P9_TA(2021)0286

Estrategia de Ciberseguridad de la UE para la Década Digital

Resolución del Parlamento Europeo, de 10 de junio de 2021, sobre la Estrategia de Ciberseguridad de la UE para la Década Digital (2021/2568(RSP))

(2022/C 67/08)

El Parlamento Europeo,

— Vista la Comunicación conjunta de la Comisión y el alto representante de la Unión para Asuntos Exteriores y Política de Seguridad, de 16 de diciembre de 2020, titulada «La Estrategia de Ciberseguridad de la UE para la Década Digital» (JOIN(2020)0018),

— Vista la propuesta de la Comisión, de 16 de diciembre de 2020, de una Directiva del Parlamento Europeo y del Consejo relativa a medidas destinadas a garantizar un elevado nivel común de ciberseguridad y por la que se deroga la Directiva (UE) 2016/1148 (COM(2020)0823),

— Vista la propuesta de la Comisión, de 24 de septiembre de 2020, de Reglamento del Parlamento Europeo y del Consejo sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014 y (UE) n.º 909/2014 (COM(2020)0595),

— Vista la propuesta de la Comisión, de 12 de septiembre de 2018, 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)0630),

— Vista la Comunicación de la Comisión, de 19 de febrero de 2020, titulada «Configurar el futuro digital de Europa» (COM(2020)0067),

— Visto el Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n.º 526/2013 («Reglamento sobre la Ciberseguridad») ([1]),

— Vista la Directiva 2014/53/UE del Parlamento Europeo y del Consejo, de 16 de abril de 2014, relativa a la armonización de las legislaciones de los Estados miembros sobre la comercialización de equipos radioeléctricos, y por la que se deroga la Directiva 1999/5/CE ([2]),

— Vista la Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2018, por la que se establece el Código Europeo de las Comunicaciones Electrónicas ([3]),

— Visto el Reglamento (UE) n.º 1290/2013 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2013, por el que se establecen las normas de participación y difusión aplicables a Horizonte 2020, Programa Marco de Investigación e Innovación (2014-2020) y por el que se deroga el Reglamento (CE) n.º 1906/2006 ([4]),

— Visto el Reglamento (UE) n.º 1291/2013 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2013, por el que se establece Horizonte 2020 — Programa Marco de Investigación e Innovación (2014-2020) y por el que se deroga la Decisión n.º 1982/2006/CE ([5]),

— Visto el Reglamento (UE) 2021/694 del Parlamento Europeo y del Consejo, de 29 de abril de 2021, por el que se establece el Programa Europa Digital y por el que se deroga la Decisión (UE) 2015/2240 ([6]),

([1]) DO L 151 de 7.6.2019, p. 15.
([2]) DO L 153 de 22.5.2014, p. 62.
([3]) DO L 321 de 17.12.2018, p. 36.
([4]) DO L 347 de 20.12.2013, p. 81.
([5]) DO L 347 de 20.12.2013, p. 104.
([6]) DO L 166 de 11.5.2021, p. 1.

— Vista la Directiva 2010/40/UE del Parlamento Europeo y del Consejo, de 7 de julio de 2010, por la que se establece el marco para el despliegue de los sistemas de transporte inteligentes en el sector del transporte por carretera y para las interfaces con otros modos de transporte ([7]),

— Visto el Convenio de Budapest sobre la Ciberdelincuencia, de 23 de noviembre de 2001, (STE n.º 185),

— Vista su Resolución, de 16 de diciembre de 2020, sobre una nueva estrategia para las pymes europeas ([8]),

— Vista su Resolución, de 25 de marzo de 2021, sobre una Estrategia Europea de Datos ([9]),

— Vista su Resolución, de 20 de mayo de 2021, sobre la configuración del futuro digital de Europa: eliminación de los obstáculos al funcionamiento del mercado único digital y mejora del uso de la inteligencia artificial para los consumidores europeos ([10]),

— Vista su Resolución, de 21 de enero de 2021, sobre el cierre de la brecha digital de género: participación de la mujer en la economía digital ([11]),

— Vista su Resolución, de 12 de marzo de 2019, sobre las amenazas en materia de seguridad relacionadas con la creciente presencia tecnológica de China en la Unión y la posible acción a escala de la Unión para reducirlas ([12]),

