



PARLAMENTO EUROPEO

2009 - 2014

---

*Comisión de Asuntos Exteriores*

---

**2013/0027(COD)**

6.12.2013

# OPINIÓN

de la Comisión de Asuntos Exteriores

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: Ana Gomes

PA\_Legam

## ENMIENDAS

La Comisión de Asuntos Exteriores 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 y el bienestar social y, en particular, para el funcionamiento del mercado interior, ***así como para la seguridad exterior de la UE.***

### 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 ***y, en última instancia, poner en peligro el bienestar de los ciudadanos de la UE y la capacidad de los Estados miembros de la UE de protegerse y garantizar la***

*seguridad de infraestructuras críticas.*

### **Enmienda 3**

#### **Propuesta de Directiva Considerando 2 bis (nuevo)**

*Texto de la Comisión*

*Enmienda*

*(2 bis) La cláusula de solidaridad, introducida en virtud del artículo 222 del TFUE, constituye el marco apropiado para la asistencia y la acción concertada entre los Estados miembros de la UE, en caso de un ataque terrorista o de actividad delictiva que ponga en peligro la seguridad de las redes y de la información. De igual modo, la cláusula de defensa mutua que establece el artículo 47, apartado 7, del TUE deberá constituir el marco de acción de la UE en el caso de que un Estado miembro fuera víctima de una agresión armada que afecte a la seguridad de las redes y la información. En los casos pertinentes, el artículo 222 del TFUE y el artículo 42, apartado 7, del TUE se aplicarán de forma complementaria.*

### **Enmienda 4**

#### **Propuesta de Directiva Considerando 2 bis (nuevo)**

*Texto de la Comisión*

*Enmienda*

*(2 bis) Un gran número de incidentes cibernéticos se producen debido a la falta de resistencia y solidez de la infraestructura de la red privada y pública, unas bases de datos mal protegidas o mal aseguradas y otros defectos en las infraestructuras críticas de información; solo algunos Estados miembros consideran la protección de sus redes y sistemas de información y datos*

*asociados como parte de su correspondiente deber de diligencia, lo cual explica la falta de inversión en tecnología de seguridad de vanguardia, formación y desarrollo de directrices adecuadas.*

## **Enmienda 5**

### **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, *así como para la seguridad interior y exterior de la UE. Por consiguiente, la Estrategia de Seguridad Interior de la Unión y la Estrategia Europea de Seguridad deben hacer debidamente hincapié en la necesidad de mejorar la seguridad de las redes y la información, en particular a la vista de la futura revisión de esos documentos.*

## **Enmienda 6**

### **Propuesta de Directiva Considerando 3 bis (nuevo)**

*Texto de la Comisión*

*Enmienda*

***(3 bis) La concienciación y la educación de los usuarios de tecnologías de la información y la comunicación sobre mejores prácticas en cuanto a la protección de datos personales y el mantenimiento sostenible de servicios de comunicación deben constituir la base de cualquier estrategia global de ciberseguridad.***

## **Enmienda 7**

### **Propuesta de Directiva Considerando 4 bis (nuevo)**

*Texto de la Comisión*

*Enmienda*

***(4 bis) La cooperación y la coordinación entre las autoridades europeas pertinentes con la VP/AR, con responsabilidad para la Política Exterior y de Seguridad Común y la Política Común de Seguridad y Defensa, así como el Coordinador de la UE para la lucha contra el terrorismo deben garantizarse en todos los casos en los que se perciban riesgos de naturaleza exterior y terrorista.***

## **Enmienda 8**

### **Propuesta de Directiva Considerando 4 ter (nuevo)**

*Texto de la Comisión*

*Enmienda*

***(4 ter) Los servicios de inteligencia y el intercambio de información sensible entre los Estados miembros y entre los Estados miembros y las autoridades de la UE competentes deben reforzarse y anclarse en los principios de confianza, solidaridad y cooperación. Todo plan de acción encaminado a mejorar la seguridad de las***

