Dictamen del Comité Económico y Social Europeo sobre la «Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen el Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad y la Red de Centros Nacionales de Coordinación»

(COM(2018) 630 final — 2018/0328 (COD))

(2019/C 159/10)

Ponente: **Antonio LONGO**

Coponente: **Alberto MAZZOLA**

Consulta	Consejo Europeo, 5.10.2018 Parlamento Europeo, 1.10.2018
Fundamento jurídico	Artículo 173, apartado 3, y artículos 188 y 304 del Tratado de Funcionamiento de la Unión Europea
Sección competente	Transportes, Energía, Infraestructuras y Sociedad de la Información
Aprobado en sección	9.1.2019
Aprobado en el pleno	23.1.2019
Pleno n.º	540
Resultado de la votación (a favor/en contra/abstenciones)	143/5/2

1. Conclusiones y recomendaciones

1.1. El Comité Económico y Social Europeo (CESE) acoge favorablemente la iniciativa de la Comisión, que considera eficaz para el desarrollo de una estrategia industrial en materia de ciberseguridad y estratégica para conseguir una autonomía digital sólida y amplia. Estos factores representan una condición previa indispensable para reforzar los mecanismos de defensa europea frente a la guerra cibernética en curso, que puede poner en peligro los sistemas políticos, económicos y sociales.

1.2. El Comité destaca que no puede haber una estrategia en materia de ciberseguridad sin una concienciación generalizada y comportamientos seguros por parte de todos los usuarios.

1.3. El CESE comparte los objetivos generales de la propuesta y es consciente de que los aspectos específicos de funcionamiento serán objeto de un análisis posterior. No obstante, al tratarse de un Reglamento, considera que algunos aspectos sensibles relativos a la gobernanza, la financiación y la consecución de los objetivos fijados deberían definirse por anticipado. Es importante que, en la medida de lo posible, la Red y el Centro futuros se apoyen en las cibercapacidades y los conocimientos especializados de los Estados miembros y que las competencias no se concentren en el Centro que se cree. Además, deberá evitarse que los ámbitos de actividad de la Red y el Centro futuros no se solapen con los mecanismos de cooperación y las instituciones existentes.

1.4. El CESE defiende que se amplíe la colaboración al mundo industrial, sobre la base de compromisos firmes en términos científicos y de inversión, integrando en el futuro a sus representantes en el Consejo de Administración. En el caso de una colaboración tripartita entre la Comisión Europea, los Estados miembros y la industria, la presencia de empresas procedentes de terceros países debería limitarse a las establecidas desde hace tiempo en territorio europeo y plenamente implicadas en la base tecnológica e industrial europea, a condición de que se sometan a mecanismos adecuados de escrutinio y control, así como al respeto del principio de reciprocidad y de las obligaciones de confidencialidad.

1.5. La ciberseguridad ha de ser un compromiso común de todos los Estados miembros, por lo que estos deben participar en el Consejo de Administración mediante formas por concretar. En cuanto a la contribución financiera de los Estados miembros, se podría obtener de los fondos europeos destinados a cada uno.

1.6. La propuesta debería explicar mejor las modalidades de intervención del Centro para coordinar las financiaciones procedentes de los programas Europa Digital y Horizonte Europa, y, en particular, qué directrices regirán la redacción y adjudicación de posibles contratos. Este aspecto es fundamental para evitar duplicaciones o solapamientos. Además, para incrementar la dotación financiera, se recomienda ampliar las sinergias con otros instrumentos financieros de la UE (por ejemplo, fondos regionales, Fondos Estructurales, MCE, EDF, InvestEU, etc.).

1.7. El CESE considera fundamental definir las modalidades de cooperación y las relaciones entre el Centro europeo y los centros nacionales. Además, es importante que los centros nacionales estén financiados por la UE, al menos en lo que atañe a los costes administrativos, facilitando la armonización administrativa y en materia de competencias para reducir la brecha existente entre los Estados europeos.

1.8. El Comité resalta la importancia del capital humano y espera que el Centro de Competencia pueda promover, en colaboración con las universidades, los centros de investigación y los centros de formación superior, así como una educación y formación de excelencia, que incluya planes de estudios universitarios específicos y en centros de enseñanza superior. Del mismo modo, es esencial prever un apoyo específico para las empresas emergentes y las pymes.

1.9. El CESE considera fundamental aclarar mejor los ámbitos de competencia y la división entre los mandatos del Centro y de la Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA), definiendo con claridad las modalidades de colaboración y apoyo mutuo y evitando solapamientos de competencias y la duplicación de esfuerzos. Problemas de índole similar se plantean con otros organismos que se ocupan de la ciberseguridad, como la AED, Europol y CERT-EU, por lo que se recomienda la creación de mecanismos de diálogo estructurado análogos entre estos.

