Conselho da
União Europeia

Bruxelas, 14 de setembro de 2017
(OR. en)

12183/17
ADD 2

Dossiê interinstitucional:
2017/0225 (COD)

CYBER 127
TELECOM 207
ENFOPOL 410
CODEC 1397
JAI 785
MI 627
IA 139

NOTA DE ENVIO

de:	Secretário-Geral da Comissão Europeia, assinado por Jordi AYET PUIGARNAU, Diretor
para:	Jeppe TRANHOLM-MIKKELSEN, Secretário-Geral do Conselho da União Europeia
n.° doc. Com.:	SWD(2017) 501 final
Assunto:	DOCUMENTO DE TRABALHO DOS SERVIÇOS DA COMISSÃO RESUMO DA AVALIAÇÃO DE IMPACTO que acompanha o documento Proposta de REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO relativo à ENISA, a «Agência da União Europeia para a Cibersegurança», e à certificação da cibersegurança das tecnologias da informação e comunicação, e que revoga o Regulamento (UE) n.º 526/2013 («Regulamento Cibersegurança»)

Envia-se em anexo, à atenção das delegações, o documento SWD(2017) 501 final.

Anexo: SWD(2017) 501 final

COMISSÃO
EUROPEIA

Bruxelas, 13.9.2017
SWD(2017) 501 final

DOCUMENTO DE TRABALHO DOS SERVIÇOS DA COMISSÃO

RESUMO DA AVALIAÇÃO DE IMPACTO

que acompanha o documento

Proposta de REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO

relativo à ENISA, a «Agência da União Europeia para a Cibersegurança», e à certificação da cibersegurança das tecnologias da informação e comunicação, e que revoga o Regulamento (UE) n.º 526/2013 («Regulamento Cibersegurança»)

{COM(2017) 477 final}
{SWD(2017) 500 final}
{SWD(2017) 502 final}

A. NECESSIDADE DE TOMAR MEDIDAS

Qual é o problema e por que motivo constitui um problema?

As tecnologias digitais e a Internet são a espinha dorsal da economia e sociedade da UE. Os setores económicos críticos, tais como os transportes, a energia, a saúde ou as finanças tornaram-se cada vez mais dependentes das redes e sistemas de informação para realizarem as suas atividades principais. A Internet das coisas liga objetos e pessoas por intermédio de redes de comunicação. Esta nova realidade cria oportunidades sem precedentes, mas também vulnerabilidades. De facto, os ciberincidentes estão a proliferar. A sua complexidade, frequência e a «superfície» do seu impacto, desde o acesso a serviços essenciais aos processos democráticos, deverão aumentar ainda mais.

Neste contexto, foram identificados os problemas interligados que se seguem:

- Fragmentação de políticas e abordagens às questões da cibersegurança nos Estados-Membros.
- Dispersão de recursos e abordagens às questões da cibersegurança pelas instituições, agências e organismos da UE.
- Conhecimento insuficiente dos cidadãos e das empresas sobre as ciberameaças e informação insuficiente em relação às propriedades de segurança dos produtos e serviços de TIC que adquirem, associados ao surgimento crescente de vários sistemas de certificação nacionais e setoriais.

Estes problemas afetam a ciber-resiliência da UE, em geral, e o funcionamento eficaz do mercado interno.

O que deverá ser alcançado?

A iniciativa tem os seguintes objetivos estratégicos específicos:

1. Melhorar as capacidades e o estado de preparação dos Estados-Membros e das empresas, nomeadamente no tocante às infraestruturas críticas.
2. Reforçar a cooperação e coordenação entre Estados-Membros e instituições, agências e organismos da UE.
3. Aumentar as capacidades a nível da UE para complementar a ação dos Estados-Membros, designadamente no caso de cibercrises transfronteiriças.
4. Aumentar a sensibilização dos cidadãos e das empresas para as questões da cibersegurança.
5. Aumentar a transparência geral da garantia de cibersegurança de produtos e serviços de TIC, a fim de reforçar a confiança no mercado único digital e na inovação digital.
6. Evitar a fragmentação dos sistemas de certificação na UE e dos requisitos de segurança conexos, bem como dos critérios de avaliação, entre Estados-Membros e setores.

Qual o valor acrescentado da ação a nível da UE?

