Consejo de la Unión Europea

Bruselas, 2 de diciembre de 2020
(OR. en)

13629/20

CYBER 263
TELECOM 248
COPEN 362
CODEC 1266
COPS 441
COSI 235
CSC 344
CSCI 86
IND 248
RECH 493
ESPACE 77

RESULTADO DE LOS TRABAJOS

De:	Secretaría General del Consejo
Fecha:	2 de diciembre de 2020
A:	Delegaciones
Asunto:	Conclusiones del Consejo sobre la ciberseguridad de los dispositivos conectados – Conclusiones del Consejo adoptadas por procedimiento escrito

Adjunto se remite a las delegaciones las Conclusiones del Consejo sobre la ciberseguridad de los dispositivos conectados, adoptadas por el Consejo mediante procedimiento escrito el 2 de diciembre de 2020.

ANEXO

Conclusiones del Consejo sobre la ciberseguridad de los dispositivos conectados

El Consejo de la Unión Europea,

RECORDANDO LO SIGUIENTE:

- las Conclusiones del Consejo sobre la Comunicación conjunta al Parlamento Europeo y al Consejo titulada «Resiliencia, disuasión y defensa: fortalecer la ciberseguridad de la UE»
- las Conclusiones del Consejo sobre el desarrollo de capacidades y competencias en materia de ciberseguridad en la UE,
- las Conclusiones del Consejo sobre la importancia de la tecnología 5G para la economía europea y la necesidad de mitigar los riesgos para la seguridad relacionados con la 5G,
- las Conclusiones del Consejo sobre el futuro de una Europa altamente digitalizada más allá de 2020: «Impulsar la competitividad digital y económica en toda la Unión y la cohesión digital»,
- las Conclusiones del Consejo sobre la configuración del futuro digital de Europa,
- las Conclusiones del Consejo Europeo sobre la COVID-19, el mercado único, la política industrial, el ámbito digital y las relaciones exteriores,
- la Comunicación de la Comisión Europea titulada «Configurar el futuro digital de Europa»,

1. DESTACA que la Unión Europea y sus Estados miembros deben garantizar su soberanía digital y su autonomía estratégica, preservando al mismo tiempo una economía abierta. Ello implica reforzar la capacidad de tomar decisiones tecnológicas autónomas y desarrollar infraestructuras, productos y servicios resilientes y seguros, que son uno de los pilares principales, con el fin de generar confianza en el mercado único digital y en la sociedad europea. Los valores fundamentales de la Unión Europea protegen, en particular, la privacidad, la seguridad, la igualdad, la dignidad humana, el Estado de Derecho y una internet abierta, todos ellos elementos indispensables para lograr una sociedad, una economía y una industria digitalizadas y centradas en el ser humano.

2. RECONOCE la creciente importancia de los dispositivos conectados y de su seguridad, incluidos las máquinas, los sensores y las redes que componen la internet de las cosas. Los dispositivos conectados tendrán un papel clave en la ulterior configuración del futuro digital de Europa, desde el punto de vista industrial y empresarial, así como en la vida cotidiana de los consumidores de una nueva generación tecnológica. Además de la 5G, la inteligencia artificial, la informática cuántica, la informática de alto rendimiento, la computación en nube, las tecnologías de registro descentralizado y en particular la cadena de bloques y otras nuevas aplicaciones y oportunidades encaminadas a lograr un crecimiento económico sostenible y un mayor nivel de digitalización en nuestra sociedad solo pueden alcanzarse mediante dispositivos conectados y ciberseguros.

3. SEÑALA que el aumento del uso de productos de consumo y dispositivos industriales conectados a internet también planteará nuevos riesgos para la privacidad, la información y la ciberseguridad, en particular, un aumento de las posibles repercusiones sobre la integridad y la disponibilidad de productos y datos, lo que puede afectar de manera directa a la seguridad. Minimizar dichos riesgos es esencial para proteger a los consumidores, reforzar la resiliencia cibernética general de Europa y reforzar la confianza que los ciudadanos depositan en las soluciones y las tecnologías digitales. Esto además contribuirá a fomentar la competitividad y las capacidades de innovación de los proveedores europeos de esos dispositivos. La ciberseguridad y la privacidad deben considerarse requisitos esenciales en la innovación de productos, así como en los procesos de producción y desarrollo, incluida la fase de diseño (seguridad desde el diseño), y deben garantizarse a lo largo de todo el ciclo de vida del producto y en toda su cadena de suministro.