2. **Contexto actual de la ciberseguridad**

2.1. La ciberseguridad es una de las principales cuestiones de la agenda de la UE, pues es un elemento irrenunciable para la defensa de las instituciones, las empresas y los ciudadanos, así como un instrumento necesario para el propio mantenimiento de las democracias. Entre los fenómenos más preocupantes cabe señalar el aumento exponencial de los programas informáticos maliciosos difundidos por la red a través de sistemas automáticos, que pasaron de 130000 en 2007 a ocho millones en 2017. Además, la Unión es un importador neto de productos y soluciones de ciberseguridad, lo que genera un problema de competitividad económica y de seguridad civil y militar.

2.2. Si bien la UE puede presumir de importantes competencias y experiencias en el ámbito de la ciberseguridad, la industria del sector, las universidades y los centros de investigación resultan aún fragmentados, descoordinados y desvinculados de una estrategia de desarrollo compartida. Ello se debe a que los sectores pertinentes en materia de ciberseguridad (por ejemplo, energía, espacio, defensa y transportes) no reciben un apoyo adecuado, y a que tampoco se valorizan las sinergias entre la ciberseguridad civil y de la defensa.

2.3. Para hacer frente a los crecientes desafíos, la Unión adoptó la Estrategia de ciberseguridad de 2013 con el fin de fomentar un ecosistema cibernético fiable, seguro y abierto ([1]). Posteriormente, en 2016, se adoptaron las primeras medidas específicas para la seguridad de las redes y los sistemas de información ([2]). Este proceso condujo a la creación de la asociación público-privada contractual sobre la ciberseguridad.

2.4. En 2017, la Comunicación titulada «Resiliencia, disuasión y defensa: fortalecer la ciberseguridad de la UE» ([3]) destacaba la necesidad de garantizar que se conservasen y desarrollasen las capacidades tecnológicas esenciales en materia de ciberseguridad para proteger el mercado único digital y, en particular, para proteger las redes y los sistemas de información fundamentales y prestar servicios clave de ciberseguridad.

([1]) JOIN(2013) 1 final.
([2]) Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (DO L 194 de 19.7.2016, p. 1).
([3]) JOIN(2017) 450 final.

2.5. Por tanto, la Unión debe estar en condiciones de garantizar la seguridad de sus recursos y procesos digitales y de competir en el mercado mundial de la ciberseguridad hasta alcanzar una sólida y amplia autonomía digital ([4]).

3. Propuestas de la Comisión

3.1. El Centro de Competencia (en lo sucesivo, el «Centro») tendrá por objetivo facilitar y contribuir a coordinar el trabajo de la Red de Centros Nacionales y alimentar la Comunidad de Competencias en Ciberseguridad, impulsando el programa tecnológico de ciberseguridad y facilitando el acceso a los conocimientos especializados reunidos de este modo.

3.2. En particular, el Centro ejecutará las partes pertinentes de los programas Europa Digital y Horizonte Europa, asignando subvenciones y efectuando contrataciones. Habida cuenta de las considerables inversiones en materia de ciberseguridad realizadas en otras partes del mundo y de la necesidad de coordinar y poner en común los recursos necesarios en Europa, se propone que el Centro de Competencia revista la forma de una Asociación Europea con un doble fundamento jurídico, de modo que se faciliten las inversiones conjuntas de la Unión, los Estados miembros y la industria.

3.3. En la propuesta se pide a los Estados miembros que contribuyan con un importe adecuado a las actuaciones del Centro de Competencia y de la Red. La dotación financiera prevista por la UE asciende a unos 2000 millones EUR por parte del programa Europa Digital; un importe por determinar procedente del programa Horizonte Europa; y una contribución global de los Estados miembros al menos igual a la comunitaria.

3.4. El principal órgano de toma de decisiones es el Consejo de Administración, en el que intervienen todos los Estados miembros, si bien solo tienen derecho a voto los que participan financieramente. El mecanismo de votación se rige por un principio de doble mayoría que exige el 75 % de la contribución financiera y el 75 % de los votos. La Comisión poseerá el 50 % de los votos. El Centro contará con la asistencia de un Consejo Consultivo Industrial y Científico, a fin de garantizar el diálogo con las empresas, los consumidores y otras partes interesadas pertinentes.

3.5. Trabajando en estrecho contacto con la Red de Centros Nacionales de Coordinación y la Comunidad de Competencias en Ciberseguridad, el Centro será el órgano ejecutivo principal para los recursos financieros de la UE consagrados a la seguridad informática en el ámbito de los programas propuestos, Europa Digital y Horizonte Europa.

