificación y otros productos y servicios que violan los derechos de propiedad intelectual, así como para experimentar con nuevas actividades criminales, lo que refleja una temible habilidad para adaptarse a las tecnologías modernas.

Enmienda 19

Propuesta de Directiva Considerando 30 bis (nuevo)

Texto de la Comisión

Enmienda

(30 bis) La delincuencia informática causa daños económicos y sociales cada vez mayores, afecta a millones de consumidores y provoca pérdidas anuales estimadas en 290 000 millones de euros⁴.

^{4a} Informe Norton sobre

Enmienda 20

Propuesta de Directiva Considerando 33

Texto de la Comisión

(33) La Comisión debe revisar periódicamente las disposiciones contenidas en la presente Directiva, en particular con vistas a determinar si es preciso modificarlas a la luz de la cambiante situación de la tecnología o el mercado.

Enmienda

(33) La Comisión debe revisar periódicamente las disposiciones contenidas en la presente Directiva, en particular con vistas a determinar si es preciso modificarlas a la luz de la cambiante situación de la tecnología o el mercado **y de las obligaciones relativas al máximo nivel de seguridad e integridad de las redes y de la información y protección de la intimidad y los datos personales.**

Enmienda 21

Propuesta de Directiva Considerando 39

Texto de la Comisión

(39) El intercambio de información sobre riesgos e incidentes en el marco de la red de cooperación y el cumplimiento de la obligación de notificar los incidentes a las autoridades nacionales competentes pueden hacer necesario el tratamiento de datos personales. Dicho tratamiento es necesario para alcanzar los objetivos de interés público perseguidos por la presente Directiva **y es por tanto** legítimo en virtud del artículo 7 de la Directiva 95/46/CE. No **constituye, en relación con esos objetivos legítimos, una intervención desmesurada e intolerable que afecte a la propia esencia del** derecho a la protección de los datos personales garantizado por el artículo 8 de la Carta de los Derechos Fundamentales. Al llevar a la práctica la presente Directiva,

Enmienda

(39) El intercambio de información sobre riesgos e incidentes en el marco de la red de cooperación y el cumplimiento de la obligación de notificar los incidentes a las autoridades nacionales competentes pueden hacer necesario el tratamiento de datos personales. **Si** dicho tratamiento es necesario para alcanzar los objetivos de interés público perseguidos por la presente Directiva, **puede ser** legítimo en virtud del artículo 7 de la Directiva 95/46/CE. No **exime, sin embargo, a las autoridades competentes de la obligación de una** intervención **proporcional que no atente contra el** derecho a la protección de los datos personales garantizado por el artículo 8 de la Carta de los Derechos Fundamentales. Al llevar a la práctica la

se debe aplicar, cuando proceda, el Reglamento (CE) nº 1049/2001 del Parlamento Europeo y del Consejo, de 30 de mayo de 2001, relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión⁸. Cuando las instituciones y órganos de la Unión procedan al tratamiento de datos a los efectos de la aplicación de la presente Directiva, dicho tratamiento deberá efectuarse de conformidad con los dispuesto en el Reglamento (CE) nº 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos.

³¹ DO L 145 de 31.5.2001, p. 43.

presente Directiva, se debe aplicar, cuando proceda, el Reglamento (CE) nº 1049/2001 del Parlamento Europeo y del Consejo, de 30 de mayo de 2001, relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión⁸. Cuando las instituciones y órganos de la Unión procedan al tratamiento de datos a los efectos de la aplicación de la presente Directiva, dicho tratamiento deberá efectuarse de conformidad con los dispuesto en el Reglamento (CE) nº 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos.

³¹ DO L 145 de 31.5.2001, p. 43.

Enmienda 22

Propuesta de Directiva Considerando 41 bis (nuevo)

Texto de la Comisión

Enmienda

(41 bis) En todas las medidas debe asegurarse una protección de los derechos humanos fundamentales, en especial, de los mencionados en el Convenio Europeo de Derechos Humanos (artículo 8, respeto de la vida privada), y debe respetarse el principio de proporcionalidad.