— Vista la pregunta a la Comisión sobre la Estrategia de Ciberseguridad de la UE para la Década Digital (O-000037/2021 — B9-0024/2021),

— Vistos el artículo 136, apartado 5, y el artículo 132, apartado 2, de su Reglamento interno,

A. Considerando que la transformación digital es una prioridad estratégica clave de la Unión que está asociada inevitablemente a una mayor exposición a las ciberamenazas;

B. Considerando que el número de dispositivos conectados, incluidas las máquinas, los sensores, los componentes industriales y las redes que conforman la internet de las cosas, sigue aumentando y que se espera que 22 300 millones de dispositivos estén conectados a la internet de las cosas en todo el mundo de aquí a 2024, lo que eleva la exposición a ciberataques;

C. Considerando que los avances tecnológicos —como la computación cuántica— y las asimetrías en el acceso a los mismos podrían representar un reto para el panorama de la ciberseguridad;

D. Considerando que la crisis de la COVID-19 ha puesto aún más de manifiesto ciertas vulnerabilidades cibernéticas en algunos sectores críticos, en particular en la asistencia sanitaria, y que las medidas asociadas de teletrabajo y distanciamiento físico han incrementado nuestra dependencia de las tecnologías digitales y la conectividad, al tiempo que los ciberataques y la ciberdelincuencia, incluido el espionaje y el sabotaje, así como el acceso a sistemas, estructuras y redes de TIC y su manipulación mediante instalaciones malintencionadas e ilícitas, están aumentando en número y sofisticación en toda Europa;

E. Considerando que el número de ciberataques está aumentando de forma significativa, como se observa en la reciente serie de ciberataques malintencionados y organizados contra sistemas sanitarios, por ejemplo, de Irlanda, Finlandia y Francia; que estos ciberataques causan perjuicios importantes a los sistemas sanitarios y a la atención a los pacientes, así como a otras instituciones públicas y privadas sensibles;

F. Considerando que las amenazas híbridas están aumentando, incluido el uso de campañas de desinformación y ciberataques contra infraestructuras, procesos económicos e instituciones democráticas, y se están convirtiendo en un problema grave tanto en el mundo cibernético como en el físico, y que corren el riesgo de afectar a los procesos democráticos como las elecciones, los procedimientos legislativos, la aplicación de la ley y la justicia;

G. Considerando que existe una dependencia cada vez mayor de la función central de Internet y de los servicios esenciales de Internet en cuanto a la comunicación y el alojamiento, las aplicaciones y los datos, cuya cuota de mercado se está concentrando progresivamente en un número cada vez menor de empresas;

([7]) DO L 207 de 6.8.2010, p. 1.
([8]) Textos Aprobados, P9_TA(2020)0359.
([9]) Textos Aprobados, P9_TA(2021)0098.
([10]) Textos Aprobados, P9_TA(2021)0261.
([11]) Textos Aprobados, P9_TA(2021)0026.
([12]) DO C 23 de 21.1.2021, p. 2.

H. Considerando que las capacidades de los ataques distribuidos de denegación de servicio están aumentando y que, por consiguiente, debe incrementarse en paralelo la resiliencia del núcleo de internet;

I. Considerando que el grado de preparación y sensibilización en materia de ciberseguridad entre las empresas, en particular las pymes, y los particulares sigue siendo bajo y que hay una escasez de trabajadores cualificados (el déficit de mano de obra se ha ampliado en un 20 % desde 2015), y que los canales de contratación tradicionales no satisfacen la demanda, incluida la de puestos de gestión e interdisciplinarios; que «casi el 90 % de las personas que trabajan en ciberseguridad son hombres» y que «esta persistente falta de diversidad de género limita aún más la reserva de talento» ([13]);

J. Considerando que las capacidades de ciberseguridad son heterogéneas entre los Estados miembros y que la notificación de incidentes y el intercambio de información entre ellos no es sistemático ni exhaustivo, mientras que el uso de los centros de puesta en común y análisis de la información (ISAC) para el intercambio de información entre los sectores público y privado no está aprovechando su potencial;