*redes y el sistema debe hacer pleno uso de las estructuras ya existentes en la UE, como el SitCen y el IntCen, y asegurar la coordinación entre todas las estructuras pertinentes para la seguridad de la información sensible en relación con la seguridad interior y exterior de la UE.*

## **Enmienda 9**

### **Propuesta de Directiva Considerando 4 quater (nuevo)**

*Texto de la Comisión*

*Enmienda*

*(4 quater) La cooperación y el intercambio de información a escala mundial con los socios internacionales pertinentes son esenciales para una estrategia eficaz de ciberseguridad y para una acción convincente con vistas a mejorar la seguridad de las redes y la información en la UE, teniendo en cuenta la naturaleza transnacional de las amenazas.*

## **Enmienda 10**

### **Propuesta de Directiva Considerando 8 bis (nuevo)**

*Texto de la Comisión*

*Enmienda*

*(8 bis) Las medidas de seguridad han de respetar los derechos fundamentales que incumben a la UE y a sus Estados miembros de conformidad con los artículos 2, 6 y 21 del TFUE, como la libertad de expresión, la protección de datos y la intimidad; el derecho a la intimidad y el derecho a la protección de datos están consignados en la Carta de la UE y en el artículo 16 del TFUE.*

## Enmienda 11

### Propuesta de Directiva Considerando 11 bis (nuevo)

*Texto de la Comisión*

*Enmienda*

***(11 bis) Todos los Estados miembros deben centrar las estrategias nacionales de ciberseguridad en la protección de los sistemas de información y los datos asociados, y han de considerar la protección de estas infraestructuras críticas como parte de su correspondiente deber de diligencia. Todos los Estados miembros deben adoptar y aplicar estrategias, directrices e instrumentos que ofrezcan niveles razonables de protección contra niveles de amenazas razonablemente identificables, en que los costes y las cargas de la protección sean proporcionales al daño probable a las partes implicadas. Asimismo, todos los Estados miembros deben adoptar las medidas adecuadas para obligar a las personas jurídicas bajo su jurisdicción a proteger los datos personales a su cuidado.***

## 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 información no confidencial sobre incidentes y riesgos. ***Cualquier dato personal publicado en este sitio web debe limitarse únicamente a lo necesario y ser lo más anónimo posible.***



### **Enmienda 13**

#### **Propuesta de Directiva Considerando 30 bis (nuevo)**

*Texto de la Comisión*

*Enmienda*

*(30 bis) La presente Directiva se entiende sin perjuicio del acervo de la Unión en lo que respecta a la protección de datos. Todo dato personal utilizado de conformidad con lo dispuesto en la presente Directiva debe mantenerse en el conjunto mínimo de datos personales estrictamente necesarios y solo ha de ser transmitido a los actores estrictamente necesarios, y debe ser lo más anónimo posible, cuando no totalmente anónimo.*

### **Enmienda 14**

#### **Propuesta de Directiva Considerando 32 bis (nuevo)**

*Texto de la Comisión*

*Enmienda*

*(32 bis) La presente Directiva (Directiva sobre SRI) no afecta a la adopción necesaria de legislación sobre protección general de datos a escala de la UE.*

### **Enmienda 15**

#### **Propuesta de Directiva Considerando 34 bis (nuevo)**

*Texto de la Comisión*

*Enmienda*

*(34 bis) Es necesario regular a escala de la UE la venta, el suministro, la transferencia o la exportación a terceros países de equipos o programas destinados principalmente a controlar o interceptar*

*las comunicaciones telefónicas o por Internet en redes fijas y móviles, y la prestación de asistencia para instalar, manejar o actualizar dichos equipos o programas. La Comisión debe elaborar lo antes posible una legislación que evite que las empresas europeas exporten dichos productos de doble uso a regímenes represivos, autoritarios y no democráticos.*