Enmienda 23

Propuesta de Directiva Artículo 1 – apartado 5

Texto de la Comisión

Enmienda

5. **Asimismo**, la presente Directiva **se**

5. La presente Directiva **respetará**

entenderá sin perjuicio de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, **de** la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, y **del** Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

totalmente la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, y **el** Reglamento **(CE) n° 45/2001** del Parlamento Europeo y del Consejo, **de 18 de diciembre de 2000**, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales **por las instituciones y órganos de la UE** y a la libre circulación de estos datos.

Enmienda 24

Propuesta de Directiva Artículo 2

Texto de la Comisión

No se impedirá que los Estados miembros adopten o mantengan disposiciones que garanticen un nivel de seguridad más elevado, sin perjuicio de las obligaciones que les impone la normativa de la Unión.

Enmienda

No se impedirá que los Estados miembros adopten o mantengan disposiciones que garanticen un nivel de seguridad más elevado, sin perjuicio de las obligaciones que les impone la normativa de la Unión, **pero dichas disposiciones deben cumplir las expectativas mínimas comunes aplicables en este caso, consagradas en la presente Directiva.**

Enmienda 25

Propuesta de Directiva Artículo 3 – punto 2

Texto de la Comisión

2. «seguridad»: la capacidad de las redes y sistemas de información de resistir, **con un nivel determinado de confianza**, a

Enmienda

(2) «seguridad»: la capacidad de las redes y sistemas de información de resistir a acciones accidentales o malintencionadas

acciones accidentales o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos;

que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos;

Enmienda 26

Propuesta de Directiva

Artículo 3 – apartado 2 – letra a (nueva)

Texto de la Comisión

Enmienda

«resistencia cibernética»: la capacidad de una red y de un sistema de información de resistir y recuperar toda su capacidad operativa después de un incidente, debido entre otras cosas a: averías técnicas, cortes de energía o incidentes de seguridad;

Enmienda 27

Propuesta de Directiva

Artículo 3 – apartado 4

Texto de la Comisión

Enmienda

«incidente»: toda circunstancia o hecho que tenga efectos adversos en la seguridad;

«incidente»: toda circunstancia o hecho que tenga efectos adversos en la seguridad **y la prestación de servicios fundamentales;**

Enmienda 28

Propuesta de Directiva

Artículo 3 – punto 8 – letra b

Texto de la Comisión

Enmienda

b) un operador de infraestructuras críticas esenciales para el mantenimiento de actividades económicas **y sociales** vitales

b) un operador de infraestructuras críticas esenciales para el mantenimiento de actividades **sociales y** económicas vitales

en los sectores de la energía, los transportes, la banca, la bolsa y la sanidad, una lista no exhaustiva de los cuales figura en el anexo II.

en los sectores de la energía, los transportes, la banca, la bolsa, **la cadena alimentaria** y la sanidad, una lista no exhaustiva de los cuales figura en el anexo II.

Enmienda 29

Propuesta de Directiva Artículo 5 – apartado 2 – letra a

Texto de la Comisión

a) **Plan de** evaluación de riesgos que permita determinarlos y evaluar los efectos de incidentes potenciales.

Enmienda

a) **Marco de gestión de riesgos con, al menos, una** evaluación **regular** de riesgos que permita determinarlos y evaluar los efectos de incidentes potenciales, **y medidas de salvaguardia de la seguridad y la integridad de la información, incluida una alerta rápida.**

Justificación

Un plan de evaluación no es suficiente y no incluye otras medidas necesarias para la gestión de riesgos en materia de seguridad de las redes y de la información. El SEPD recomienda que se establezca un marco de gestión de riesgos, lo que implica una evaluación de los riesgos.

Enmienda 30

Propuesta de Directiva Artículo 5 – apartado 3

Texto de la Comisión

3. La estrategia nacional de SRI y el plan de cooperación nacional en materia de SRI se deberán remitir a la Comisión en el plazo de un mes a partir de su adopción.

Enmienda

3. La estrategia nacional de SRI y el plan de cooperación nacional en materia de SRI se deberán remitir a la Comisión, **el Parlamento Europeo, el Consejo y el Supervisor Europeo de Protección de Datos** en el plazo de un mes a partir de su adopción **y no más tarde de 12 meses después de la entrada en vigor de la presente Directiva.**

Enmienda 31

Propuesta de Directiva

Artículo 5 – apartado 3 bis (nuevo)

Texto de la Comisión

Enmienda

3 bis. La Comisión elaborará un resumen con las estrategias de SRI de todos los Estados miembros y lo remitirá a los mismos de forma organizada.

