Conselho da
União Europeia

Bruxelas, 2 de dezembro de 2020
(OR. en)

13629/20

CYBER 263
TELECOM 248
COPEN 362
CODEC 1266
COPS 441
COSI 235
CSC 344
CSCI 86
IND 248
RECH 493
ESPACE 77

RESULTADOS DOS TRABALHOS

de:	Secretariado-Geral do Conselho
data:	2 de dezembro de 2020
para:	Delegações
Assunto:	Conclusões do Conselho sobre a cibersegurança dos dispositivos conectados – Conclusões do Conselho aprovadas por procedimento escrito

Junto se enviam, à atenção das delegações, as Conclusões do Conselho sobre a cibersegurança dos dispositivos conectados, aprovadas pelo Conselho por procedimento escrito em 2 de dezembro de 2020.

ANEXO

Conclusões do Conselho sobre a cibersegurança dos dispositivos conectados

O Conselho da União Europeia,

RECORDANDO

- as conclusões do Conselho sobre a comunicação conjunta da Comissão ao Parlamento Europeu e ao Conselho intitulada: "Resiliência, dissuasão e defesa: reforçar a cibersegurança na UE",
- as conclusões do Conselho sobre o desenvolvimento de capacidades e competências em matéria de cibersegurança na UE,
- as conclusões do Conselho sobre a importância da tecnologia 5G para a economia europeia e a necessidade de atenuar os riscos de segurança a ela associados,
- as conclusões do Conselho sobre o futuro de uma Europa altamente digitalizada para além de 2020, intituladas: "Impulsionar a competitividade digital e económica na União e a coesão digital",
- as conclusões do Conselho sobre a construção do futuro digital da Europa,
- as conclusões do Conselho Europeu sobre a COVID-19, o mercado único, a política industrial, a digitalização e as relações externas,
- a comunicação da Comissão Europeia intitulada "Construir o futuro digital da Europa".

1. SALIENTA que a União Europeia e os seus Estados-Membros têm de assegurar a sua soberania digital e a sua autonomia estratégica, preservando ao mesmo tempo uma economia aberta. Tal inclui o reforço da capacidade de fazer escolhas tecnológicas autónomas e, enquanto um dos principais pilares, infraestruturas, produtos e serviços resilientes e seguros para aumentar a confiança no mercado único digital e a nível da sociedade europeia. Os valores fundamentais da União Europeia preservam, em particular, a privacidade, a segurança, a igualdade, a dignidade humana, o Estado de direito e a Internet aberta como condições prévias para alcançar uma sociedade, uma economia e uma indústria impulsionadas pela digitalização e centradas no ser humano.

2. RECONHECE a importância crescente dos dispositivos conectados e da respetiva segurança, incluindo máquinas, sensores e redes que compõem a Internet das coisas (IdC). Os dispositivos conectados terão um papel fundamental a desempenhar na construção do futuro digital da Europa, tanto do ponto de vista industrial e empresarial, como na vida quotidiana dos consumidores de uma nova geração de tecnologia. Para além da tecnologia 5G, a inteligência artificial, a computação quântica, a computação de alto desempenho, a computação na nuvem, as tecnologias de registo distribuído, nomeadamente a cadeia de blocos, e quaisquer outras novas aplicações e oportunidades para um crescimento económico sustentável e um nível mais elevado de digitalização da nossa sociedade só podem ser alcançadas através de dispositivos conectados ciberseguros.

3. OBSERVA que o aumento da utilização de produtos de consumo e de dispositivos industriais ligados à Internet implicará também novos riscos para a privacidade, a segurança da informação e a cibersegurança, incluindo um aumento dos potenciais impactos na integridade e disponibilidade de produtos e dados, o que poderá afetar diretamente a segurança. É essencial minimizar esses riscos a fim de proteger os consumidores, reforçar a ciber-resiliência global da Europa e aumentar a confiança dos cidadãos nas soluções e tecnologias digitais, o que promoverá também a competitividade e as capacidades de inovação dos fornecedores europeus desses dispositivos. A cibersegurança e a privacidade deverão ser reconhecidas como requisitos essenciais no que toca aos processos de inovação, de produção e de desenvolvimento dos produtos, incluindo a fase de conceção (segurança desde a conceção), e deverão ser asseguradas ao longo de todo o ciclo de vida de um produto e em toda a sua cadeia de abastecimento.