## **Enmienda 16**

### **Propuesta de Directiva Artículo 1 – apartado 2 – letra b**

#### *Texto de la Comisión*

b) establece un mecanismo de cooperación entre los Estados miembros con el fin de garantizar la aplicación uniforme de la presente Directiva en la Unión y, en su caso, una gestión y una respuesta eficaces y coordinadas ante los riesgos e incidentes que afecten a las redes y los sistemas de información;

#### *Enmienda*

b) establece un mecanismo de cooperación entre los Estados miembros con el fin de garantizar la aplicación uniforme de la presente Directiva en la Unión y, en su caso, una gestión y una respuesta eficaces, **eficientes** y coordinadas ante los riesgos e incidentes que afecten a las redes y los sistemas de información;

## **Enmienda 17**

### **Propuesta de Directiva Artículo 3 – punto 1 – letra b**

#### *Texto de la Comisión*

b) todo **dispositivo o** grupo de dispositivos interconectados o relacionados entre sí, uno o varios de los cuales realizan, mediante un programa, el tratamiento automático de datos informáticos,

#### *Enmienda*

b) todo grupo de dispositivos interconectados o relacionados entre sí, uno o varios de los cuales realizan, mediante un programa, el tratamiento automático de datos informáticos,

## **Enmienda 18**

### **Propuesta de Directiva Artículo 3 – punto 2 bis (nuevo)**

*Texto de la Comisión*

*Enmienda*

**2 bis) «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 19**

### **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 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.

b) un operador de infraestructuras críticas esenciales para el mantenimiento de actividades económicas y sociales vitales en los sectores de la energía, los transportes, la banca, la bolsa, la sanidad, **la seguridad y la defensa**, una lista no exhaustiva de los cuales figura en el anexo II.

## **Enmienda 20**

### **Propuesta de Directiva Artículo 3 – punto 8 – letra b bis (nueva)**

*Texto de la Comisión*

*Enmienda*

**b bis) proveedores de dispositivos, redes y sistemas de información como los que se mencionan en el punto 1), o sus componentes que son fundamentales para un elevado nivel común de seguridad de las redes y la información.**

## Enmienda 21

### 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 22

### 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 **al menos** 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 23

### Propuesta de Directiva Artículo 8 – apartado 3 – letra f bis (nueva)

#### *Texto de la Comisión*

#### *Enmienda*

***f bis) cuando sea pertinente, dada la naturaleza del riesgo o de la amenaza, deberá informarse al Coordinador de la UE para la lucha contra el terrorismo mediante informes y se le podrá pedir que contribuya con un análisis a la acción y los trabajos preparatorios de la red de cooperación;***

## Enmienda 24

### Propuesta de Directiva Artículo 9 – apartado 1 bis (nuevo)

*Texto de la Comisión*

*Enmienda*

***1 bis. Los datos personales solo se divulgarán a los destinatarios que necesiten procesarlos para el ejercicio de sus funciones, de conformidad con un fundamento jurídico apropiado. Los datos divulgados se limitarán a lo necesario para el ejercicio de sus funciones. Se garantizará el cumplimiento del principio de limitación del objetivo. El plazo límite de retención de estos datos se especificará para los efectos previstos en la presente Directiva.***

## Enmienda 25

### Propuesta de Directiva Artículo 10 – apartado 3

*Texto de la Comisión*

*Enmienda*

3. A petición de un Estado miembro o por iniciativa propia, la Comisión podrá solicitar a un Estado miembro que proporcione la información pertinente sobre un riesgo o incidente concreto.