4. HACE HINCAPIÉ en que, además de garantizar un alto nivel de seguridad de los dispositivos conectados, también es importante sensibilizar más a los consumidores sobre los riesgos que estos dispositivos pueden generan para la privacidad y la seguridad. Ello contribuiría a minimizar las amenazas que se derivan de un mayor uso de los dispositivos conectados, reforzar la confianza en el mercado único digital y aprovechar al máximo los beneficios económicos y sociales que ofrecen las tecnologías de los dispositivos conectados.

5. SUBRAYA que las inversiones públicas en investigación e innovación, en particular, a través de los programas Horizonte Europa y Europa Digital, así como las inversiones privadas, podrían constituir un valioso incentivo para mejorar la seguridad y la protección de los dispositivos conectados y, por tanto, mejorar la resiliencia de las redes de comunicación inteligentes. También deben acelerarse las inversiones en las infraestructuras y tecnologías digitales necesarias para el despliegue de las últimas tecnologías de dispositivos conectados, con el fin de alcanzar el liderazgo industrial y digital y de garantizar la autonomía estratégica, al tiempo que se mantiene una economía abierta.

6. DESTACA que es necesario garantizar un nivel elevado de complementariedad y comparabilidad de las funcionalidades de seguridad de los sistemas y componentes de TIC, que se utilizan en muchos sectores distintos del mercado único digital.

7. RECONOCE los avances que se están produciendo a escala de la Unión para elevar el nivel de ciberseguridad de los dispositivos conectados, en particular, con respecto a las iniciativas que la Comisión ha adoptado recientemente para abordar, a corto plazo, cuestiones de ciberseguridad en los actos jurídicos pertinentes, por ejemplo los actos en virtud del nuevo marco legislativo, y en particular la Directiva 2014/53/UE (Directiva sobre Equipos Radioeléctricos). SUBRAYA que es importante evaluar si se precisa de una legislación horizontal, que especifique también las condiciones necesarias para la comercialización, para abordar a largo plazo todas las cuestiones pertinentes de la ciberseguridad de los dispositivos conectados, como la disponibilidad, la integridad y la confidencialidad. ACOGE FAVORABLEMENTE, a este respecto, la celebración de un debate para estudiar el ámbito de aplicación de dicha legislación y sus vínculos con el marco de certificación de la ciberseguridad que se define en el Reglamento sobre la Ciberseguridad, con el objetivo de elevar el nivel de seguridad en el mercado único digital.

8. SUBRAYA que los requisitos de ciberseguridad deben definirse con arreglo a la legislación pertinente de la Unión, incluidos el Reglamento sobre la Ciberseguridad, el nuevo marco legislativo, el Reglamento sobre la Normalización Europea y la posible futura legislación horizontal, con el fin de evitar la ambigüedad y la fragmentación de la legislación.

9. RECONOCE que todas las partes interesadas, en particular los fabricantes, desempeñan un papel importante a la hora de elevar el nivel de ciberseguridad de los dispositivos conectados en el mercado único digital; por tanto, PIDE que se establezca una coordinación y una estrecha cooperación con todas las partes interesadas pertinentes de los sectores público y privado, también de cara a una posible legislación horizontal en el futuro.

9 *bis*. ACOGE CON SATISFACCIÓN la labor que está llevando a cabo la Agencia de la Unión Europea para la Ciberseguridad (ENISA) para elaborar los primeros esquemas de certificación de la UE, a saber, la propuesta de criterios comunes de la Unión Europea y la propuesta de esquemas relativos a los servicios en la nube. Estos esquemas constituyen una base importante para la certificación de dispositivos conectados.

10. HACE HINCAPIÉ en que cualquier esquema de certificación adicional de dispositivos conectados y de servicios relacionados que se establezca en el programa de trabajo evolutivo de la Unión y se defina con arreglo al Reglamento sobre la Ciberseguridad debe especificar cómo han de cumplirse los requisitos de seguridad aplicables al nivel de garantía pertinente, conforme a las normas específicas europeas reconocidas a nivel internacional —independientemente del sector en el que vaya a utilizarse el producto—, y qué especificaciones en materia de ensayo, certificaciones, etc., deben aplicarse.

