Consejo de la Unión Europea

Bruselas, 16 de septiembre de 2022
(OR. en)

Expediente interinstitucional: 2022/0272(COD)

12429/22
ADD 6

CYBER 298
JAI 1181
DATAPROTECT 254
TELECOM 369
MI 665
CSC 388
CSCI 133
CODEC 1310
IA 133

NOTA DE TRANSMISIÓN

De:	Por la secretaria general de la Comisión Europea, D.ª Martine DEPREZ, directora
Fecha de recepción:	15 de septiembre de 2022
A:	D.ª Thérèse BLANCHET, secretaria general del Consejo de la Unión Europea
N.° doc. Ción.:	SWD(2022) 283 final
Asunto:	DOCUMENTO DE TRABAJO DE LOS SERVICIOS DE LA COMISIÓN RESUMEN DEL INFORME DE LA EVALUACIÓN DE IMPACTO sobre la Ley de Ciberresiliencia que acompaña al documento Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales y por el que se modifica el Reglamento (UE) 2019/1020

Adjunto se remite a las Delegaciones el documento – SWD(2022) 283 final.

Adj.: SWD(2022) 283 final

COMISIÓN
EUROPEA

Bruselas, 15.9.2022
SWD(2022) 283 final

DOCUMENTO DE TRABAJO DE LOS SERVICIOS DE LA COMISIÓN

RESUMEN DEL INFORME DE LA EVALUACIÓN DE IMPACTO

sobre la Ley de Ciberresiliencia

que acompaña al documento

Propuesta de Reglamento del Parlamento Europeo y del Consejo

relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales y por el que se modifica el Reglamento (UE) 2019/1020

{COM(2022) 454 final} - {SEC(2022) 321 final} - {SWD(2022) 282 final}

Ficha resumen (máximo dos páginas)

Evaluación de impacto de la Ley de Ciberresiliencia

A. Necesidad de actuar

¿Cuál es el problema y por qué es un problema en la UE?

Los productos consistentes en equipos informáticos (*hardware*) y programas informáticos (*software*) a menudo se enfrentan a ciberataques llevados a cabo con éxito, lo que eleva el coste anual mundial estimado de la ciberdelincuencia a 5,5 billones EUR en 2021. Estos productos enfrentan dos problemas principales que suponen costes adicionales para los usuarios y la sociedad: 1) un bajo nivel de ciberseguridad, que se refleja en vulnerabilidades generalizadas y en la oferta insuficiente e incoherente de actualizaciones de seguridad para hacerles frente, y 2) una comprensión de la información y un acceso a ella insuficientes por parte de los usuarios, lo que les impide elegir productos con las características de ciberseguridad adecuadas o utilizarlos de manera segura.

La ciberseguridad de los productos con elementos digitales tiene una importante dimensión transfronteriza, ya que los productos fabricados en un país a menudo se utilizan en todo el mercado interior. Además, es habitual que los incidentes que inicialmente afectan a una única entidad o Estado miembro se expandan en minutos a todo el mercado interior.

Si bien la legislación vigente sobre el mercado interior se aplica a determinados productos con elementos digitales, actualmente la mayoría de los productos consistentes en equipos informáticos y programas informáticos no están contemplados en ninguna norma de la Unión Europea (UE) que regule su ciberseguridad. En particular, el marco jurídico actual de la UE no aborda la ciberseguridad de los programas informáticos no incorporados, aun cuando los ataques de ciberseguridad se centran cada vez más en las vulnerabilidades de estos productos, lo que genera considerables costes sociales y económicos. Algunos ejemplos recientes son el programa espía Pegasus, que aprovechó vulnerabilidades en teléfonos móviles, o el programa de chantaje de tipo gusano WannaCry, que explotó una vulnerabilidad Windows y afectó a ordenadores de todo el mundo.

¿Qué se pretende conseguir?

Se identificaron dos objetivos principales para garantizar el correcto funcionamiento del mercado interior: 1) crear condiciones que permitan el desarrollo de productos con elementos digitales seguros, garantizando que los productos consistentes en equipos informáticos y programas informáticos se introduzcan en el mercado con menos vulnerabilidades y que los fabricantes se tomen en serio la seguridad a lo largo de todo el ciclo de vida de un producto; y 2) crear condiciones que permitan a los usuarios tener en cuenta la ciberseguridad a la hora de elegir y utilizar productos con elementos digitales. Se establecieron cuatro objetivos específicos: i) garantizar que los fabricantes mejoren la seguridad de los productos con elementos digitales desde la fase de diseño y desarrollo y a lo largo de todo el ciclo de vida; ii) garantizar un marco de ciberseguridad coherente y facilitar su cumplimiento por parte de los fabricantes de equipos y programas informáticos; iii) mejorar la transparencia de las características de seguridad de los productos con elementos digitales; y iv) permitir a las empresas y a los consumidores utilizar productos con elementos digitales de forma segura.