3.6. Los Estados miembros seleccionarán los centros nacionales de coordinación. Estos deberán poseer o tener acceso directo a conocimientos tecnológicos especializados en materia de ciberseguridad, especialmente en ámbitos como la criptografía, los servicios de seguridad de TIC, la detección de intrusiones, la seguridad de los sistemas, la seguridad de las redes, la seguridad de los programas informáticos y las aplicaciones, o los aspectos humanos y sociales de la seguridad y la privacidad. También se requiere que tengan la capacidad de interactuar y coordinarse eficazmente con la industria y el sector público, incluidas las autoridades designadas con arreglo a la Directiva (UE) 2016/1148.

4. Observaciones generales

4.1. El CESE acoge favorablemente la iniciativa de la Comisión y la considera estratégica para el desarrollo de la ciberseguridad, en aplicación de lo decidido en la Cumbre de Tallin de septiembre de 2017. En tal ocasión, los jefes de Estado o de Gobierno pidieron que la Unión se convirtiera en «*un líder mundial en ciberseguridad para 2025, a fin de garantizar la confianza, la seguridad y la protección de nuestros ciudadanos, consumidores y empresas en línea y permitir una internet libre y legal*».

4.2. El CESE resalta que está en curso una auténtica guerra cibernética que puede poner en peligro los sistemas políticos, económicos y sociales, atacando los sistemas informáticos de instituciones, infraestructuras críticas (energía, transportes, bancos y entidades financieras, etc.) y empresas, y también condicionando con noticias falsas los procesos electorales y democráticos en general ([5]). Es necesaria, por tanto, una sólida toma de conciencia y una reacción firme y oportuna. Por estas razones, es preciso establecer una estrategia industrial de ciberseguridad que sea clara y cuente con un apoyo adecuado, como condición previa indispensable para el logro de la autonomía digital. El CESE considera que el programa de trabajo debería dar prioridad a los sectores identificados en la Directiva (UE) 2016/1148, que se aplica a las empresas proveedoras de servicios esenciales, ya sean públicas o privadas, debido a la importancia que estos revisten para la sociedad ([6]).

([4]) DO C 227 de 28.6.2018, p. 86.

([5]) Informe sobre «La forma en que los medios de comunicación se utilizan para influir en los procesos sociales y políticos en la UE y los países de la Asociación Oriental», Sra. Vareikytė, 2014.

([6]) DO C 227 de 28.6.2018, p. 86.

4.3. El Comité destaca que no puede haber una estrategia en materia de ciberseguridad sin una concienciación generalizada y comportamientos seguros por parte de todos los usuarios. Por esta razón, toda iniciativa tecnológica ha de ir acompañada de campañas de información y sensibilización adecuadas a fin de crear una «cultura de la seguridad digital» ([7]).

4.4. El CESE comparte los objetivos generales de la propuesta y es consciente de que los aspectos específicos de funcionamiento serán objeto de un análisis posterior. No obstante, al tratarse de un Reglamento, considera que algunos aspectos sensibles relativos a la gobernanza, la financiación y la consecución de los objetivos fijados deberían definirse por anticipado. Es importante que, en la medida de lo posible, la Red y el Centro futuros se apoyen en las cibercapacidades y los conocimientos especializados de los Estados miembros y que las competencias no se concentren en el Centro que se cree. Además, deberá evitarse que los ámbitos de actividad de la Red y el Centro futuros no se solapen con los mecanismos de cooperación y las instituciones existentes.

4.5. El CESE recuerda que, en su Dictamen TEN/646 sobre el Reglamento de Ciberseguridad ([8]), propuso una colaboración tripartita APP entre la Comisión Europea, los Estados miembros y la industria, incluyendo a las pymes, mientras que la estructura actual, cuya forma jurídica debe analizarse mejor, prevé en esencia una asociación público-privada entre la Comisión Europea y los Estados miembros.

4.6. El CESE defiende que se amplíe la colaboración al mundo industrial, sobre la base de compromisos firmes en términos científicos y de inversión, integrando en el futuro a sus representantes en el Consejo de Administración. La creación de un Consejo Consultivo Industrial y Científico podría no garantizar el diálogo constante con las empresas, los consumidores y otras partes interesadas pertinentes. Además, en el nuevo contexto trazado por la Comisión no parece claro qué papel desempeñará la Organización de Ciberseguridad Europea, creada en junio de 2016 con el estímulo de la Comisión en calidad de contraparte de esta última y cuyo capital de red y conocimientos no debería perderse.