Justificación

Es conveniente que los Estados miembros puedan consultar también los planes del resto de Estados. Esto les ayudará a determinar sus planteamientos e incluso podrían surgir oportunidades para un intercambio de mejores prácticas.

Enmienda 32

Propuesta de Directiva

Artículo 5 - apartado 3 ter (nuevo)

Texto de la Comisión

Enmienda

3 ter. En un plazo de seis meses tras la aprobación de la presente Directiva, la Comisión confeccionará una guía relativa a la estructura de la estrategia de SRI. Tendrá por finalidad ayudar a los Estados miembros a elaborar y aprobar documentos que tengan aproximadamente la misma estructura.

Justificación

La labor de organización y resumen a escala comunitaria sería más efectiva si los veintiocho documentos en los que se basa cumpliesen una cierta estructura general. Aunque la guía de la Comisión no fuera vinculante, aun así induciría a los Estados miembros a cumplir con esta estructura o modelo recomendado a la hora de elaborar sus propias estrategias nacionales.

Enmienda 33

Propuesta de Directiva Artículo 6 – apartado 1

Texto de la Comisión

1. Cada Estado miembro designará una autoridad nacional competente en materia de seguridad de las redes y los sistemas de información («la autoridad competente»).

Enmienda

1. Cada Estado miembro designará una autoridad **civil** nacional competente en materia de seguridad de las redes y los sistemas de información («la autoridad competente»).

Enmienda 34

Propuesta de Directiva Artículo 6 – apartado 5

Texto de la Comisión

5. Las autoridades competentes llevarán a cabo consultas y cooperarán, **cuando proceda**, con las fuerzas de seguridad nacionales y las autoridades responsables de la protección de datos.

Enmienda

5. Las autoridades competentes llevarán a cabo consultas y cooperarán **estrechamente**, con las fuerzas de seguridad nacionales y las autoridades responsables de la protección de datos **competentes, cuando proceda y teniendo en cuenta el principio de proporcionalidad**.

Enmienda 35

Propuesta de Directiva Artículo 6 – apartado 5 (nuevo)

Texto de la Comisión

Enmienda

5. Las autoridades competentes cumplirán, en relación con la información recogida, procesada e intercambiada, los requisitos relativos a la protección de los datos personales tal como se establecen en el artículo 17 de la Directiva 95/46/CE.

Enmienda 36

Propuesta de Directiva Artículo 7 – apartado 1

Texto de la Comisión

1. Cada Estado miembro creará **un equipo** de respuesta a emergencias informáticas (en lo sucesivo, «CERT») responsable de la gestión de incidentes y riesgos de acuerdo con un procedimiento claramente definido, que se ajustará a los requisitos establecidos en el anexo I, punto 1. **Podrá crearse** un CERT en el marco de la autoridad competente.

Enmienda

1. Cada Estado miembro creará **equipos** de respuesta a emergencias informáticas (en lo sucesivo, «CERT») responsable de la gestión de incidentes y riesgos de acuerdo con un procedimiento claramente definido, que se ajustará a los requisitos establecidos en el anexo I, punto 1. **Si procede, se creará** un CERT en el marco de la autoridad competente.

Enmienda 37

Propuesta de Directiva Artículo 8 – apartado 2

Texto de la Comisión

2. La Comisión y las autoridades competentes mantendrán una comunicación constante en el marco de la red de cooperación. Cuando así se le solicite, la Agencia Europea de Seguridad de las Redes y de la Información («ENISA») asistirá a la red de cooperación ofreciéndole **su experiencia, conocimientos y asesoramiento**.

Enmienda

2. La Comisión y las autoridades competentes mantendrán una comunicación constante en el marco de la red de cooperación. Cuando así se le solicite, la Agencia Europea de Seguridad de las Redes y de la Información («ENISA») asistirá a la red de cooperación ofreciéndole **orientación tecnológica neutra con medidas adecuadas tanto para el sector público como para el privado**.