K. Considerando la falta de acuerdo a escala de la Unión acerca de la colaboración en materia de inteligencia cibernética y de la respuesta colectiva a los ataques cibernéticos e híbridos; que las contramedidas ante las ciberamenazas y los ciberataques, especialmente los de naturaleza híbrida, revisten una gran dificultad tanto desde el punto de vista técnico como del geopolítico, lo que complica que los Estados miembros las puedan acometer por sí solos;

L. Considerando que el intercambio transfronterizo de datos y el intercambio de datos a escala mundial son importantes para la creación de valor, siempre que se garanticen la privacidad y los derechos de propiedad intelectual e industrial; que la aplicación de legislación extranjera en materia de datos podría suponer un riesgo para la ciberseguridad de los datos europeos, dado que las empresas que operan en diferentes regiones están sujetas a obligaciones que se solapan, con independencia de la ubicación de los datos o de su origen;

M. Considerando que la ciberseguridad representa un mercado mundial por valor de 600 000 000 000 EUR —cifra que se espera vaya en rápido aumento— y que la Unión es un importador neto de productos y soluciones;

N. Considerando que existe un riesgo de fragmentación del mercado único debido a las normativas nacionales en materia de ciberseguridad y a la falta de legislación horizontal en cuanto a los requisitos esenciales de ciberseguridad para los equipos y programas informáticos, incluidos los productos y aplicaciones conectados;

1. Acoge con agrado las iniciativas esbozadas por la Comisión en la Comunicación conjunta titulada «La Estrategia de Ciberseguridad de la UE para la Década Digital»;

2. Pide que se promueva el desarrollo de redes y sistemas de información, infraestructuras y conectividad seguros y fiables en toda la Unión;

3. Pide que se establezca el objetivo de que todos los productos conectados a Internet en la Unión, incluidos los destinados a usos industriales y al consumo, junto con el conjunto de las cadenas de suministro que los proporcionan, tengan que ser seguros desde el diseño, sean resistentes a los ciberincidentes y se parcheen rápidamente cuando se descubran vulnerabilidades; acoge con agrado los planes de la Comisión de proponer legislación horizontal sobre los requisitos de ciberseguridad para los productos conectados y los servicios asociados, y pide que dicha legislación proponga la armonización de las legislaciones nacionales para evitar la fragmentación del mercado único; solicita que se tenga en cuenta la legislación existente (el Reglamento sobre la Ciberseguridad, el nuevo marco legislativo y el Reglamento sobre normalización) con el fin de evitar ambigüedades y fragmentaciones;

4. Pide a la Comisión que evalúe la necesidad de una propuesta de normativa horizontal que introduzca requisitos de ciberseguridad para las aplicaciones, los programas informáticos, los programas informáticos incorporados y los sistemas operativos de aquí a 2023, sobre la base del acervo de la Unión en materia de requisitos de gestión del riesgo; destaca que las aplicaciones, los programas informáticos, los programas informáticos incorporados y los sistemas operativos obsoletos (es decir, los que ya no reciben parches ni actualizaciones de seguridad periódicamente) suponen una proporción nada desdeñable de todos los dispositivos conectados y un riesgo para la ciberseguridad; pide a la Comisión que incluya en esta cuestión en su propuesta; sugiere que la propuesta incluya la obligación de que los creadores comuniquen por adelantado el período mínimo durante el cual proporcionarán parches de seguridad y actualizaciones con el fin de que los compradores puedan tomar decisiones informadas; considera que los creadores deben formar parte del programa de divulgación coordinada de las vulnerabilidades, tal como se establece en la propuesta de Directiva SRI 2;

([13]) Documento informativo del Tribunal de Cuentas Europeo titulado «Desafíos de una política eficaz de ciberseguridad en la UE», marzo de 2019.

5. Subraya que la ciberseguridad debe estar integrada en la digitalización; pide, por tanto, que los proyectos de digitalización financiados por la Unión incluyan requisitos de ciberseguridad; acoge con satisfacción el apoyo a la investigación y la innovación en el ámbito de la ciberseguridad, especialmente en lo que se refiere a las tecnologías disruptivas (como la computación cuántica y la criptografía cuántica), cuya aparición podría desestabilizar el equilibrio internacional; pide, además, que se siga investigando sobre los algoritmos postcuánticos como norma de ciberseguridad;

