Parlamento Europeo
2014-2019

Documento de sesión

B8-0153/2019

6.3.2019

PROPUESTA DE RESOLUCIÓN

tras las declaraciones del Consejo y de la Comisión

presentada de conformidad con el artículo 123, apartado 2, del Reglamento interno

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
(2019/2575(RSP))

Tiziana Beghin, Dario Tamburrano, Isabella Adinolfi, Rolandas Paksas
en nombre del Grupo EFDD

B8-0153/2019

Resolución del Parlamento Europeo 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
(2019/2575(RSP))

El Parlamento Europeo,

– Vistas las Comunicaciones de la Comisión, de 14 de septiembre de 2016, tituladas «La conectividad para un mercado único digital competitivo – hacia una sociedad europea del Gigabit» (COM(2016)0587) y «La 5G para Europa: un plan de acción» (COM(2016)0588),

– Vista la propuesta modificada de la Comisión de Reglamento del Parlamento Europeo y del Consejo, de 29 de enero de 2016, sobre el acceso de los productos y servicios de terceros países al mercado interior de la Unión en el ámbito de la contratación pública, así como sobre los procedimientos de apoyo a las negociaciones para el acceso de los productos y servicios de la Unión a los mercados de contratación pública de terceros países (COM(2016)0034),

– Vista la 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[1] (Directiva SRI),

– Vista la propuesta de Reglamento del Parlamento Europeo y del Consejo, de 13 de septiembre de 2017, 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)0477),

– 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[2],

– Vista la propuesta de la Comisión de Reglamento del Parlamento Europeo y del Consejo, de 12 de septiembre de 2018, 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),

– Visto el procedimiento de solución de diferencias de la OMC WT/DS549/6, de 1 de junio de 2018, en relación con determinadas medidas impuestas por China relativas a la transferencia de tecnología extranjera a este país,

– Vista su Posición aprobada en primera lectura el 14 de febrero de 2019 sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establece

[1] DO L 194 de 19.7.2016, p. 1.
[2] DO L 321 de 17.12.2018, p. 36.

un marco para el control de las inversiones extranjeras directas en la Unión Europea[3],

– Vistas las negociaciones en curso de un acuerdo integral en materia de inversiones entre la Unión y China,

– Visto el artículo 123, apartado 2, de su Reglamento interno,

A. Considerando que los últimos avances en las tecnologías de la información y de las comunicaciones (TIC), en particular las telecomunicaciones de quinta generación (5G), han dado paso a nuevas vías tanto de producción, distribución y obtención de bienes y servicios como de interacción entre los dispositivos y entre los ciudadanos, las administraciones públicas y otros agentes socioeconómicos, por lo que tienen la posibilidad de impulsar la economía europea;

B. Considerando que la ciberseguridad en relación con las TIC, la protección de la información delicada, el respeto de los derechos individuales y la defensa frente a las amenazas cibernéticas externas son condiciones necesarias para garantizar la soberanía tecnológica de la ciudadanía de la Unión y, en definitiva, conseguir la prosperidad de esta y apoyar en ella la democracia;

C. Considerando que la investigación y los ensayos en relación con la 5G apenas si logran estar a la altura de la presión internacional en cuanto al despliegue y comercialización de esta, mientras que algunos estudios científicos han generado preocupación y dudas en cuanto a su seguridad e inocuidad, en particular en lo que respecta a los riesgos que para la salud humana y el medio ambiente comporta la contaminación electromagnética;

D. Considerando que velar por la ciberseguridad de las redes 5G es un nuevo y complejo reto debido al carácter virtual y descentralizado de la 5G y a su cadena de valor fragmentada y altamente especializada, que incluye desde la producción hasta la distribución, pasando por la instalación, la configuración, las operaciones, el mantenimiento y las actualizaciones de los programas informáticos; que la Unión ha de colmar las lagunas que en materia de ciberseguridad presentan sus infraestructuras vitales en, entre otros sectores, las telecomunicaciones, la energía, el transporte, la salud, la defensa y la seguridad;

E. Considerando que garantizar la inocuidad y seguridad de las redes 5G es una tarea que se halla fuera del alcance por cuenta propia de fabricantes o gestores de redes, sino que exige la actuación coordinada y eficaz de todas las autoridades nacionales e internacionales pertinentes;

F. Considerando que la Unión goza de la capacidad necesaria para liderar el fomento de las tecnologías en materia de ciberseguridad brindando apoyo a las empresas europeas del sector e impulsando todo cambio en la cadena de valor que pueda redundar en una menor dependencia de la Unión de la tecnología extranjera;

G. Considerando que la Unión ha estado preparando un conjunto de medidas tendentes a garantizar la ciberseguridad, en particular la Directiva SRI y el Reglamento de

[3] Textos Aprobados, P8_TA(2019)0121.