4.6.1. En el caso de una colaboración tripartita, es importante prestar atención a las empresas procedentes de terceros países. En particular, el CESE destaca que esta debería basarse en un mecanismo riguroso que evite la presencia de empresas procedentes de Estados no pertenecientes a la UE que puedan obstaculizar la seguridad y la autonomía de la Unión. Las correspondientes cláusulas definidas en el Programa Europeo de Desarrollo Industrial en materia de Defensa ([9]) deberían aplicarse también en este contexto.

4.6.2. Al mismo tiempo, el CESE reconoce que algunas empresas procedentes de países no pertenecientes a la UE, pero establecidas desde hace tiempo en territorio europeo y plenamente implicadas en la base tecnológica e industrial europea, podrían ser muy útiles para los proyectos comunitarios, y deberían tener acceso, a condición de que los Estados miembros establezcan mecanismos adecuados de escrutinio y control de esas empresas, así como de que estas últimas respeten el principio de reciprocidad y las obligaciones de confidencialidad.

4.7. La ciberseguridad ha de ser un compromiso común de todos los Estados miembros, por lo que estos deben participar en el Consejo de Administración mediante formas por concretar. Es importante asimismo que todos los Estados contribuyan financieramente y de forma adecuada a la iniciativa de la Comisión. En cuanto a la contribución financiera de los Estados miembros, se podría obtener de los fondos europeos destinados a cada uno.

4.8. El CESE está de acuerdo con que cada Estado miembro sea libre para designar a su representante en el Consejo de Administración del Centro Europeo de Competencia. El Comité recomienda que se defina con claridad el currículo de los representantes nacionales, que debería integrar las competencias estratégicas y tecnológicas con aquellas en materia de gestión, administración y finanzas.

4.9. La propuesta debería explicar mejor las modalidades de intervención del Centro para coordinar las financiaciones procedentes de los programas Europa Digital y Horizonte Europa, todavía en curso de negociación, y, en particular, qué directrices regirán la redacción y adjudicación de posibles contratos. Este aspecto es fundamental para evitar duplicaciones o solapamientos. Además, para incrementar la dotación financiera, se recomienda ampliar las sinergias con otros instrumentos financieros de la UE (por ejemplo, fondos regionales, Fondos Estructurales, MCE, EDF, InvestEU, etc.). El Comité espera que la Red de Centro Nacionales participe en la gestión y coordinación de los fondos.

([7]) DO C 227 de 28.6.2018, p. 86.
([8]) DO C 227 de 28.6.2018, p. 86.
([9]) COM(2017) 294.

4.10. El CESE señala que el Consejo Consultivo debería tener dieciséis miembros y que no se especifican los mecanismos con los que debería llegarse al mundo empresarial, las universidades, la investigación y los consumidores. El Comité considera que sería útil y adecuado que los miembros de dicho Consejo destacaran por unos elevados conocimientos en la materia y representaran de forma equilibrada a los distintos sectores implicados.

4.11. El CESE considera importante definir las modalidades de cooperación y las relaciones entre el Centro europeo y los centros nacionales. Además, es importante que los centros nacionales estén financiados por la UE, al menos en lo que atañe a los costes administrativos, facilitando la armonización administrativa y en materia de competencias para reducir la brecha existente entre los Estados europeos.

4.12. En consonancia con sus dictámenes anteriores ([10]), el CESE resalta la importancia de la educación y la formación de excelencia de recursos humanos en el sector de la ciberseguridad, también mediante cursos escolares, universitarios y de posgrado específicos. Es importante asimismo brindar un apoyo financiero adecuado a las pymes y empresas emergentes del sector ([11]), que son fundamentales en el desarrollo de la investigación de vanguardia.

4.13. El CESE considera fundamental aclarar mejor los ámbitos de competencia y la división entre los mandatos del Centro y de ENISA, definiendo con claridad las modalidades de colaboración y apoyo mutuo y evitando solapamientos de competencias y la duplicación de esfuerzos ([12]). En la propuesta de Reglamento se prevé la presencia de un delegado de la ENISA como observador permanente en el Consejo de Administración, pero dicha presencia no garantiza un diálogo estructurado entre los dos organismos. Problemas de índole similar se plantean con otros organismos que se ocupan de la ciberseguridad, como la AED, EUROPOL y CERT-EU. A este respecto, es interesante el memorando de entendimiento firmado en mayo de 2018 entre la ENISA, la AED, EUROPOL y CERT-EU.

Bruselas, 23 de enero de 2019.

El Presidente
del Comité Económico y Social Europeo
Luca JAHIER

([10]) DO C 451 de 16.12.2014, p. 25.
([11]) DO C 227 de 28.6.2018, p. 86.
([12]) DO C 227 de 28.6.2018, p. 86.