6. Considera que la digitalización de nuestra sociedad significa que todos los sectores están interconectados y que las deficiencias de un sector pueden causar dificultades en otros; insiste, por tanto, en que las políticas de ciberseguridad se integren en la estrategia digital y en la financiación de la Unión, y en que sean coherentes e interoperables en todos los sectores;

7. Pide un uso coherente de los fondos de la Unión en lo que respecta a la ciberseguridad y el despliegue de las infraestructuras conexas; pide a la Comisión y a los Estados miembros que velen por que se aprovechen las sinergias relacionadas con la ciberseguridad entre los diferentes programas, en particular el programa Horizonte Europa, el Programa Europa Digital, el Programa Espacial de la Unión, el Mecanismo de Recuperación y Resiliencia de la Unión, InvestEU y el MCE, y que hagan pleno uso del Centro y la Red de Competencia en Ciberseguridad;

8. Recuerda que la infraestructura de comunicación es la piedra angular de toda actividad digital y que garantizar su seguridad es una prioridad estratégica para la Unión; respalda el desarrollo actual del esquema de certificación de ciberseguridad de la Unión para las redes 5G; acoge con satisfacción el conjunto de instrumentos de la Unión sobre ciberseguridad de la tecnología 5G y pide a la Comisión, a los Estados miembros y a la industria que prosigan sus esfuerzos por lograr unas redes de comunicación seguras, que incluyan medidas relativas a toda la cadena de suministro; pide a la Comisión que evite la dependencia de un solo proveedor y que mejore la seguridad de la red promoviendo iniciativas que mejoren la virtualización y la migración a la nube de los distintos componentes de las redes; pide el rápido desarrollo de las próximas generaciones de tecnologías de comunicación con ciberseguridad desde el diseño como principio fundamental y garantizando la protección de la privacidad y los datos personales;

9. Reitera la importancia de establecer un nuevo marco de seguridad sólido para las infraestructuras críticas de la Unión con el fin de salvaguardar los intereses de seguridad de la Unión y aprovechar las capacidades existentes al objeto de responder adecuadamente a los riesgos, las amenazas y los cambios tecnológicos;

10. Pide a la Comisión que prepare disposiciones con miras a garantizar la accesibilidad, disponibilidad e integridad del núcleo público de internet y, por ende, la estabilidad del ciberespacio, en particular en lo que se refiere al acceso de la Unión al sistema raíz mundial del DNS; considera que esas disposiciones deben incluir medidas para la diversificación de los proveedores a fin de mitigar el riesgo actual de dependencia en las pocas empresas que dominan el mercado; acoge con agrado la propuesta de un sistema europeo de nombres de dominio (DNS4EU) como herramienta en favor de un núcleo de internet más resiliente; pide a la Comisión que evalúe cómo este DNS4EU podría utilizar las tecnologías más actuales, los protocolos de seguridad y los conocimientos especializados en ciberamenazas con miras a ofrecer un DNS rápido, seguro y resiliente a todos los europeos; recuerda la necesidad de una mejor protección del protocolo de puerta de enlace de frontera (BGP por sus siglas en inglés) para evitar pirateos a través del BGP; recuerda su respaldo a un modelo multilateral para la gobernanza de Internet, en el que la ciberseguridad debe constituir uno de los temas centrales; subraya que la Unión debe acelerar la aplicación del IPv6; reconoce que el modelo de código abierto, como base para el funcionamiento de Internet, ha demostrado ser eficiente y eficaz; alienta, por tanto, su uso;

11. Reconoce la necesidad de reforzar los análisis forenses digitales con el fin de luchar contra la delincuencia, la ciberdelincuencia y los ciberataques, incluidos los ataques patrocinados por Estados, pero advierte contra las medidas desproporcionadas que ponen en peligro la privacidad y la libertad de expresión de los ciudadanos de la Unión cuando utilizan Internet; recuerda la necesidad de concluir la revisión del segundo protocolo adicional al Convenio de Budapest sobre la Ciberdelincuencia, que podría aumentar la preparación frente a la ciberdelincuencia;

12. Pide a la Comisión y a los Estados miembros que pongan en común sus recursos al objeto de mejorar la resiliencia estratégica de la Unión, reducir su dependencia de tecnologías extranjeras y fomentar su liderazgo y competitividad en materia de ciberseguridad en toda la cadena de suministro digital (incluido el almacenamiento y el tratamiento de datos en la nube, las tecnologías de procesadores, los circuitos integrados (chips), la conectividad ultrasegura, la computación cuántica y la próxima generación de redes);