Dado que a digitalização e interligação da economia e da sociedade têm um alcance mundial, a dimensão dos problemas vai muito para lá do território de um único Estado-Membro, o que, por conseguinte, exige intervenção a nível da União. No contexto atual e ponderando os cenários futuros, constata-se que as ações individuais dos Estados-Membros e uma abordagem fragmentada à cibersegurança, sobretudo à sua forte dimensão transfronteiriça, não conseguem aumentar a ciber-resiliência coletiva da União.

B. SOLUÇÕES

Quais são as várias opções para cumprir os objetivos? Há alguma opção preferida?

A presente avaliação de impacto explora um conjunto específico de opções políticas, que abrangem a revisão da Agência da União Europeia para a Segurança das Redes e da Informação (ENISA) e a certificação da segurança das TIC.

Revisão da ENISA

Opção 0 — Cenário de base — Esta opção consiste em manter o *statu quo*. O mandato da ENISA seria prolongado e os objetivos e atribuições da Agência manter-se-iam em grande parte inalterados, tendo paralelamente em conta as funções confiadas à ENISA pela legislação da UE subsequente (por exemplo, a Diretiva SRI).

Opção 1 — Expiração do mandato da ENISA (extinção da ENISA). Esta opção levaria à extinção da ENISA no fim do seu mandato (junho de 2020) e, eventualmente, a uma redistribuição de competências/atividades a nível da UE e/ou nacional.

Opção 2 — «ENISA reformada». Esta opção teria por base o mandato atual da ENISA com vista a adotar mudanças seletivas que tivessem em conta a evolução do cenário da cibersegurança. A Agência obteria um mandato permanente, baseado nos seguintes elementos fundamentais: apoio ao desenvolvimento e à execução de políticas da UE; reforço das capacidades; conhecimentos e informação; atribuições relacionadas com o mercado; investigação e inovação; cooperação operacional e gestão dos riscos.

Opção 3 — Agência da UE para a Cibersegurança com capacidades operacionais plenas. Esta opção implica reformar a ENISA, juntando três funções principais: 1. Uma função política/consultiva; 2. Um centro de informação e conhecimentos especializados; 3. Uma equipa de resposta a emergências informáticas (CERT). Esta opção implicaria, em grande medida, a mesma mudança do âmbito de aplicação do mandato decorrente da opção 2. No entanto, seriam acrescentadas atribuições adicionais no domínio da resposta a incidentes e gestão de crises, para que a Agência cobrisse todo o ciclo da cibersegurança e lidasse com a prevenção, deteção e resposta a ciberincidentes.

Certificação

Opção 0 — Cenário de base — Não fazer nada. De acordo com esta opção, a Comissão manteria o *statu quo* e não adotaria ações políticas ou legislativas.

Opção 1 — Medidas não legislativas (atos não vinculativos). De acordo com esta opção, a Comissão utilizaria instrumentos políticos não vinculativos (por exemplo, comunicações

interpretativas, apoio a iniciativas de autorregulação e a atividades de normalização a nível da UE), a fim de melhorar a transparência e reduzir a fragmentação.

<u>Opção 2</u> — Um ato legislativo da UE para alargar o acordo SOG-IS a todos os Estados-Membros. De acordo com esta opção política, a Comissão proporia um ato legislativo para alargar juridicamente a filiação a todos os Estados-Membros.

<u>Opção 3</u> - Um quadro geral da UE para a certificação da segurança das TIC. Esta opção implica a criação de um quadro europeu de certificação da segurança das TIC (incluindo um grupo de peritos composto por autoridades nacionais) baseado, tanto quanto possível, nos sistemas de certificação da segurança de TIC existentes. Em suma, o quadro permitiria a criação de sistemas de certificação da UE que seriam aceites nos Estados-Membros.

A opção preferida é uma combinação da opção 2 para a ENISA com a opção 3 para a certificação.

Quais são as diferentes partes interessadas? Quem apoia cada uma das opções?

A grande maioria das partes interessadas de todas as categorias (Estados-Membros, indústria, instituições da UE, comunidade de investigação) que participaram nas consultas parece saudar a opção preferida, sendo a favor do reforço da ENISA e da criação de um quadro europeu de certificação da segurança das TIC.

