Comité Económico y Social Europeo

TEN/646
Reglamento de Ciberseguridad

DICTAMEN

Comité Económico y Social Europeo

Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a ENISA, la «Agencia de Ciberseguridad de la UE», y por el que se deroga el Reglamento (UE) n.º 526/2013, y relativo a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación («Reglamento de Ciberseguridad»)
[COM(2017) 477 final/2 2017/0225 (COD)]

Ponente: **Alberto MAZZOLA**
Coponente: **Antonio LONGO**

Consulta	Parlamento Europeo, 23.10.2017 Consejo de la Unión Europea, 25.10.2017
Fundamento jurídico	Artículo 114 del Tratado de Funcionamiento de la Unión Europea
Sección competente	Sección de Transportes, Energía, Infraestructuras y Sociedad de la Información
Aprobado en sección	05/02/2018
Aprobación en el pleno	14/02/2018
Pleno n.º	532
Resultado de la votación (a favor/en contra/abstenciones)	206/1/2

1. Conclusiones y recomendaciones

1.1 El CESE considera que el nuevo mandato permanente de la Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA) propuesto por la Comisión contribuirá de forma significativa a mejorar la resiliencia de los sistemas europeos. Sin embargo, el presupuesto provisional asociado y los recursos asignados a la ENISA no serán suficientes para que la Agencia cumpla su mandato.

1.2 El CESE recomienda a todos los Estados miembros que establezcan una contraparte clara y equivalente a la ENISA, ya que la mayoría de ellos aún no lo ha hecho.

1.3 El CESE opina asimismo que, en términos de creación de capacidades, la ENISA debería dar prioridad a acciones dirigidas a apoyar la administración electrónica[1]. La identidad digital en la UE y en el mundo para las personas, las organizaciones y los objetos es clave, y la prevención y la lucha contra la usurpación de identidad y el fraude en línea deben ser una prioridad.

1.4 El CESE recomienda que la ENISA proporcione informes periódicos sobre la ciberpreparación de los Estados miembros, centrados principalmente en los sectores determinados en el anexo II de la Directiva SRI. Cada año, un ciberejercicio realizado a escala europea debería evaluar la preparación de los Estados miembros y la eficacia del mecanismo europeo de respuesta a cibercrisis, y formular recomendaciones al respecto.

1.5 El CESE respalda la propuesta de crear una red de competencias en el ámbito de la ciberseguridad. Dicha red se apoyaría en un Centro de Investigación y Competencias sobre Ciberseguridad (CICC) y permitiría respaldar la soberanía digital europea desarrollando una base industrial europea competitiva para capacidades tecnológicas clave sobre la base del trabajo realizado por la asociación público-privada contractual (APPc), que debería convertirse en una empresa común tripartita.

1.6 El factor humano constituye una de las causas más importantes de los ciberaccidentes. Para el CESE, es necesario crear una base sólida de cibercompetencias y mejorar la ciberhigiene, en particular mediante campañas de sensibilización dirigidas a particulares y empresas. El CESE apoya la creación de un plan de estudios certificado por la UE para las escuelas secundarias y los profesionales.

1.7 El CESE considera que un mercado único digital europeo también necesita una interpretación homogénea de las normas en materia de ciberseguridad, incluido el reconocimiento mutuo entre Estados miembros, y que un marco de certificación, acompañado de sistemas de certificación para los distintos sectores, podría proporcionar una base común. Sin embargo, deberán preverse diferentes enfoques para los distintos sectores, en función de su modo de funcionamiento. Por lo tanto, el CESE considera que las agencias sectoriales de la UE (AESA, AFE, EMA, etc.) deberían participar en el proceso y, en ciertos casos y con el consentimiento de la ENISA para garantizar la coherencia, encargarse de elaborar regímenes de ciberseguridad. Se deberían

[1] Mercado único digital: revisión intermedia

adoptar normas mínimas europeas para la seguridad informática en cooperación con el CEN, el Cenelec y el ETSI.

1.8 El Grupo Europeo de Certificación de la Ciberseguridad previsto apoyado por la ENISA debe estar formado por autoridades nacionales de supervisión de la certificación, partes interesadas del sector privado, incluidos operadores de varios ámbitos de aplicación, científicos y agentes de la sociedad civil.

1.9 El CESE opina que la Agencia debería efectuar un seguimiento del rendimiento y la toma de decisiones de las autoridades nacionales de supervisión de la certificación mediante auditorías e inspecciones en nombre de la Comisión, y que las responsabilidades y sanciones en caso de incumplimiento de las normas deberían definirse en el Reglamento.