Enmienda 38

Propuesta de Directiva Artículo 9 – apartado 2 - letra b bis (nueva)

Texto de la Comisión

Enmienda

b bis) los criterios de participación de los Estados miembros en el sistema para compartir información segura para garantizar en todos los participantes un

elevado nivel de seguridad y resistencia en todas las fases del proceso, incluso mediante medidas apropiadas de confidencialidad y seguridad de conformidad con los artículos 16 y 17 de la Directiva 95/46/CE y los artículos 21 y 22 del Reglamento (CE) n° 45/2001.

Enmienda 39

Propuesta de Directiva Artículo 9 – apartado 3

Texto de la Comisión

Enmienda

3. La Comisión adoptará mediante actos de ejecución decisiones sobre el acceso de los Estados miembros a esta infraestructura segura, con arreglo a los criterios mencionados en los apartados 2 y 3. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 19, apartado 3.

suprimido

Enmienda 40

Propuesta de Directiva Artículo 12 – apartado 2 – letra a – guión 2

Texto de la Comisión

Enmienda

– los **procedimientos** y criterios de evaluación de riesgos e incidentes por parte de la red de cooperación;

– los criterios de evaluación de riesgos e incidentes por parte de la red de cooperación;

Enmienda 41

Propuesta de Directiva Artículo 13

Texto de la Comisión

Enmienda

Sin perjuicio de la posibilidad de que la red de cooperación mantenga relaciones

Sin perjuicio de la posibilidad de que la red de cooperación mantenga relaciones

informales de colaboración a escala internacional, la Unión podrá concluir acuerdos internacionales con terceros países u organizaciones internacionales que hagan posible y organicen su participación en algunas actividades de la red de cooperación. **En** tales acuerdos se **tendrá en cuenta la necesidad de deparar una** protección **adecuada a** los datos personales que circulen en la red de cooperación.

informales de colaboración a escala internacional, la Unión podrá concluir acuerdos internacionales con terceros países u organizaciones internacionales que hagan posible y organicen su participación en algunas actividades de la red de cooperación. Tales acuerdos **solo se concluirán si puede garantizarse un nivel de** protección **de** los datos personales que circulen en la red de cooperación **adecuado y comparable al de la Unión.**

Enmienda 42

Propuesta de Directiva Artículo 14 –apartado 1

Texto de la Comisión

1. Los Estados miembros velarán por que las administraciones públicas y los operadores del mercado tomen las medidas técnicas y de organización apropiadas para gestionar los riesgos existentes para la seguridad de las redes y los sistemas de información que controlan y utilizan en sus operaciones. Habida cuenta del estado de la técnica, dichas medidas garantizarán un nivel de seguridad adecuado en relación con el riesgo existente. En particular, adoptarán medidas para prevenir y reducir al mínimo los efectos de los incidentes que afecten a sus redes y sistemas de información en los servicios básicos que prestan, garantizando de este modo la continuidad de los servicios que dependen de tales redes y sistemas de información.

Enmienda

1. Los Estados miembros velarán por que las administraciones públicas y los operadores del mercado tomen las medidas técnicas y de organización apropiadas para **detectar**, gestionar **eficazmente y limitar** los riesgos existentes para la seguridad de las redes y los sistemas de información que controlan y utilizan en sus operaciones. Habida cuenta del estado de la técnica, dichas medidas garantizarán un nivel de seguridad adecuado **y proporcional** en relación con el riesgo existente. En particular, adoptarán medidas para prevenir y reducir al mínimo los efectos de los incidentes que afecten a sus redes y sistemas de información en los servicios básicos que prestan, garantizando de este modo la continuidad de los servicios **y la seguridad de los datos** que dependen de tales redes y sistemas de información.

Enmienda 43

Propuesta de Directiva Artículo 14 – apartado 2 – letra a (nueva)

Enmienda

a) Los fabricantes de programas informáticos comerciales serán considerados responsables a pesar de las cláusulas de exención de responsabilidad del acuerdo con el usuario en caso de grave negligencia en relación con la seguridad.