3. A petición de un Estado miembro o por iniciativa propia, la Comisión podrá solicitar a un Estado miembro que proporcione la información pertinente sobre un riesgo o incidente concreto, ***de conformidad con las disposiciones del Reglamento general sobre protección de datos.***

## Enmienda 26

### Propuesta de Directiva Artículo 13 – párrafo –1 bis (nuevo)

*Texto de la Comisión*

*Enmienda*

***(–1 bis) La VP/AR integrará en las***

*acciones exteriores de la UE, en particular en relación con los países terceros, los aspectos relativos a la ciberseguridad. El objetivo será intensificar el intercambio de las lecciones aprendidas y la cooperación sobre cuestiones de ciberseguridad.*

## **Enmienda 27**

### **Propuesta de Directiva Artículo 13 – párrafo –1 ter (nuevo)**

*Texto de la Comisión*

*Enmienda*

*(–1 ter) El Consejo y la Comisión insistirán en las normas mínimas para la seguridad de los sistemas de información, en el marco de sus relaciones y acuerdos de cooperación con terceros países, en particular los que implican la cooperación en materia de tecnologías.*

## **Enmienda 28**

### **Propuesta de Directiva Artículo 20 – título**

*Texto de la Comisión*

*Enmienda*

Revisión

*Presentación de informes y revisión*

## **Enmienda 29**

### **Propuesta de Directiva Artículo 20 – párrafo –1 bis (nuevo)**

*Texto de la Comisión*

*Enmienda*

*(–1 bis) La Comisión presentará al Parlamento Europeo y al Consejo un informe anual sobre los incidentes y las medidas que se le notifiquen en virtud de la presente Directiva.*

## Enmienda 30

### Propuesta de Directiva Anexo 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, ***cumpliendo los requisitos de protección de datos.***

## Enmienda 31

### Propuesta de Directiva Anexo II – segundo subtítulo (Contemplados en el artículo 3, apartado 8, letra b) – apartado 5 bis (nuevo)

#### *Texto de la Comisión*

#### *Enmienda*

***(5 bis) Sector de la seguridad y la defensa: operadores económicos para trabajos y servicios a los que hace referencia la Directiva 2009/81/CE, en particular su artículo 46.***

## PROCEDIMIENTO

<b>Título</b>	Medidas para garantizar un elevado nivel común de seguridad de las redes y de la información en la Unión
<b>Referencias</b>	COM(2013)0048 – C7-0035/2013 – 2013/0027(COD)
<b>Comisión competente para el fondo</b> Fecha del anuncio en el Pleno	IMCO 15.4.2013
<b>Opinión emitida por</b> Fecha del anuncio en el Pleno	AFET 15.4.2013
<b>Ponente de opinión</b> Fecha de designación	Ana Gomes 19.2.2013
<b>Examen en comisión</b>	18.9.2013
<b>Fecha de aprobación</b>	5.12.2013
<b>Resultado de la votación final</b>	+ :                31 - :                3 0 :                8
<b>Miembros presentes en la votación final</b>	Elmar Brok, Jerzy Buzek, Mark Demesmaeker, Marietta Giannakou, Ana Gomes, Andrzej Grzyb, Anna Ibrisagic, Jelko Kacin, Tunne Kelam, Nicole Kiil-Nielsen, Andrey Kovatchev, Eduard Kukan, Marusya Lyubcheva, Annemie Neyts-Uyttebroeck, Norica Nicolai, Raimon Obiols, Kristiina Ojuland, Ria Oomen-Ruijten, Ioan Mircea Paşcu, Alojz Peterle, Mirosław Piotrowski, Bernd Posselt, Hans-Gert Pöttering, Cristian Dan Preda, Libor Rouček, Tokia Saïfi, José Ignacio Salafranca Sánchez-Neyra, György Schöpflin, Werner Schulz, Marek Siwiec, Charles Tannock, Geoffrey Van Orden, Nikola Vuljanić, Boris Zala
<b>Suplente(s) presente(s) en la votación final</b>	Marije Cornelissen, Barbara Lochbihler, Doris Pack, Marietje Schaake, Indrek Tarand, Ivo Vajgl, Paweł Zalewski
<b>Suplente(s) (art. 187, apdo. 2) presente(s) en la votación final</b>	Hiltrud Breyer