1.10 El CESE considera que las actividades de certificación no pueden carecer de un sistema de etiquetado apropiado, que deberá aplicarse también a los productos importados con el fin de reforzar la confianza de los consumidores.

1.11 Europa debe aumentar las inversiones haciendo que diferentes fondos de la UE, fondos nacionales e inversiones del sector privado converjan hacia objetivos estratégicos en una sólida cooperación entre los sectores público y privado, también mediante la creación, en el actual y en el futuro programa marco de investigación, de un Fondo de Ciberseguridad de la UE para la Innovación y la I+D. Además, Europa debería crear un fondo para el despliegue de la ciberseguridad, abriendo una nueva perspectiva en el actual y en el futuro Mecanismo «Conectar Europa», así como en el próxima el FEIE 3.0.

1.12 El CESE cree que es necesario un nivel de seguridad mínimo para los dispositivos «ordinarios» de la «internet de las personas». En este caso, la certificación es un método clave para proporcionar un nivel de seguridad superior. La seguridad de la internet de las cosas debe ser una prioridad.

2. Marco actual de la ciberseguridad

2.1 La ciberseguridad es fundamental para la prosperidad y la seguridad nacional, así como para el funcionamiento mismo de nuestras democracias, libertades y valores. La ciberseguridad es un ecosistema en el que las leyes, las organizaciones, las competencias, la cooperación y la ejecución técnica deben estar en armonía para maximizar su eficacia, según se afirma en el índice global de ciberseguridad de la ONU, y se añade que la ciberseguridad está adquiriendo cada vez mayor relevancia para los responsables políticos de los países.

2.2 La necesidad de un ecosistema seguro está cobrando una importancia fundamental debido a la revolución de internet. Esta revolución no solo ha redefinido las relaciones entre empresas y consumidores (B2C) en sectores como los medios de comunicación, el comercio al por menor y los servicios financieros, sino que también está remodelando los sectores de la fabricación, la energía, la agricultura, el transporte y otros sectores industriales de la economía que, en su conjunto, representan casi dos tercios del producto interior bruto mundial, así como las infraestructuras de servicios y las interacciones de las personas con la administración pública.

2.3 La Estrategia para el Mercado Único Digital se basa en la mejora del acceso a los bienes, los servicios y el contenido, la creación de un marco jurídico apropiado para las redes y los servicios digitales y el aprovechamiento de los beneficios de una economía basada en datos. Se ha estimado que la estrategia podría contribuir con 415 000 millones de euros al año a la economía de la UE. Se prevé un déficit de 350 000 profesionales con competencias en ciberseguridad en el sector privado en Europa para 2022[2].

2.4 Un estudio de 2014 estimó que el impacto económico de la ciberdelincuencia en la Unión ascendía al 0,41 % del PIB de la UE (es decir alrededor de 55 000 millones de euros) en 2013[3].

2.5 Según el Eurobarómetro especial 464a sobre la «Actitud de los europeos frente a la ciberseguridad», el 73 % de los usuarios de internet se muestran preocupados por que los sitios web puedan no mantener protegida su información personal en línea y el 65 % por que puedan no hacerlo las autoridades públicas. La mayoría de los encuestados manifiestan su preocupación porque podrían ser víctimas de varias formas de ciberdelincuencia, especialmente programas informáticos maliciosos en sus dispositivos (69 %), usurpación de identidad (69 %) y fraude de tarjeta bancaria o fraude bancario en línea (66 %)[4].

2.6 Hasta la fecha, ningún marco jurídico ha sido capaz de hacer frente al ritmo de la innovación digital, y varios textos legislativos están contribuyendo punto por punto a establecer un marco apropiado: la revisión del Código de Telecomunicaciones, el Reglamento general de protección de datos (RGPD), la Directiva sobre seguridad de las redes y los sistemas de información (Directiva SRI), el Reglamento relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (Reglamento eIDAS), el Escudo de la privacidad UE-EE, la Directiva sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo, etc.

2.7 Además de la ENISA, la «Agencia de ciberseguridad de la UE», hay muchas organizaciones distintas que se ocupan de cuestiones de ciberseguridad: Europol, el equipo de respuesta a emergencias informáticas de la Unión Europea (CERT-UE), el Centro de Análisis de Inteligencia de la UE (INTCEN), la Agencia Europea para la Gestión Operativa de Sistemas Informáticos de Gran Magnitud en el Espacio de Libertad, Seguridad y Justicia (eu-LISA), los centros de puesta en común y análisis de la información (ISAC), la Organización Europea de Ciberseguridad (ECSO), la Agencia Europea de Defensa (AED), el Centro de Excelencia para la Ciberdefensa Cooperativa de la OTAN, el Grupo de Expertos Gubernamentales sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional.