Justificación

En el acuerdo de licencia, los fabricantes de programas informáticos comerciales se eximen de toda responsabilidad que pueda surgir debido a un sistema deficiente en materia de seguridad y una programación inferior. Para fomentar que los fabricantes de programas informáticos inviertan en medidas de seguridad es necesaria una cultura diferente. Solo puede lograrse si los fabricantes de programas informáticos son considerados responsables de cualquier déficit en materia de seguridad.

Enmienda 44

Propuesta de Directiva Artículo 14 – apartado 3

Texto de la Comisión

3. Los requisitos establecidos en los apartados 1 y 2 serán aplicables a todos los operadores del mercado que prestan servicios en la Unión Europea.

Enmienda

3. Los requisitos establecidos en los apartados 1 y 2 serán aplicables a todos los operadores del mercado **y productores de programas informáticos** que prestan servicios en la Unión Europea.

Enmienda 45

Propuesta de Directiva Artículo 14 - apartado 6

Texto de la Comisión

6. A reserva de cualesquiera actos delegados adoptados en virtud del apartado 5, las autoridades competentes podrán adoptar directrices y, en caso necesario, impartir instrucciones sobre las circunstancias en que las

Enmienda

suprimido

administraciones públicas y los operadores del mercado estarán obligados a notificar incidentes.

Enmienda 46

Propuesta de Directiva Artículo 15 – apartado 1

Texto de la Comisión

1. Los Estados miembros velarán por que las autoridades competentes dispongan de ***todas*** las competencias necesarias para investigar los casos de incumplimiento por parte de las administraciones públicas o los operadores del mercado de las obligaciones que les impone el artículo 14 y los efectos que tengan en la seguridad de las redes y los sistemas de información.

Enmienda

1. Los Estados miembros velarán por que las autoridades competentes dispongan de las competencias necesarias para investigar los casos de incumplimiento por parte de las administraciones públicas o los operadores del mercado de las obligaciones que les impone el artículo 14 y los efectos que tengan en la seguridad de las redes y los sistemas de información.

Enmienda 47

Propuesta de Directiva Artículo 15 – apartado 5

Texto de la Comisión

5. Las autoridades competentes cooperarán estrechamente con las autoridades responsables de la protección de datos personales a la hora de hacer frente a incidentes que den lugar a violaciones de datos personales.

Enmienda

5. ***Sin perjuicio de la legislación aplicable en materia de protección de datos, y en plena consulta con los correspondientes responsables del tratamiento de datos,*** las autoridades competentes ***y las ventanillas únicas*** cooperarán estrechamente con las autoridades responsables de la protección de datos personales a la hora de hacer frente a incidentes que den lugar a violaciones de datos personales.

Enmienda 48

Propuesta de Directiva Artículo 19 bis (nuevo)

Texto de la Comisión

Enmienda

Artículo 19 bis

Tratamiento y protección de los datos personales

- 1. El tratamiento de los datos personales en los Estados miembros con arreglo a la presente Directiva se llevará a cabo de conformidad con las Directivas 95/46/CE y 2002/58/CE.**
- 2. El tratamiento de los datos personales por la Comisión y ENISA con arreglo al presente Reglamento se llevará a cabo de conformidad con el Reglamento (CE) n° 45/2001.**
- 3. El tratamiento de los datos personales por el Centro Europeo de Ciberdelincuencia de Europol a efectos de la presente Directiva se llevará a cabo de conformidad con la Decisión 2009/371/JAI.**
- 4. El tratamiento de los datos personales será justo y legítimo y se limitará estrictamente a los datos mínimos necesarios para los efectos para los que se procesan. Deberán conservarse en una forma que permita la identificación de los interesados durante un periodo no superior al necesario para los fines para los que dichos datos personales son procesados.**
- 5. Las notificaciones de incidentes mencionadas en el artículo 14 se tramitarán sin perjuicio de las disposiciones y obligaciones en materia de notificación de violaciones de datos personales contempladas en el artículo 4 de la Directiva 2002/58/CE y en el Reglamento (UE) n° 611/2013.**
- 6. Las referencias a la Directiva 95/46/CE**

se interpretarán como referencias al Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general sobre protección de datos), una vez que entre en vigor.