4. SALIENTA que, para além de garantir um elevado nível de segurança dos dispositivos conectados, é igualmente importante aumentar a sensibilização dos consumidores para os seus potenciais riscos em matéria de privacidade e segurança. Tal ajudaria a minimizar as ameaças decorrentes do aumento da utilização de dispositivos conectados, a aumentar a confiança no mercado único digital e a tirar o máximo partido dos benefícios económicos e sociais que as tecnologias de dispositivos conectados oferecem.

5. SUBLINHA que o investimento público em investigação e inovação, nomeadamente através do Horizonte Europa e da Europa Digital, bem como o investimento privado, poderiam gerar incentivos valiosos para aumentar a segurança e a proteção dos dispositivos conectados e, consequentemente, a resiliência das redes de comunicação inteligentes. Importa também acelerar o investimento em infraestruturas e tecnologias digitais necessárias à aplicação das mais recentes tecnologias de dispositivos conectados, a fim de alcançar a liderança industrial e digital e assegurar a autonomia estratégica, preservando ao mesmo tempo uma economia aberta.

6. SALIENTA a necessidade de assegurar um elevado nível de complementaridade e de comparabilidade das funcionalidades de segurança dos sistemas e componentes das TIC, utilizadas em muitos setores diferentes do mercado único digital.

7. RECONHECE a atual evolução a nível da União no sentido de aumentar o nível de cibersegurança dos dispositivos conectados, em particular no que diz respeito às recentes iniciativas da Comissão para abordar, a curto prazo, aspetos de cibersegurança nos atos jurídicos pertinentes, por exemplo os que se inserem no novo quadro legislativo, em particular a Diretiva 2014/53/UE (Diretiva Equipamento de Rádio). SUBLINHA a importância de avaliar a necessidade de dispor, a longo prazo, de uma legislação horizontal que especifique também as condições necessárias para a colocação no mercado, a fim de abordar todos os aspetos relevantes da cibersegurança dos dispositivos conectados, tais como a disponibilidade, a integridade e a confidencialidade. CONGRATULA-SE, a este respeito, com um debate para explorar o âmbito de aplicação dessa legislação e as suas ligações ao quadro de certificação da cibersegurança, tal como definido no Regulamento Cibersegurança, com o objetivo de aumentar o nível de segurança no mercado único digital.

8. SALIENTA que os requisitos em matéria de cibersegurança deverão ser definidos em conformidade com a legislação pertinente da União, incluindo o Regulamento Cibersegurança, o novo quadro legislativo, o regulamento relativo à normalização europeia e uma eventual legislação horizontal futura, de modo a evitar a ambiguidade e a fragmentação da legislação.

9. RECONHECE o importante papel de todas as partes interessadas, em particular dos fabricantes, para aumentar o nível de cibersegurança dos dispositivos conectados no mercado único digital, pelo que APELA à coordenação e à estreita cooperação de todos os intervenientes públicos e privados, tendo também em vista uma eventual legislação horizontal futura.

9-A. CONGRATULA-SE com os trabalhos em curso conduzidos pela ENISA no sentido de elaborar os primeiros sistemas de certificação da cibersegurança da UE, nomeadamente a proposta de critérios comuns da União Europeia e a proposta de sistemas relativos aos prestadores de serviços de computação em nuvem. Estes sistemas constituirão alicerces importantes para certificar dispositivos conectados.

10. SALIENTA que qualquer sistema adicional de certificação de dispositivos conectados e de serviços conexos que seja estabelecido no programa de trabalho evolutivo da União e definido ao abrigo do Regulamento Cibersegurança deverá especificar o modo como os requisitos de segurança aplicáveis ao nível de segurança pertinente devem ser cumpridos com base em normas europeias e internacionalmente reconhecidas, independentemente do setor em que o produto seja utilizado, e quais as especificações de ensaio, certificados, etc., a aplicar.