---

2 JOIN/2017/0450 final.

3 Documento de trabajo de los servicios de la Comisión – Resumen de la evaluación de impacto que acompaña a la propuesta de Reglamento del Parlamento Europeo y del Consejo, Parte 1/6, p. 21, Bruselas, 13.9.2017.

4 Eurobarómetro especial 464a – Wave EB87.4 – *Europeans' attitudes towards cyber security* (Actitud de los europeos frente a la ciberseguridad), septiembre de 2017.

2.8 La seguridad a través del diseño resulta clave para proporcionar bienes y servicios de alta calidad; los dispositivos inteligentes no son tan inteligentes si no están protegidos, y lo mismo ocurre con los coches inteligentes, las ciudades inteligentes y los hospitales inteligentes: todos precisan una seguridad integrada para dispositivos, sistemas, arquitecturas y servicios.

2.9 Los días 19 y 20 de octubre de 2017, el Consejo Europeo pidió la adopción de un planteamiento común de la ciberseguridad de la UE tras el paquete de reformas propuesto, solicitando «un planteamiento común de la ciberseguridad: el mundo digital se basa en la confianza, y esta solo puede lograrse si, en todas las políticas digitales, garantizamos una seguridad más proactiva desde su concepción, proporcionamos una certificación adecuada de seguridad de los productos y servicios y aumentamos nuestra capacidad para prevenir, disuadir, detectar y responder a los ciberataques»[5].

2.10 En su Resolución de 17 de mayo de 2017, el Parlamento Europeo «destaca la necesidad de garantizar la seguridad integral de toda la cadena de valor de los servicios financieros; señala los importantes y diversos riesgos que representan los ciberataques dirigidos contra la infraestructura de nuestros mercados financieros, la internet de las cosas, las monedas y los datos; [...] pide a las AES que revisen regularmente las normas operativas en vigor que cubren los riesgos relacionados con las TIC de las entidades financieras; solicita, por otra parte, la elaboración de directrices de las AES sobre la supervisión de esos riesgos; destaca la importancia de los conocimientos tecnológicos de las AES»[6].

2.11 El CESE ha tenido varias oportunidades previas para abordar esta cuestión[7], en particular, durante la Cumbre de Tallin, en la conferencia sobre el futuro desarrollo de la administración electrónica, y ha creado un Grupo de Estudio Permanente sobre la Agenda Digital[8].

3. Propuestas de la Comisión

3.1 El paquete de ciberseguridad incluye una Comunicación conjunta para revisar la anterior Estrategia de Ciberseguridad de la Unión Europea (2013), así como un Reglamento de Ciberseguridad centrado en el nuevo mandato de la ENISA y una propuesta de marco de certificación.

3.2 La estrategia se estructura en torno a tres secciones principales: resiliencia, disuasión y cooperación internacional. La parte de disuasión se centra principalmente en los asuntos relacionados con la ciberdelincuencia, incluido el Convenio de Budapest, y la parte de cooperación internacional se ocupa de ciberdefensa, ciberdiplomacia y cooperación con la OTAN.

---

5 Conclusiones del Consejo Europeo de 19 de octubre de 2017.

6 Resolución del Parlamento Europeo del 17 de mayo de 2017 - A8-0176/2017.

7 Mercado único digital: revisión intermedia.DO C 75 de 10.3.2017, p. 124, DO C 246 de 28.7.2017, p. 8, DO C 345 de 13.10.2017, p. 52, DO C 288 de 31.8.2017, p. 62, DO C 271 de 19.9.2013, p. 133.

8 Comunicado de prensa del CESE n.° 31/2017 *Civil Society debates E-government and cybersecurity with incoming Estonian Presidency* (La sociedad civil debate sobre la administración electrónica y la ciberseguridad con la futura Presidencia estonia): http://api.eesc.europa.eu/documents/eesc-2017-03031-00-00-cp-tra-en.docx

3.3 La propuesta presenta nuevas iniciativas, como:

- la creación de una Agencia de Ciberseguridad de la UE más fuerte;
- la introducción de un régimen de certificación de la ciberseguridad a escala de la UE, y
- la rápida aplicación de la Directiva SRI.

3.4 La parte de resiliencia propone medidas relacionadas con la ciberseguridad, en particular relativas a: cuestiones de mercado, la Directiva SRI, respuesta rápida de emergencia, desarrollo de las competencias, la educación y la formación de la UE en materia de cibercompetencias y ciberhigiene y sensibilización.

3.5 Al mismo tiempo, el Reglamento de Ciberseguridad propone la creación de un marco de certificación de la ciberseguridad de la UE para productos y servicios de TIC.