11. RECONOCE que la certificación de dispositivos conectados exigiría normas, criterios y especificaciones técnicas pertinentes para las evaluaciones de ciberseguridad en el marco del Reglamento sobre la Ciberseguridad. Por tanto, HACE HINCAPIÉ en que es necesario establecer normas, criterios o especificaciones técnicas en materia de ciberseguridad para los dispositivos conectados y RECOMIENDA reforzar la labor de las organizaciones europeas de normalización en este ámbito. Al mismo tiempo, SEÑALA que la norma ETSI EN 303 645 en materia de ciberseguridad para los dispositivos de consumo de la internet de las cosas constituye un paso importante en este sentido.

12. PIDE a la Comisión que considere solicitar propuestas de esquemas de certificación de la ciberseguridad para dispositivos conectados y servicios relacionados, sobre la base del programa de trabajo evolutivo de la Unión, tomando en la mayor consideración posible los esquemas de certificación europeos horizontales que se están desarrollando actualmente. De forma voluntaria, dicho esquema permitirá que los fabricantes de esos productos promocionen productos que presenten el nivel de garantía evaluado.

13. PROPONE que se organice un debate para estudiar de qué modo puede integrarse el objetivo de la ciberseguridad en una futura legislación horizontal en la que se aborden los riesgos de ciberseguridad relacionados con los dispositivos conectados, y al mismo tiempo SEÑALA que es necesario considerar, cuando proceda, la adaptación de los requisitos esenciales que se recogen en las respectivas Directivas del nuevo marco legislativo.

14. ANIMA a la Comisión a que también examine, cuando sea necesario, los reglamentos sectoriales complementarios que definan el nivel de ciberseguridad que deben cumplir los dispositivos conectados, con el fin de garantizar que se establezcan requisitos específicos en materia de seguridad y privacidad para los dispositivos que presentan mayores riesgos para la seguridad.

15. SUBRAYA la necesidad de mejorar la calidad de vida y el bienestar de los ciudadanos europeos y fomentar la confianza en el mercado único digital. La seguridad y la privacidad de nuestras sociedades son esenciales para preservar los valores fundamentales de la Unión. Por tanto, INSISTE en la necesidad de utilizar como base el marco que proporciona el Reglamento sobre la Ciberseguridad para armonizar los requisitos de seguridad en todos los sectores del nuevo marco legislativo, en función de los distintos niveles de garantía, con el fin de evitar la fragmentación y la verificación repetida de requisitos idénticos, y ofrecer unas condiciones equitativas en materia de competencia e innovación en toda la Unión Europea.

16. PIDE a la Comisión, a la Agencia de la Unión Europea para la Ciberseguridad (ENISA), al Comité de Vigilancia del Mercado y Evaluación de la Conformidad en materia de Telecomunicaciones y al Grupo Europeo de Certificación de la Ciberseguridad que participen activamente en esta iniciativa que pretende reforzar el mercado único digital y la confianza en los productos, servicios y procesos de TIC para dispositivos conectados, garantizando la privacidad y la ciberseguridad, y que contribuyan a que la industria europea de la internet de las cosas sea más competitiva a nivel mundial, garantizando el máximo nivel de resiliencia, seguridad y protección.

17. DESTACA, en este contexto, que es necesario apoyar a las pymes, que constituyen un pilar esencial del ecosistema europeo de la ciberseguridad, y ANIMA a las pymes a que participen en todas las consultas públicas que se organicen, así como en actividades de normalización, con el fin de tener en cuenta su importante y valiosa contribución a la hora de hacer de la ciberseguridad un objetivo alcanzable, así como una ventaja competitiva en el mercado europeo.

18. SEÑALA que la obligación de garantizar la ciberseguridad y la privacidad a lo largo de todo el ciclo de vida de un producto y en toda su cadena de suministro podría tener efectos positivos para la huella ambiental del sector tecnológico al orientar a los fabricantes hacia unos procesos de desarrollo y producción inteligentes y sostenibles, lo que contribuiría a reducir el volumen de residuos electrónicos procedente de la eliminación de los dispositivos conectados.