11. RECONHECE que a certificação de dispositivos conectados exigiria normas, padrões ou especificações técnicas pertinentes para as avaliações da cibersegurança no âmbito do Regulamento Cibersegurança. Por conseguinte, SALIENTA a necessidade de estabelecer normas, padrões e especificações técnicas de cibersegurança para dispositivos conectados e RECOMENDA que se intensifiquem os esforços envidados pelas organizações europeias de normalização nesta matéria. Ao mesmo tempo, REGISTA que a norma de segurança ETSI EN 303 645 em matéria de cibersegurança para dispositivos da Internet das coisas (IdC) destinados ao consumidor constitui um passo importante neste sentido.

12. CONVIDA a Comissão a considerar a possibilidade de apresentar um pedido de propostas de sistemas de certificação da cibersegurança para dispositivos conectados e serviços conexos com base no programa de trabalho evolutivo da União, cuja elaboração está em curso, tendo na melhor conta os sistemas horizontais europeus de certificação da cibersegurança atualmente em desenvolvimento. A título voluntário, um sistema deste tipo permitirá aos fabricantes desses produtos promover produtos com o nível de segurança avaliado.

13. PROPÕE que se realize um debate sobre a forma de consagrar o objetivo em matéria de cibersegurança numa futura legislação horizontal que abranja os riscos no domínio da cibersegurança associados aos dispositivos conectados, e ao mesmo tempo REGISTA a necessidade de ponderar, se for caso disso, a adaptação dos requisitos essenciais das diretivas pertinentes do novo quadro legislativo.

14. INCENTIVA a Comissão a avaliar igualmente, se necessário, as regulamentações setoriais complementares que deverão definir o nível de cibersegurança que o dispositivo conectado deverá cumprir, a fim de assegurar que os requisitos específicos em matéria de segurança e privacidade se aplicam a esses dispositivos que apresentam riscos de segurança acrescidos.

15. SALIENTA a necessidade de melhorar a qualidade de vida e o bem-estar dos cidadãos europeus e de promover a confiança no mercado único digital. A segurança e a privacidade das nossas sociedades são essenciais para a preservação dos valores fundamentais da União. Assim, SALIENTA que o quadro fornecido pelo Regulamento Cibersegurança deverá servir de base para harmonizar os requisitos de segurança, em função dos diferentes níveis de segurança, em todos os setores do novo quadro legislativo, a fim de evitar a fragmentação e os múltiplos controlos de requisitos idênticos e de oferecer condições equitativas em toda a União Europeia para a concorrência e a inovação.

16. CONVIDA a Comissão, a Agência da UE para a Cibersegurança (ENISA), o Comité de Avaliação da Conformidade e de Fiscalização do Mercado das Telecomunicações e o Grupo Europeu para a Certificação da Cibersegurança a participarem ativamente nesta iniciativa para reforçar o mercado único digital e aumentar a confiança nos produtos, serviços e processos das TIC para dispositivos conectados, assegurando a privacidade e a cibersegurança, e para promover o aumento da competitividade mundial da indústria da União no domínio da IdC através da garantia dos mais elevados padrões de resiliência, segurança e proteção.

17. SALIENTA, neste contexto, a necessidade de apoiar as PME enquanto elemento essencial do ecossistema europeu de cibersegurança, e INCENTIVA as PME a participarem em todas as consultas públicas lançadas, bem como nas atividades de normalização, de modo a que o seu valioso e importante contributo no sentido de tornar a cibersegurança uma meta acessível e uma vantagem competitiva no mercado europeu seja tido em conta.

18. OBSERVA que a obrigação de assegurar a cibersegurança e a privacidade ao longo de todo o ciclo de vida de um produto e em toda a sua cadeia de abastecimento pode ter um impacto positivo na pegada ambiental do setor tecnológico, conduzindo os fabricantes a processos de desenvolvimento e produção inteligentes e sustentáveis, reduzindo assim a quantidade de resíduos eletrónicos relacionados com a eliminação de dispositivos conectados.