3.6 El Reglamento de Ciberseguridad también propone un papel más amplio para la ENISA en cuanto agencia de ciberseguridad de la UE, otorgando a la Agencia un mandato permanente. Además de sus responsabilidades actuales, se espera que la ENISA se ocupe de nuevas tareas de apoyo y coordinación relacionadas con el apoyo a la aplicación de la Directiva SRI, la Estrategia de Ciberseguridad de la UE, el plan director, la creación de capacidades, conocimientos e información, la sensibilización, tareas relacionadas con el mercado como apoyo a la normalización y la certificación, la investigación y la innovación, los ejercicios paneuropeos de ciberseguridad y la secretaría de la red de equipos de respuesta a incidentes de seguridad informática (CSIRT).

4. Observaciones generales – Resumen

4.1 Contexto: Resiliencia

4.1.1 Mercado único de la ciberseguridad

Deber de diligencia: El desarrollo del principio propuesto de «deber de diligencia» mencionado en la Comunicación conjunta sobre el uso de procesos seguros del ciclo de vida de desarrollo constituye un concepto interesante a desarrollar con la industria de la UE que podría conducir a un planteamiento global de la conformidad legal de la UE. Para la evolución futura, debería considerarse la seguridad por defecto.

Responsabilidad: La certificación facilitará la depuración de las responsabilidades en caso de litigio.

4.1.2 Directiva SRI: energía, transporte, banca/finanzas, sanidad, agua, infraestructura digital, comercio electrónico.

En opinión del CESE, la aplicación completa y efectiva de la Directiva SRI es esencial para garantizar la resiliencia de sectores críticos nacionales.

El CESE cree que debe reforzarse el intercambio de información entre agentes públicos y privados a través de centros sectoriales de puesta en común y análisis de la información (ISAC). Debe desarrollarse un mecanismo adecuado para intercambiar de forma segura información de confianza dentro de un ISAC y entre los CSIRT e ISAC sobre la base de una evaluación o análisis del mecanismo actualmente en uso.

4.1.3 Respuesta rápida de emergencia

El enfoque del «plan director» proporcionaría un proceso efectivo para una respuesta operativa a nivel de la UE y de los Estados miembros a un incidente a gran escala. El Comité subraya la necesidad de implicar al sector privado; también se deberían tomar en consideración los operadores de servicios esenciales del mecanismo de respuesta operativa, ya que podrían proporcionar información valiosa sobre amenazas o apoyar la detección de amenazas y crisis a gran escala y la respuesta a las mismas.

La Comunicación conjunta propone la incorporación de los ciberincidentes en los mecanismos de gestión de crisis de la UE. A pesar de que el CESE comprende la necesidad de una respuesta y solidaridad colectiva en caso de ataque, se precisa una mejor comprensión de cómo podría aplicarse esto, habida cuenta de que las ciberamenazas habitualmente se propagan entre países. Las herramientas empleadas en emergencias nacionales podrían compartirse solo parcialmente en caso de necesidad local.

4.1.4 Desarrollo de las competencias de la UE

Para que la UE sea realmente competitiva a escala mundial y para construir una base tecnológica sólida, es esencial crear un marco coherente y a largo plazo que abarque todas las etapas de la cadena de valor de la ciberseguridad. A este respecto, es fundamental fomentar la cooperación entre los ecosistemas regionales europeos para desarrollar una cadena de valor de la ciberseguridad europea. El CESE acoge favorablemente la propuesta de crear una red de competencias en el ámbito de la ciberseguridad.

Esta red podría apoyar la soberanía digital europea desarrollando una base industrial europea competitiva y reduciendo la dependencia de conocimientos desarrollados fuera de la Unión para capacidades tecnológicas clave, proporcionando ejercicios técnicos, talleres e incluso formación esencial en ciberhigiene para profesionales y no profesionales y fomentando —sobre la base del trabajo llevado a cabo por la asociación público-privada contractual— el desarrollo de una red de organizaciones público-privadas nacionales para apoyar el desarrollo de un mercado en Europa. «El desarrollo de la asociación público-privada contractual debe conducir a su optimización, adaptación o expansión» (Programa de trabajo sobre ciberseguridad del Trío de Presidencias EE-BG-AT)a través del establecimiento de una empresa común tripartita (Comisión, Estados miembros, empresas).

Para ser eficaz y alcanzar los objetivos que se propone a escala europea, la red debe basarse en un sistema de gobernanza bien definido.