Enmienda 49

Propuesta de Directiva Artículo 20 – apartado 1

Texto de la Comisión

La Comisión revisará periódicamente el funcionamiento de la presente Directiva e informará al Parlamento Europeo y al Consejo. El primer informe se presentará a más tardar **tres** años después de la fecha de transposición mencionada en el artículo 21. A tal fin, la Comisión podrá solicitar a los Estados miembros que faciliten información sin demoras injustificadas.

Enmienda

La Comisión revisará periódicamente el funcionamiento de la presente Directiva e informará al Parlamento Europeo y al Consejo. El primer informe se presentará a más tardar **dos** años después de la fecha de transposición mencionada en el artículo 21. A tal fin, la Comisión podrá solicitar a los Estados miembros que faciliten información sin demoras injustificadas.

Enmienda 50

Propuesta de Directiva Anexo – apartado 1 – punto 1 – letra b

Texto de la Comisión

b) El CERT aplicará y gestionará medidas de seguridad para garantizar la confidencialidad, integridad, disponibilidad y autenticidad de la información que reciba y trate.

Enmienda

b) El CERT aplicará y gestionará medidas de seguridad para garantizar la confidencialidad, integridad, disponibilidad y autenticidad de la información que reciba y trate, **y garantizará la protección de datos.**

Enmienda 51

Propuesta de Directiva Anexo 2 – apartado 1

Texto de la Comisión

Lista de operadores del mercado

Contemplados en el artículo 3, apartado 8, letra a):

1. Plataformas de comercio electrónico.
2. Pasarelas de pago por Internet.

3. Redes sociales.

4. Motores de búsqueda.

5. Servicios de computación en nube.

6. Tiendas de aplicaciones.

Enmienda 52

Propuesta de Directiva

Anexo 2 – apartado 2 – punto 5 bis (nuevo)

Texto de la Comisión

Enmienda

Lista de operadores del mercado

Contemplados en el artículo 3, apartado 8, letra a)

1. Plataformas de comercio electrónico.
2. Pasarelas de pago por Internet.

3. Motores de búsqueda.

4. Servicios de computación en nube **que almacenen datos sobre infraestructuras críticas de la Unión Europea.**

Enmienda

5 bis. Cadena alimentaria

PROCEDIMIENTO

Título	Medidas para garantizar un elevado nivel común de seguridad de las redes y de la información en la Unión			
Referencias	COM(2013)0048 – C7-0035/2013 – 2013/0027(COD)			
Comisión competente para el fondo Fecha del anuncio en el Pleno	IMCO 15.4.2013			
Opinión emitida por Fecha del anuncio en el Pleno	LIBE 15.4.2013			
Comisión(es) asociada(s) - fecha del anuncio en el pleno	12.9.2013			
Ponente de opinión Fecha de designación	Carl Schlyter 7.3.2013			
Examen en comisión	25.4.2013	18.9.2013	4.11.2013	13.1.2014
Fecha de aprobación	13.1.2014			
Resultado de la votación final	+: 36 -: 6 0: 0			
Miembros presentes en la votación final	Jan Philipp Albrecht, Roberta Angelilli, Edit Bauer, Rita Borsellino, Arkadiusz Tomasz Bratkowski, Philip Claey's, Frank Engel, Cornelia Ernst, Tanja Fajon, Monika Flašíková Beňová, Kinga Gál, Kinga Göncz, Salvatore Iacolino, Sophia in 't Veld, Timothy Kirkhope, Juan Fernando López Aguilar, Baroness Sarah Ludford, Monica Luisa Macovei, Svetoslav Hristov Malinov, Véronique Mathieu Houillon, Anthea McIntyre, Nuno Melo, Roberta Metsola, Claude Moraes, Jacek Protasiewicz, Carmen Romero López, Birgit Sippel, Csaba Sógor, Renate Sommer, Axel Voss, Renate Weber, Josef Weidenholzer, Cecilia Wikström, Tatjana Ždanoka, Auke Zijlstra			
Suplente(s) presente(s) en la votación final	Monika Hohlmeier, Jean Lambert, Ulrike Lunacek, Jan Mulder, Carl Schlyter, Marco Scurria			
Suplente(s) (art. 187, apdo. 2) presente(s) en la votación final	Katarína Neveďalová			