¿Cuál es el valor añadido de la actuación de la UE en este ámbito (respecto a la subsidiariedad)?

La importante naturaleza transfronteriza de la ciberseguridad y el aumento de los incidentes, cuyas repercusiones pueden extenderse a otros países, sectores y productos, hacen que los Estados miembros por sí solos no puedan alcanzar eficazmente los objetivos planteados. Habida cuenta de la dimensión mundial

de los mercados de los productos con elementos digitales, los Estados miembros hacen frente en su territorio a los mismos riesgos para un mismo producto con elementos digitales. El mosaico de normas nacionales con posibles divergencias que está surgiendo corre el riesgo de poner barreras a un mercado único abierto y competitivo para los productos con elementos digitales. Por lo tanto, se hace necesaria la acción conjunta a escala de la UE para aumentar el nivel de confianza entre los usuarios y el atractivo de los productos con elementos digitales introducidos en el mercado de la UE. La acción conjunta también beneficiaría al mercado interior al proporcionar seguridad jurídica y condiciones de competencia equitativas para los fabricantes de productos con elementos digitales.

B. Soluciones

¿Cuáles son las distintas opciones posibles para alcanzar los objetivos? ¿Existe o no una opción preferida? En caso negativo, ¿por qué?

Se analizaron cuatro opciones, así como subopciones relacionadas con estas, que van más allá de lo hecho hasta el momento: 1) enfoque de Derecho indicativo y medidas voluntarias; 2) intervención reguladora *ad hoc* para la ciberseguridad de los productos tangibles con elementos digitales y sus respectivos programas informáticos incorporados; 3) enfoque mixto que incluya normas horizontales obligatorias para la ciberseguridad de los productos tangibles con elementos digitales y sus respectivos programas informáticos incorporados y un enfoque escalonado para los programas informáticos no incorporados, con dos subopciones para la evaluación de la conformidad; 4) intervención reguladora horizontal que introduzca requisitos de ciberseguridad para una amplia gama de productos con elementos digitales, incluidos los programas informáticos no incorporados, con subopciones relativas al ámbito de aplicación y a la evaluación de la conformidad.

La evaluación de impacto concluyó que **la opción preferida** es la opción 4, que abarca todos los productos con elementos digitales y prevé la evaluación de terceros obligatoria para los productos críticos, sobre la base de la evaluación de la eficacia con respecto a los objetivos específicos, la eficiencia entre costes y beneficios y la coherencia.

¿Cuáles son las opiniones de las distintas partes interesadas? ¿Quién apoya cada opción?

Al pedírseles que evaluaran la eficacia de las intervenciones políticas, los participantes en la consulta pública coincidieron en que la opción 4 sería la medida más eficaz (4,08 en una escala de 1 a 5). Aquí se incluyen las valoraciones de las organizaciones de consumidores (5,00), los encuestados que se identifican como usuarios (4,22), los organismos notificados (4,17), las autoridades de vigilancia del mercado (5,00) y los fabricantes de productos con elementos digitales (3,85), incluidas las pymes (4,05).

C. Repercusiones de la opción preferida

¿Cuáles son las ventajas de la opción preferida (o, en su defecto, de las opciones principales)?

La opción preferida beneficiaría considerablemente a las distintas partes interesadas. Por lo que respecta a las empresas, evitaría la divergencia entre las normas de seguridad para los productos con elementos digitales y reduciría los costes de cumplimiento de la legislación pertinente en materia de ciberseguridad. Reduciría el número de ciberincidentes, los costes de gestión de incidentes y el daño a la reputación. Para el conjunto de la UE, se calcula que la iniciativa podría dar lugar a una reducción de los costes derivados de los incidentes que afectan a las empresas de entre 180 000 y 290 000 millones EUR anuales aproximadamente. Además, la iniciativa permitiría un aumento del consumo de productos con elementos digitales y, por tanto, del volumen de negocio. También mejoraría la reputación mundial de las empresas, lo que también daría lugar a un aumento de la demanda fuera de la UE. A nivel de los usuarios finales, la

opción preferida aumentaría la transparencia de las propiedades de seguridad y facilitaría el uso de productos con elementos digitales. Los consumidores y los ciudadanos también se beneficiarían de una mejor protección de sus derechos fundamentales, como la privacidad y la protección de datos.