Concretamente, existe um consenso relativamente à necessidade de ter (no mínimo) uma agência da UE com um mandato permanente e que funcione corretamente, que esteja dotada de recursos adequados e mandatada para enfrentar os desafios de cibersegurança presentes e futuros. Existe também um amplo acordo entre as partes interessadas sobre a criação de um quadro europeu modulável e voluntário.

Do lado da indústria, esta solução para a certificação é apoiada pelas empresas que já estão sujeitas a requisitos de certificação e que beneficiariam de um mecanismo a nível da UE assente no reconhecimento mútuo de certificados. É também apoiada pelas PME, que seriam as mais afetadas se já tiverem, ou se tivessem, de iniciar diferentes processos de certificação em diversos Estados-Membros. Alguns Estados-Membros, sobretudo aqueles com menores recursos, e alguns representantes da indústria e das instituições da UE manifestaram opiniões favoráveis também em relação à opção 3 para a ENISA.

C. IMPACTOS DA OPÇÃO PREFERIDA:

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

De acordo com a opção preferida, a UE teria uma agência concentrada em prestar apoio aos Estados-Membros, às instituições da UE e às empresas em domínios nos quais proporcionaria o maior valor acrescentado. Os mesmos abrangem: o apoio à execução da Diretiva SRI; o desenvolvimento e execução de políticas; o conhecimento, a informação e a sensibilização; a investigação; a cooperação operacional e as crises; o mercado. A ENISA apoiaria, nomeadamente, a política da UE no domínio da certificação da segurança das TIC, assegurando a manutenção administrativa e a gestão técnica de um quadro europeu de certificação da segurança das TIC. Esse quadro criaria eficazmente um conjunto de regras

sobre a governação da certificação da segurança das TIC na UE, o que promoveria um sistema de reconhecimento mútuo de certificados emitidos nos Estados-Membros. A solução, que combina estas duas opções, é considerada a mais eficaz para que a UE consiga alcançar os objetivos identificados: aumentar as capacidades, o estado de preparação, a cooperação, a sensibilização, e a transparência em matéria de cibersegurança, e evitar a fragmentação do mercado. Esta opção é também a mais coerente com as prioridades políticas, dado que está enraizada na Estratégia para a Cibersegurança e em políticas conexas (por exemplo, a Diretiva SRI), e na Estratégia para o Mercado Único Digital. Além disso, esta opção alcançaria os objetivos mediante uma utilização razoável de recursos.

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

Apesar de receber novas funções, uma «ENISA reformada» continuaria a ser uma organização ágil. A contribuição financeira necessária do orçamento da UE seria superior à atual, mas ainda assim bastante inferior à de outras agências que também operam em áreas cruciais.

A criação de um quadro europeu de certificação da segurança das TIC não implicaria custos adicionais e iniciais para a indústria (incluindo as PME). Pelo contrário, geraria economias significativas para as empresas que já certificam os seus produtos ou que estão dispostas a realizar uma certificação da segurança, com efeitos benéficos na sua competitividade a nível mundial. Por outro lado, envolveria algumas autorizações orçamentais para assegurar a manutenção do quadro, que seria sobretudo fornecida pelo modelo da «ENISA reformada», no que diz respeito às funções técnicas e de secretariado.

Haverá impactos significativos nos orçamentos e administrações nacionais?

Não. Os custos associados ao reforço da ENISA serão maioritariamente suportados pelo orçamento da UE, embora os Estados-Membros continuem a poder prestar contribuições financeiras a título voluntário à Agência. No tocante à certificação, o principal impacto nos orçamentos e administrações nacionais resultaria da instituição de uma autoridade de certificação, quando apropriado.

Haverá outros impactos significativos?

Não.

Proporcionalidade?

A opção preferida inclui medidas equilibradas, todas consideradas necessárias para alcançar os objetivos em causa, sem impor encargos excessivos às partes interessadas. Nesta perspetiva, considera-se que a iniciativa cumpre o princípio da proporcionalidade.

D. SEGUIMENTO

Quando será reexaminada a medida proposta?

Propõe-se que a primeira avaliação ocorra cinco anos após a entrada em vigor do instrumento jurídico. Posteriormente, a Comissão comunicará ao Parlamento Europeu e ao Conselho a sua avaliação, acompanhada, quando pertinente, de uma proposta de revisão. São necessárias avaliações posteriores, que devem realizar-se de cinco em cinco anos.