Esta red estaría apoyada por un Centro de Investigación y Competencias sobre Ciberseguridad (CICC) a escala europea, encargado de conectar todos los centros de competencias nacionales existentes en la UE. El CICC no solo coordinaría y gestionaría la investigación, como en otras empresas comunes, sino que también permitiría el desarrollo efectivo de un ecosistema de ciberseguridad europeo que apoyaría la aplicación y el despliegue de la innovación de la UE.

4.2 **Contexto: Disuasión**

4.2.1 La lucha contra la ciberdelincuencia es una prioridad absoluta a escala nacional y europea que requiere un compromiso político firme. Las actividades de disuasión deben llevarse a cabo sobre la base de una asociación sólida entre los sectores público y privado, estableciendo un intercambio de información eficaz y desarrollando los conocimientos técnicos tanto a escala nacional como europea. Debe considerarse la posibilidad de extender las actividades de Europol a los ámbitos de informática forense y seguimiento.

4.3 **Contexto: Cooperación internacional**

4.3.1 Crear y mantener una cooperación con terceros países basada en la confianza a través de la ciberdiplomacia y las asociaciones empresariales es clave para reforzar la capacidad de Europa de impedir, disuadir y responder a ciberataques a gran escala. Europa debe impulsar la cooperación con Estados Unidos, China, Israel, India y Japón. La modernización de los controles a la exportación de la UE debe evitar las violaciones de derechos humanos o el uso indebido de tecnologías en contra de la propia seguridad de la UE, pero también debe garantizar que la industria de la UE no se vea penalizada respecto a otras ofertas de terceros países. Debería preverse una estrategia específica para los países candidatos a la adhesión a fin de prepararlos para el intercambio de datos transfronterizos sensibles. En particular, se podría brindar a estos países la posibilidad de participar, en calidad de observadores, en algunas actividades de la ENISA; los países deberían clasificarse en función de su disposición a luchar contra la ciberdelincuencia, y podría contemplarse la elaboración de una lista negra.

4.3.2 El CESE celebra la introducción de la ciberdefensa en la segunda fase prevista de un posible futuro centro de competencias de ciberseguridad de la UE. Por este motivo, Europa podría centrarse mientras tanto en el desarrollo de competencias de doble uso, incluidos el aprovechamiento del Fondo Europeo de Defensa y la creación prevista, a más tardar en 2018, de una plataforma de formación y de educación en ciberdefensa. Teniendo en cuenta las amenazas potenciales mutuamente reconocidas, el CESE considera necesario desarrollar la cooperación entre la UE y la OTAN. La industria europea también debería seguir de cerca la evolución de esta cooperación en materia de mejora de la interoperabilidad de las normas de ciberseguridad y otras formas de cooperación en el contexto del planteamiento de la UE en el ámbito de la ciberdefensa.

4.4 **Marco de certificación de la UE**

4.4.1 El CESE considera que Europa debe hacer frente al desafío de la fragmentación de la ciberseguridad mediante una interpretación homogénea de las normas, incluido el reconocimiento mutuo entre Estados miembros dentro de un marco unificado para facilitar la

protección de un mercado único digital. Un marco de certificación podría proporcionar una base común (con reglamentos específicos en los niveles superiores, si fuera necesario), garantizando sinergias entre los sectores verticales y reduciendo la fragmentación actual.

4.4.2 El CESE celebra la creación de un marco europeo de certificación de la ciberseguridad y de regímenes de certificación para los distintos sectores sobre la base de requisitos adecuados y en cooperación con las principales partes interesadas. Sin embargo, los plazos de comercialización y los costes de certificación, así como la calidad y la seguridad, constituyen elementos clave que deben tomarse en consideración. Se establecerán sistemas de certificación para aumentar la seguridad en función de los conocimientos actuales de las necesidades y amenazas; estos sistemas deberán ser flexibles y capaces de evolucionar para permitir las oportunas actualizaciones. Deberán preverse diferentes enfoques para los distintos sectores, en función de su modo de funcionamiento. Por lo tanto, el CESE considera que las agencias sectoriales de la UE (AESA, ABE, AFE, EMA, etc.) deberían participar en el proceso y, en ciertos casos y con el consentimiento de la ENISA, para evitar la duplicación de esfuerzos y la falta de coherencia, encargarse de elaborar regímenes de ciberseguridad.

4.4.3 Para el Comité resulta importante basar el marco de certificación en normas europeas en materia de ciberseguridad y de TIC, definidas en común a escala europea y, en la medida de lo posible, reconocidas a escala internacional. Teniendo en cuenta los plazos y las prerrogativas nacionales, se deben adoptar normas mínimas europeas para la seguridad informática en cooperación con el CEN, el Cenelec y el ETSI. Deben acogerse favorablemente las normas profesionales, pero no deben ser legalmente vinculantes ni obstaculizar la competencia.

