Conselho da
União Europeia

Bruxelas, 16 de setembro de 2022
(OR. en)

12429/22
ADD 6

Dossiê interinstitucional:
2022/0272(COD)

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

NOTA DE ENVIO

de:	Secretária-geral da Comissão Europeia, com a assinatura de Martine DEPREZ, diretora
data de receção:	15 de setembro de 2022
para:	Secretariado-Geral do Conselho
n.° doc. Com.:	SWD(2022) 283 final
Assunto:	DOCUMENTO DE TRABALHO DOS SERVIÇOS DA COMISSÃO RELATÓRIO DO RESUMO DA AVALIAÇÃO DE IMPACTO relativo ao Regulamento Ciber-Resiliência que acompanha o documento Proposta de Regulamento do Parlamento Europeu e do Conselho relativo aos requisitos horizontais de cibersegurança dos produtos com elementos digitais e que altera o Regulamento (UE) 2019/1020

Envia-se em anexo, à atenção das delegações, o documento SWD(2022) 283 final.

Anexo: SWD(2022) 283 final

COMISSÃO
EUROPEIA

Bruxelas, 15.9.2022
SWD(2022) 283 final

DOCUMENTO DE TRABALHO DOS SERVIÇOS DA COMISSÃO

RELATÓRIO DO RESUMO DA AVALIAÇÃO DE IMPACTO

relativo ao Regulamento Ciber-Resiliência

que acompanha o documento

Proposta de Regulamento do Parlamento Europeu e do Conselho

relativo aos requisitos horizontais de cibersegurança dos produtos com elementos digitais e que altera o Regulamento (UE) 2019/1020

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

Ficha de síntese (máximo 2 páginas)

Avaliação de impacto do Regulamento Ciber-Resiliência

A. Necessidade de agir

Qual o problema e por que motivo tem dimensão europeia?

Os produtos de *hardware* e *software* são muitas vezes alvo de ciberataques bem-sucedidos, o que, até 2021, terá dado origem a um custo anual global estimado da cibercriminalidade de 5,5 biliões de EUR. Estes produtos são afetados por dois problemas importantes que aumentam os custos para os utilizadores e para a sociedade: 1) um baixo nível de cibersegurança, que se traduz em vulnerabilidades generalizadas e numa disponibilização insuficiente e incoerente de atualizações de segurança para as resolver, e 2) um entendimento e um acesso deficientes dos utilizadores à informação, o que os impede de escolher produtos com propriedades de cibersegurança adequadas ou de os utilizar de forma segura.

A cibersegurança dos produtos com elementos digitais tem uma forte dimensão transfronteiriça, uma vez que os produtos fabricados num país são muitas vezes utilizados em todo o mercado interno. Além disso, os incidentes que afetam inicialmente uma única entidade ou um único Estado-Membro propagam-se com frequência numa questão de minutos por todo o mercado interno.

Embora a legislação em vigor relativa ao mercado interno se aplique a determinados produtos com elementos digitais, a maioria dos produtos de *hardware* e *software* não está atualmente abrangida por nenhuma legislação da UE que aborde a sua cibersegurança. Em especial, o atual quadro jurídico da UE não aborda a cibersegurança de *software* não incorporado, apesar de os ataques de cibersegurança visarem cada vez mais as vulnerabilidades destes produtos, dando origem a custos sociais e económicos significativos. São exemplos recentes de tais ataques o *software* espião Pegasus, que explorou vulnerabilidades nos telemóveis, ou o *software* de sequestro (do tipo verme) WannaCry, que explorou uma vulnerabilidade do Windows que afeta computadores em todo o mundo.

Quais são os resultados esperados?

Foram identificados dois objetivos principais destinados a assegurar o bom funcionamento do mercado interno: 1) criar condições para o desenvolvimento de produtos com elementos digitais seguros, garantindo que sejam colocados no mercado produtos de *hardware* e *software* com menos vulnerabilidades e que os fabricantes encarem a segurança com seriedade durante todo o ciclo de vida de um produto; e 2) criar condições que permitam aos utilizadores ter em conta a cibersegurança aquando da seleção e da utilização de produtos com elementos digitais. Foram definidos quatro objetivos específicos**:** i) assegurar que os fabricantes melhorem a segurança dos produtos com elementos digitais desde a fase de conceção e desenvolvimento e ao longo de todo o ciclo de vida; ii) assegurar um quadro de cibersegurança coerente, que facilite a conformidade por parte dos fabricantes de *hardware* e *software*; iii) aumentar a transparência das propriedades de segurança dos produtos com elementos digitais; e iv) permitir que as empresas e os consumidores utilizem produtos com elementos digitais de forma segura.