13. Estima que el plan para una infraestructura de conectividad ultrasegura es un instrumento importante para la seguridad de las comunicaciones digitales sensibles; acoge con satisfacción el anuncio del desarrollo de un sistema global de comunicaciones seguras de la UE basado en el espacio, que integre tecnologías de encriptación cuántica; recuerda que deben realizarse esfuerzos continuos, en cooperación con la Agencia de la Unión Europea para el Programa Espacial (EUSPA) y la Agencia Espacial Europea (AEE), a fin de garantizar la seguridad de las actividades espaciales europeas;

14. Lamenta que las prácticas de intercambio de información sobre las amenazas y los incidentes cibernéticos no hayan sido bien acogidas por los sectores público y privado; pide a la Comisión y a los Estados miembros que incrementen la confianza y reduzcan los obstáculos con respecto al intercambio de información sobre ciberamenazas y ciberataques a todos los niveles; celebra los esfuerzos realizados por algunos sectores y pide una colaboración intersectorial, ya que las vulnerabilidades rara vez son específicas de un sector; destaca que los Estados miembros deben unir fuerzas a nivel europeo para compartir eficazmente sus conocimientos más recientes sobre los riesgos de ciberseguridad; alienta la creación de un grupo de trabajo de los Estados miembros sobre inteligencia cibernética, con el fin de fomentar el intercambio de información en la Unión y en el espacio económico europeo, en particular para evitar ciberataques a gran escala;

15. Se felicita por la creación prevista de una unidad informática conjunta para reforzar la cooperación entre los órganos de la Unión y las autoridades de los Estados miembros responsables de prevenir, disuadir y responder a los ciberataques; pide a los Estados miembros y a la Comisión que sigan mejorando la cooperación en materia de ciberdefensa y desarrollen la investigación sobre las capacidades de ciberdefensa más avanzadas;

16. Recuerda la importancia del factor humano en la estrategia de ciberseguridad; pide que prosigan los esfuerzos para difundir la cuestión de la sensibilización en materia de ciberseguridad, incluidas la ciberhigiene y la alfabetización digital;

17. Pone de relieve la importancia de un marco de seguridad sólido y coherente de cara a proteger a todo el personal, los datos, las redes de comunicación y los sistemas de información, y los procesos de toma de decisiones de la Unión contra las ciberamenazas basado en normas exhaustivas, coherentes y homogéneas y en una gobernanza adecuada; pide que se asignen recursos y capacidades suficientes, también en el contexto del refuerzo del mandato del CERT-UE y en relación con los debates en curso sobre la definición de normas comunes vinculantes en materia de ciberseguridad para todas las instituciones, órganos y agencias de la Unión;

18. Pide un uso más amplio de la certificación voluntaria y de las normas de ciberseguridad, ya que representan herramientas importantes para mejorar el nivel general de ciberseguridad; acoge con satisfacción la creación del marco europeo de certificación y la labor del Grupo Europeo de Certificación de la Ciberseguridad; pide a ENISA y a la Comisión que, a la hora de preparar el esquema europeo de certificación de la ciberseguridad para los servicios en la nube, consideren obligatoria la aplicación del Derecho de la Unión en lo que respecta al nivel de garantía «elevado»;

19. Pone de relieve la necesidad de adaptar la demanda de mano de obra en el sector de la ciberseguridad a la reducción de la brecha de competencias mediante la continuación de los esfuerzos en materia de educación y formación; pide que se preste especial atención a la eliminación de la brecha de género, que también está presente en este sector;

20. Reconoce la necesidad de incrementar el apoyo a las microempresas y a las pequeñas y medianas empresas a fin de que comprendan mejor todos los riesgos y oportunidades en materia de seguridad de la información y eleven su nivel de ciberseguridad; pide a ENISA y a las autoridades nacionales que desarrollen portales de autodiagnóstico y guías de mejores prácticas para las microempresas y las pequeñas y medianas empresas; recuerda la importancia de la formación y del acceso a financiación específica para la seguridad de estas entidades;

21. Encarga a su presidente que transmita la presente Resolución a la Comisión, al Consejo y a los Gobiernos y los Parlamentos de los Estados miembros.