4.4.4 Hay una necesidad patente de asociar el nivel de responsabilidades con los diferentes niveles de garantía basados en el impacto de las amenazas. Abrir el diálogo con las compañías de seguros podría contribuir a la adopción de requisitos de ciberseguridad efectivos en función del sector de aplicación. En opinión del CESE, se debe apoyar y otorgar incentivos a las empresas que buscan una «garantía de alto nivel», especialmente para dispositivos y sistemas críticos para la vida humana.

4.4.5 Dado el tiempo transcurrido desde la aprobación de la Directiva 85/374/CEE[9], el CESE le pide a la Comisión que, vista la evolución tecnológica existente, estudie la pertinencia de la inclusión en el ámbito de aplicación de esta Directiva de los supuestos contemplados en esta propuesta de Reglamento, para lograr productos más seguros y un elevado nivel de protección.

4.4.6 El CESE considera que el Grupo Europeo de Certificación de la Ciberseguridad previsto, apoyado por la ENISA, debería estar formado por autoridades nacionales de supervisión de la certificación, partes interesadas del sector privado y operadores de varios ámbitos de aplicación, a fin de garantizar el desarrollo de unos regímenes de certificación completos. Además, debería contemplarse la cooperación entre este grupo y asociaciones representativas del sector de la UE/EEE (por ej., asociación público-privada contractual, sector bancario, transporte, energía, federaciones, etc.) mediante el nombramiento de expertos. Dicho grupo debería tener en cuenta los resultados europeos en materia de certificación (principalmente sobre la base del Acuerdo de

9 DO L 210 de 7.8.1985, p. 29.

Reconocimiento Mutuo [ARM] del Grupo de altos funcionarios sobre seguridad de los sistemas de información [SOG-IS], los regímenes nacionales y los regímenes propietarios) y tratar de mantener las ventajas competitivas europeas.

4.4.7 El CESE propone que se otorgue a este grupo de partes interesadas la responsabilidad de preparar de forma conjunta regímenes de certificación junto con la Comisión Europea. También deberían definirse unos requisitos sectoriales a través de un acuerdo consensuado entre las partes interesadas (usuarios y proveedores) públicas y privadas.

4.4.8 Además, el grupo debería revisar periódicamente los regímenes de certificación, tomando en consideración los requisitos de cada sector, y adaptarlos cuando sea necesario.

4.4.9 El CESE apoya la eliminación progresiva de los regímenes de certificación nacionales cuando se introduzca un régimen europeo, como se propone en el artículo 49 del Reglamento. Un mercado único no puede funcionar con normas nacionales distintas y en competencia. A tal fin, el CESE sugiere realizar un censo de todos los regímenes nacionales.

4.4.10 El CESE sugiere que la Comisión ponga en marcha una acción para promover la certificación de la ciberseguridad y los certificados de ciberseguridad en la UE y apoye su reconocimiento en todos los acuerdos comerciales internacionales.

4.5 **La ENISA**

4.5.1 El CESE considera que el nuevo mandato permanente de la ENISA propuesto por la Comisión contribuirá de forma significativa a mejorar la resiliencia de los sistemas europeos. Sin embargo, el presupuesto provisional asociado y los recursos asignados a la ENISA reformada pueden no ser suficientes para que la Agencia cumpla su mandato.

4.5.2 El CESE anima a todos los Estados miembros a que establezcan una contraparte clara y similar a la ENISA, ya que la mayoría de ellos aún no lo ha hecho. Debería promoverse un programa estructurado a fin de enviar a expertos nacionales en comisión de servicios a la ENISA para apoyar el intercambio de las mejores prácticas y reforzar la confianza. El Comité también recomienda a la Comisión que vele por que se recojan y compartan las buenas prácticas actuales y las medidas eficaces existentes en los Estados miembros.

4.5.3 El CESE opina asimismo que, en términos de creación de capacidades, la ENISA debería dar prioridad a acciones dirigidas a apoyar la administración electrónica[10]. La identidad digital en la UE y en el mundo para las personas, las organizaciones, las empresas y los objetos es clave, y la prevención y la lucha contra la usurpación de identidad y el fraude en línea, así como la lucha contra la usurpación de los derechos de propiedad intelectual industrial, deben ser una prioridad.

4.5.4 La ENISA también debe proporcionar informes periódicos sobre la ciberpreparación de los Estados miembros, centrados principalmente en los sectores determinados en el anexo II de la Directiva SRI. Cada año, un ciberejercicio europeo debería evaluar la preparación de los

10 Mercado único digital: revisión intermedia

Estados miembros y la eficacia del mecanismo europeo de respuesta a cibercrisis y elaborar recomendaciones al respecto.