¿Cuáles son los costes de la opción preferida (o, en su defecto, de las opciones principales)?

La opción preferida añadiría costes de cumplimiento y de ejecución para las empresas, los organismos notificados y las autoridades públicas, incluidas las autoridades notificantes, de acreditación y de vigilancia del mercado. Por lo que se refiere a los desarrolladores de programas informáticos y los fabricantes de equipos informáticos, aumentará los costes directos de cumplimiento en relación con los nuevos requisitos de ciberseguridad, la evaluación de la conformidad, la documentación y las obligaciones de información, lo que resultará en unos costes de cumplimiento agregados aproximados de hasta 29 000 millones EUR para un valor de mercado estimado de los productos con elementos digitales de hasta 1 485 000 millones EUR en volumen de negocio. Es posible que los usuarios finales, incluidos los usuarios finales profesionales, los consumidores y los ciudadanos tengan que hacer frente a precios más elevados de los productos con elementos digitales. Sin embargo, estos costes deben considerarse en el contexto de los importantes beneficios descritos anteriormente. Por lo que se refiere a los organismos notificados, se prevé que los costes adicionales se vean compensados por un aumento en el volumen de negocio.

¿Cuáles son las repercusiones para las pymes y la competitividad?

Las pymes se verán afectadas por los nuevos requisitos, como también lo harán los fabricantes y los usuarios finales. En términos de costes de cumplimiento, las pymes se verían, en principio, más afectadas que las grandes empresas, que, por lo general, tienen mejores economías de escala y están más concienciadas con respecto a la ciberseguridad. Sin embargo, la iniciativa beneficiaría enormemente a las pymes, ya que la ciberseguridad integrada en los productos con elementos digitales supondría para ellas un ahorro significativo como usuarias. Como fabricantes, las pymes se beneficiarían de una mayor confianza de los usuarios finales y de nuevos clientes. Un acceso sin restricciones al mercado interior y una reducción de la fragmentación del mercado pueden resultar aún más beneficiosos para las pymes, ya que están menos equipadas para manejar diferentes requisitos reglamentarios. Si bien las pymes subrayaron la necesidad de un enfoque proporcionado y de medidas de apoyo, por lo general se mostraron favorables a la igualdad de condiciones entre todas las empresas y no creyeron verse desfavorecidas en comparación con las grandes empresas en un escenario de requisitos horizontales obligatorios.

¿Habrá repercusiones significativas en los presupuestos y las administraciones nacionales?

La iniciativa afectará a las autoridades nacionales, como las autoridades notificantes, las autoridades de acreditación y las autoridades de vigilancia del mercado responsables de la supervisión y la aplicación de las medidas propuestas. Estas autoridades deberán asumir ajustes (por ejemplo, en materia de formación y recursos humanos) y costes de ejecución adicionales para tener en cuenta los nuevos requisitos. Sin embargo, los recursos empleados por los organismos de acreditación los compensan y soportan en gran medida los organismos de evaluación de la conformidad mediante la compra de servicios de acreditación.

¿Habrá otras repercusiones significativas?

No se prevé ninguna otra repercusión negativa significativa. La opción de actuación preferida contribuiría a reducir el número y la gravedad de los incidentes, incluidas las violaciones de la seguridad de los datos personales, y tendría repercusiones sociales positivas, como la reducción de la ciberdelincuencia. Es probable que aumente la demanda de profesionales de la seguridad y se reduzca la asimetría de la

información de ciberseguridad.
¿Proporcionalidad?
La opción preferida no rebasa los límites estrictamente necesarios para lograr los objetivos específicos de manera satisfactoria. La intervención garantizaría que los productos con elementos digitales dispusieran de la seguridad necesaria a lo largo de todo su ciclo de vida, de manera proporcional a los riesgos a los que se enfrenten.
D. Seguimiento
¿Cuándo se revisará la política?
A más tardar [treinta y seis meses] después de que la iniciativa sea aplicable, y posteriormente cada cuatro años, la Comisión presentará al Parlamento Europeo y al Consejo un informe sobre la evaluación y revisión de la iniciativa.