Ciberseguridad, que deben aplicarse rápidamente y ser objeto de un seguimiento continuo, a fin de velar por que no pierdan eficacia a lo largo de las actualizaciones y revisiones que resulten necesarias;

H. Considerando que la mayor presencia de proveedores de tecnología chinos y procedentes de otros terceros países, en particular de empresas estatales o poco transparentes, ha quedado de manifiesto en el mercado de la 5G de la Unión;

I. Considerando que la reciprocidad es una de las maneras más eficaces de avanzar hacia unas condiciones de competencia equitativas a escala mundial;

J. Considerando que las empresas extranjeras tienen en la actualidad que enfrentarse a las diferencias existentes en las normas de protección de datos de la Unión entre el Reglamento General de Protección de Datos y las distintas obligaciones que establecen las legislaciones nacionales;

K. Considerando que la Unión y China llevan negociando desde 2013 un acuerdo integral en materia de inversiones; que con el acuerdo que se plantea, se contribuiría a dar respuesta a las cuestiones relativas al acceso a los mercados, se crearía un marco para la protección de las inversiones y se implantarían normas básicas en materia de trabajo y de medio ambiente;

L. Considerando que, si bien no resultan concluyentes, han salido a la luz pruebas relativas a fallos de seguridad en aparatos suministrados por proveedores de terceros países, incluida China, que podrían poner en peligro tanto el derecho a la intimidad como la protección de la información delicada en la Unión;

1. Subraya que el despliegue y la comercialización de la 5G deben regirse por el principio de cautela, previendo todos los agentes socioeconómicos las posibles repercusiones en materia de seguridad y protección y adoptando medidas de precaución proporcionadas, en particular la rápida revelación de aquellos factores que puedan entrañar peligro para la salud pública o el medio ambiente;

2. Hace hincapié en que deben estudiarse a fondo las repercusiones sociales y económicas de la 5G y de las tecnologías que esta hace posible, desde la internet de las cosas hasta la inteligencia artificial, y tomarse medidas al objeto de que la transición a la sociedad europea del Gigabit tenga lugar de una manera que resulte justa y equitativa para todos y esté basada en la responsabilidad ética;

3. Pide a la Comisión y a los Estados miembros que establezcan un entorno favorable a la innovación para que los proveedores de la Unión creen nuevos productos, servicios y tecnologías, y que apoyen el emprendimiento de la Unión en lo que respecta al despliegue y la comercialización de una 5G inocua y segura, velando al mismo tiempo por que el potencial que encierra esté al alcance de todas las empresas de la economía digital de la Unión, en particular las pequeñas y medianas empresas;

4. Recuerda que la ciberseguridad es uno de los retos más importantes a los que se enfrenta actualmente la Unión y que cosechar malos resultados en este ámbito podría vulnerar los derechos tanto a la intimidad como fundamentales de los consumidores y productores de la Unión, socavar gravemente la confianza de los ciudadanos en los

productos y servicios de TIC y, en definitiva, acarrear graves perjuicios económicos; aboga por una red segura desde el diseño y por defecto;

5. Solicita a la Comisión y a los Estados miembros que colaboren estrechamente en lo que a la puesta en práctica de la Estrategia de Ciberseguridad de la Unión Europea respecta, así como que conjuguen las medidas nacionales y de la Unión al objeto de reducir lo más posible a lo largo de toda la cadena de valor el riesgo tanto de fallos de seguridad como de violaciones de la seguridad de los datos; considera que estas medidas podrían, entre otras, consistir en un certificado de ciberseguridad de la Unión, requisitos de configuración, y procedimientos y prácticas operativos, así como en la promoción de la ciberhigiene y la educación digital;

6. Estima que la agencia de ciberseguridad de la Unión (la Agencia de Seguridad de las Redes y de la Información de la Unión Europea, o ENISA, por sus siglas en inglés) está llamada a desempeñar un papel fundamental en el estudio de las posibles amenazas procedentes de los proveedores extranjeros, incluida China, y en la coordinación de un planteamiento común entre los Estados miembros al objeto de hacer frente a las amenazas para la ciberseguridad y los ataques;

7. Pide a la Comisión y a los Estados miembros que pongan rápidamente en práctica el paquete sobre la economía circular e impulsen tanto la gestión de las materias primas a lo largo de todo su ciclo de vida como el reciclado de residuos de modo que la Unión tenga un mejor acceso a materias primas fundamentales, las cuales resultan esenciales para los productos de alta tecnología y las innovaciones que van surgiendo;

8. Cree urgente abordar las posibles amenazas que para la seguridad tecnológica plantea la actual penetración en el mercado de la Unión por parte de proveedores extranjeros, en particular de China, mediante la adopción de un planteamiento común en materia de seguridad y protección de datos entre los Estados miembros;

9. Pide a la Comisión y a los Estados miembros que lleven a cabo un seguimiento y análisis de la seguridad de aquellos sistemas TIC con una elevada presencia de tecnologías de terceros países, y que ello incluya la realización de pruebas de esfuerzo;

10. Subraya que no se debe discriminar a los proveedores de terceros países por su país de origen, pero que, con objeto de garantizar la igualdad de condiciones, sí que se deben tener en cuenta la transparencia de estas empresas, sus normas de ciberseguridad y la reciprocidad de condiciones para las empresas europeas en dicho país;

11. Hace hincapié en que bajo ningún concepto han de poner en peligro los proveedores y gestores de China o de otros terceros países los derechos subjetivos garantizados por el Derecho de la Unión, aun en el caso de que los requisitos con arreglo a la legislación nacional de su país de origen sean distintos;

12. Pide al Consejo que valore positivamente la posibilidad de volver a abrir el debate sobre la nueva propuesta modificada de la Comisión relativa al procedimiento de restricción del acceso de productos extranjeros al mercado de contratación pública de la Unión en caso de falta de reciprocidad;

13. Recuerda la importancia de seguir mejorando las negociaciones relativas a la

cooperación en el ámbito de la regulación sobre tecnología digital con terceros países y de garantizar un mayor compromiso por parte de estos en los organismos internacionales de normalización;

14. Encarga a su presidente que transmita la presente Resolución al Consejo y a la Comisión.