4.5.5 El CESE manifiesta su preocupación por la escasez de los recursos en términos de cooperación operativa, incluida la red de CSIRT.

4.5.6 Respecto de las tareas relacionadas con el mercado, el CESE considera que impulsar la cooperación con los Estados miembros y establecer una red formal de agencias de ciberseguridad ayudaría a apoyar la cooperación entre las partes interesadas[11]. El plazo de comercialización es muy reducido y resulta crítico para que las empresas de la UE puedan competir en este campo; la ENISA debería poder reaccionar al respecto. El CESE considera que, al igual que otras agencias de la Unión, la ENISA podría aplicar en el futuro un sistema de tasas y gravámenes. El CESE teme que la competición por las competencias entre la UE y las agencias nacionales pueda, como ha ocurrido en otros campos, retrasar el correcto establecimiento del marco reglamentario de la UE y perjudicar al mercado único de la UE.

4.5.7 El CESE observa que las tareas relacionadas con la investigación e innovación y la cooperación internacional son actualmente mínimas.

4.5.8 El CESE considera que la ciberseguridad debe ser objeto periódico de debate durante las reuniones conjuntas periódicas de las Agencias de Justicia y Asuntos de Interior (JAI) y que la ENISA y Europol deberían cooperar regularmente.

4.5.9 Dado que el cibermundo es muy innovador, es necesario estudiar cuidadosamente las normas para evitar obstaculizar la innovación, lo que requiere un marco dinámico; en la medida de lo posible, debería garantizarse tanto la compatibilidad futura como la retrocompatibilidad, con el fin de proteger las inversiones tanto de los ciudadanos como de las empresas.

4.5.10 Dada la importancia de las autoridades nacionales de supervisión de la certificación, el CESE sugiere que el Reglamento objeto de examen establezca ya una red formal de autoridades facultadas para resolver los problemas transfronterizos con el apoyo de la ENISA. En una fase posterior, la red podría evolucionar y convertirse en una agencia única.

4.5.11 Aunque la confianza es fundamental, la ENISA no podrá adoptar decisiones ni elaborar informes de auditoría. El CESE opina que la Agencia debería efectuar un seguimiento del rendimiento y la toma de decisiones de las autoridades nacionales de supervisión de la certificación mediante auditorías e inspecciones en nombre de la Comisión.

4.5.12 La participación en el consejo de administración de la ENISA debería ampliarse a la industria y a las organizaciones de consumidores, en calidad de observadores.

11 DO C 75 de 10.3.2017, p. 124.

4.6 **Industria, pymes, financiación/inversiones y modelos empresariales innovadores**

4.6.1 Industria e inversiones

A fin de aumentar la competitividad global de las empresas de la UE que operan en el ámbito de las TIC, las medidas deberían orientarse hacia un mejor apoyo del crecimiento y la competitividad de la industria de las TIC, incluidas las pymes.

Europa debería aumentar las inversiones haciendo converger diferentes fondos de la UE, fondos nacionales e inversiones del sector privado hacia los objetivos estratégicos, en el marco de una sólida cooperación entre los sectores público y privado. El nivel de inversión en sectores críticos debería aumentarse y apoyarse mediante la creación, en el actual y en el futuro programa marco de investigación, de un Fondo de Ciberseguridad de la UE para la Innovación y la I+D. Además, Europa debería crear un fondo para el despliegue de la ciberseguridad, abriendo una nueva perspectiva en el actual y en el futuro Mecanismo «Conectar Europa», así como en el próxima el FEIE 3.0.

Deberían crearse incentivos para que los Estados miembros de la UE adquieran soluciones europeas siempre que sea posible y elijan proveedores europeos siempre que estén disponibles, especialmente para las aplicaciones sensibles. Europa debe apoyar el crecimiento de cibercampeones europeos que puedan competir en el mercado mundial.

4.6.2 Pymes

Dada la fragmentación del mercado, es preciso conocer con mayor claridad la demanda de los clientes, a fin de responder mejor a las exigencias del mercado. Sin una demanda estructurada, ni las pymes ni las empresas emergentes pueden crecer a un ritmo rápido. En este contexto, sería positivo crear una plataforma europea de ciberseguridad para las pymes.

La tecnología de ciberseguridad está cambiando rápidamente y las pymes, gracias a su agilidad, pueden proveer las soluciones de vanguardia necesarias para seguir siendo competitivas. En comparación con los terceros países, la UE sigue buscando un modelo empresarial apropiado para las pymes.