Qual é o valor acrescentado da ação a nível da UE (subsidiariedade)?

A natureza marcadamente transfronteiriça da cibersegurança e o aumento dos incidentes com repercussões além-fronteiras e entre setores e produtos significam que os objetivos não podem ser eficazmente alcançados pelos Estados-Membros de forma isolada. Dada a natureza global dos mercados de produtos com elementos digitais, os Estados-Membros enfrentam, no respetivo território, os mesmos riscos para o mesmo produto com elementos digitais. A emergência de um mosaico de regras nacionais potencialmente divergentes poderá também prejudicar a criação de um mercado único aberto e competitivo para os produtos com elementos digitais. Torna-se, deste modo, necessária uma ação conjunta a nível da UE a fim de aumentar o nível de confiança entre os utilizadores e a atratividade dos produtos com elementos digitais colocados no mercado da UE. Esta beneficiará igualmente o mercado interno, proporcionando segurança jurídica e criando condições de concorrência equitativas para os fabricantes de produtos com elementos

digitais.

B. Soluções

Quais são as várias opções para alcançar os objetivos? Há alguma opção preferida? Em caso negativo, por que razão?

Analisaram-se quatro opções políticas, e subopções conexas, que vão além do *statu quo*: 1) abordagem não vinculativa e medidas voluntárias; 2) intervenção regulamentar *ad hoc* específica para cada produto, referente à cibersegurança dos produtos corpóreos com elementos digitais e respetivo *software* incorporado; 3) abordagem mista, incluindo regras vinculativas horizontais para a cibersegurança dos produtos corpóreos com elementos digitais e respetivo *software* incorporado e uma abordagem faseada para o *software* não incorporado, com duas subopções para a avaliação da conformidade; e 4) uma intervenção regulamentar horizontal que introduza requisitos de cibersegurança para um vasto leque de produtos com elementos digitais, incluindo *software* não incorporado, com subopções para o âmbito de aplicação e a avaliação da conformidade.

A avaliação de impacto concluiu, com base na avaliação da eficácia em relação aos objetivos específicos, da eficiência custos-benefícios e da coerência, que a **opção preferida** é a opção 4, que abrange todos os produtos com elementos digitais e prevê uma avaliação por terceiros obrigatória para os produtos críticos.

Quais são as perspetivas dos vários intervenientes? Quem apoia cada uma das opções?

Quando convidados a classificar a eficácia das intervenções estratégicas, os respondentes na consulta pública concordaram que a opção 4 seria a medida mais eficaz (4,08 numa escala de 1 a 5). Entre os respondentes, contavam-se organizações de consumidores (5,00), pessoas que se identificavam como utilizadores (4,22), organismos notificados (4,17), autoridades de fiscalização do mercado (5,00) e fabricantes de produtos com elementos digitais (3,85), incluindo os de pequena e média dimensão (4,05).

C. Impactos da opção preferida

Quais os benefícios da opção preferida (se existir; caso contrário, das principais opções)?

A opção preferida gerará benefícios significativos para as várias partes interessadas. Para as empresas, permitirá evitar a aplicação de regras de segurança divergentes aos produtos com elementos digitais e reduzir os custos de conformidade com a legislação conexa em matéria de cibersegurança. Reduzirá o número de ciberincidentes, os custos do tratamento de incidentes e os danos à reputação. Para a UE no seu conjunto, estima-se que a iniciativa possa conduzir a uma redução do custo decorrente de incidentes que afetam as empresas de cerca de 180 a 290 mil milhões de EUR por ano. Além disso, a iniciativa conduzirá a um aumento do volume de negócios em virtude do aumento da adoção de produtos com elementos digitais. Melhorará igualmente a reputação global das empresas, conduzindo a um aumento da procura por parte de países terceiros. Para os utilizadores finais, a opção preferida reforçará a transparência das propriedades de segurança e facilitará a utilização de produtos com elementos digitais. Os consumidores e os cidadãos também beneficiarão de uma melhor proteção dos seus direitos fundamentais, como a privacidade e a proteção de dados.