Podrían diseñarse planes específicos para las nuevas empresas y las pymes, que permitan sufragar los costes de certificación para contrarrestar la gran dificultad de obtener fondos para su desarrollo tecnológico y comercial.

4.7 **El factor humano: educación y protección**

4.7.1 El CESE observa que la propuesta de la Comisión no tiene debidamente en consideración la persona humana como actor importante de los procesos digitales, ya sea como beneficiario o como causa de los principales incidentes informáticos.

4.7.2 Es necesario desarrollar una base sólida de cibercompetencias, mejorar la ciberhigiene y reforzar la sensibilización entre particulares y empresas. Para alcanzar este resultado, habrá que

realizar inversiones específicas, disponer de tiempo para formar a instructores de alto nivel y realizar campañas de sensibilización eficaces. La aplicación de estas tres líneas de acción requiere la participación de las autoridades nacionales y regionales (responsables de establecer programas educativos eficaces e invertir en ellos) y de las empresas y pymes, en el marco de un enfoque colectivo.

4.7.3 Debería considerarse la creación de un posible plan de estudios certificado por la UE para las escuelas secundarias y los profesionales con la participación activa de la ENISA y de sus homólogas nacionales. Además, deberá tomarse en consideración la igualdad de género al desarrollar los programas educativos para mejorar los niveles de empleo en ciberseguridad.

4.7.4 El CESE considera que la actividad de certificación debería incluir un sistema de etiquetado apropiado, tanto para los equipos como para los programas informáticos, como ocurre para muchos otros productos (por ejemplo los productos energéticos). Dicho instrumento contará con la triple ventaja de reducir los costes para las empresas, eliminar la fragmentación existente en el mercado a causa de los diferentes sistemas de certificación ya adoptados a escala nacional y facilitar la comprensión por parte de los consumidores de la calidad y las características del objeto adquirido. En este sentido, resulta importante que los productos importados de terceros países también se sometan a los mismos mecanismos de certificación y de etiquetado. Por último, el CESE considera que la creación de un logotipo ad hoc podría resultar práctico para comunicar de forma inmediata a los consumidores y los usuarios la fiabilidad de los productos adquiridos o de los sitios en los que se realizan operaciones de compraventa o que prevén la transmisión de datos sensibles.

4.7.5 La ENISA debería encargarse de una actividad fundamental de información y sensibilización a múltiples niveles, a fin de concienciar sobre los comportamientos digitales «seguros» y reforzar la confianza de los usuarios en internet. A tal fin, convendría implicar a las asociaciones de empresas, las asociaciones de consumidores y otros organismos que operan en el sector de los servicios digitales.

4.7.6 Como complemento de la Ley de Ciberseguridad, y con arreglo a lo que ya se propuso en el dictamen INT/828, el CESE considera crucial poner en marcha cuanto antes un amplio programa europeo destinado a la educación y formación digital para garantizar a todos los ciudadanos los instrumentos necesarios para afrontar la transición lo mejor posible. En particular, el CESE, consciente de las competencias nacionales específicas en la materia, espera que ese programa parta de las escuelas, reforzando los conocimientos de los docentes, adecuando los planes de estudio y la didáctica a las tecnologías digitales (incluido el e-learning) y facilitando a todos los estudiantes una formación de gran calidad. Tal programa será seguido del aprendizaje permanente para reajustar o actualizar las competencias de todos los trabajadores[12].

12 Mercado único digital: revisión intermedia

5. Observaciones específicas

5.1 Tecnologías y soluciones emergentes: el caso de la internet de las cosas

El número de dispositivos conectados aumenta constantemente y se espera que se multiplique con respecto al número de habitantes del planeta, debido a la digitalización de los componentes, sistemas y soluciones y a la mejora de la conectividad. Esta tendencia ofrece nuevas oportunidades a los ciberdelincuentes, sobre todo porque los dispositivos de la internet de las cosas a menudo no están tan bien protegidos como los dispositivos tradicionales.

Las normas de seguridad europeas en diferentes sectores verticales que utilizan dispositivos de internet de las cosas podrían reducir los esfuerzos, el tiempo y los costes de desarrollo para todos los agentes del sector en la cadena de valor de los productos conectados.

Es probable que se necesite algún tipo de nivel mínimo de seguridad mediante un servicio de gestión de identidad y acceso (IAM), reparación y gestión de dispositivos para los dispositivos «ordinarios» de «internet de las personas». Dado que la certificación es un método clave para proporcionar un nivel de seguridad más elevado, debería prestarse mayor atención a la seguridad de la internet de las cosas en el nuevo enfoque de la certificación de la UE.

Bruselas, 14 de febrero de 2018

Georges Dassis
Presidente del Comité Económico y Social Europeo