Quais são os custos da opção preferida (se existir; caso contrário, das principais opções)?

A opção preferida aumentará os custos de conformidade e de execução para as empresas, os organismos notificados e as autoridades públicas, incluindo as autoridades notificadoras, de acreditação e de fiscalização do mercado. Para os criadores de *software* e os fabricantes de *hardware*, aumentará os custos de conformidade diretos decorrentes de novos requisitos de cibersegurança, da avaliação da conformidade, de obrigações em matéria de documentação e comunicação de informações, gerando custos de conformidade agregados que ascendem a cerca de 29 mil milhões de EUR para um volume de negócios de produtos com elementos digitais com valor de mercado estimado de 1,485 biliões de EUR. Os utilizadores

finais, incluindo os utilizadores profissionais finais, os consumidores e os cidadãos, podem ver-se confrontados com um aumento dos preços dos produtos com elementos digitais. No entanto, tal deve ser considerado no contexto dos benefícios significativos acima descritos. No caso dos organismos notificados, prevê-se que os custos adicionais sejam compensados por um aumento do volume de negócios.

Quais são os efeitos para as PME e a competitividade?

As PME serão afetadas pelos novos requisitos, tanto enquanto fabricantes como enquanto utilizadores finais. Em termos de custos de conformidade, em princípio, as PME serão mais afetadas do que as grandes empresas, que normalmente obtêm maiores economias de escala e estão mais sensibilizadas para a cibersegurança. No entanto, as PME beneficiarão consideravelmente da iniciativa, uma vez que a integração da cibersegurança em produtos com elementos digitais representará uma poupança de custos significativa para as mesmas enquanto utilizadoras. Enquanto fabricantes, as PME beneficiarão de uma maior confiança dos utilizadores finais e de novos clientes. Um acesso sem obstáculos ao mercado interno e a redução da fragmentação do mercado podem proporcionar ainda mais benefícios às PME, uma vez que estas estão menos preparadas para lidar com diferentes requisitos regulamentares. Embora tenham sublinhado a necessidade de uma abordagem proporcionada e de medidas de apoio, as PME apoiaram, de um modo geral, a igualdade das condições de concorrência entre todas as empresas e não consideraram que ficariam em desvantagem em comparação com as empresas de maior dimensão num cenário de imposição de requisitos obrigatórios horizontais.

Haverá impactos significativos nos orçamentos e administrações nacionais?

A iniciativa terá impacto nas autoridades nacionais, tais como as autoridades notificadoras nacionais, as autoridades de acreditação e as autoridades de fiscalização do mercado responsáveis pelo controlo e a execução das medidas propostas. Estas autoridades suportarão custos adicionais de ajustamento (por exemplo, formação e recursos humanos) e de execução de forma a ter em conta os novos requisitos. Os recursos despendidos pelos organismos de acreditação são, porém, compensados e suportados em grande parte pelos organismos de avaliação da conformidade através da aquisição de serviços de acreditação.

Haverá outros impactos significativos?

Não são esperados outros impactos negativos significativos. A opção política preferida ajudará a reduzir o número e a gravidade dos incidentes, incluindo violações de dados pessoais, e terá impactos sociais positivos, como a redução da cibercriminalidade. É provável que aumente a procura de profissionais de segurança e que reduza as assimetrias em termos de informações sobre cibersegurança.

Proporcionalidade

A opção preferida não excede o necessário para atingir os objetivos específicos de forma satisfatória. A intervenção assegurará que os produtos com elementos digitais sejam seguros durante todo o seu ciclo de vida e de forma proporcionada face aos riscos enfrentados.

D. Acompanhamento

Quando será reexaminada a política?

Até [36 meses] após a data de aplicação da iniciativa e subsequentemente de quatro em quatro anos, a Comissão apresenta ao Parlamento Europeu e ao Conselho um relatório sobre a avaliação e o reexame da iniciativa.