Parlamento Europeu
2014-2019

Documento de sessão

B8-0153/2019

6.3.2019

PROPOSTA DE RESOLUÇÃO

apresentada na sequência de declarações do Conselho e da Comissão

nos termos do artigo 123.º, n.º 2, do Regimento

sobre ameaças para a segurança decorrentes da crescente presença tecnológica da China na UE e eventual ação ao nível da UE para reduzir tais riscos (2019/2575(RSP))

Tiziana Beghin, Dario Tamburrano, Isabella Adinolfi, Rolandas Paksas
em nome do Grupo EFDD

B8-0153/2019

Resolução do Parlamento Europeu sobre as ameaças para a segurança decorrentes da crescente presença tecnológica da China na UE e eventual ação ao nível da UE para reduzir tais riscos
(2019/2575(RSP))

O Parlamento Europeu,

– Tendo em conta as comunicações da Comissão, de 14 de setembro de 2016, intituladas «Conectividade para um Mercado Único Digital Concorrencial – Rumo a uma Sociedade Europeia a Gigabits» (COM(2016)0587) e «5G para a Europa: um Plano de ação» (COM(2016)0588),

– Tendo em conta a proposta alterada da Comissão de regulamento do Parlamento Europeu e do Conselho relativo ao acesso de bens e serviços de países terceiros ao mercado interno de contratos públicos da União Europeia e que estabelece os procedimentos de apoio às negociações sobre o acesso de bens e serviços da União Europeia aos mercados de contratos públicos dos países terceiros (COM(2016)0034),

– Tendo em conta a Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União[1] (Diretiva SRI),

– Tendo em conta a proposta de regulamento do Parlamento Europeu e do Conselho, de 13 de setembro de 2017, 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)0477),

– Tendo em conta a Diretiva (UE) 2018/1972 do Parlamento Europeu e do Conselho, de 11 de dezembro de 2018, que estabelece o Código Europeu das Comunicações Eletrónicas[2],

– Tendo em conta a proposta da Comissão de regulamento do Parlamento Europeu e do Conselho que estabelece o Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança e a Rede de Centros Nacionais de Coordenação (COM(2018)0630),

– Tendo em conta o processo de resolução de litígios no âmbito da OMC (WT/DS549/6), de 1 de junho de 2018, relativo a certas medidas impostas pela China relativamente à transferência de tecnologia estrangeira para a China,

– Tendo em conta a sua posição, adotada em primeira leitura em 14 de fevereiro de 2019, sobre a proposta de regulamento do Parlamento Europeu e do Conselho que estabelece

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

um quadro para a análise de investimentos diretos estrangeiros na União Europeia[3],

– Tendo em conta as negociações em curso entre a UE e a China com vista a um acordo global em matéria de investimento,

– Tendo em conta o artigo 123.º, n.º 2, do seu Regimento,

A. Considerando que os recentes progressos no domínio das TIC, incluindo as telecomunicações de quinta geração (5G), abriram novas perspetivas para a produção, a distribuição e o usufruto de bens e serviços, bem como para a interação entre dispositivos e entre cidadãos, administrações públicas e outros intervenientes socioeconómicos, e, por conseguinte, têm potencial para impulsionar a economia europeia;

B. Considerando que a cibersegurança no domínio das TIC, a proteção das informações sensíveis, o respeito pelos direitos individuais e a salvaguarda contra ciberameaças externas são condições prévias para garantir a soberania tecnológica dos cidadãos da UE e, em última análise, trazer prosperidade à UE e apoiar a sua democracia;

C. Considerando que a investigação e os ensaios relativos à tecnologia 5G dificilmente conseguem acompanhar a pressão internacional em prol da implantação e da comercialização de 5G, ao passo que alguns estudos científicos suscitaram preocupações e incertezas quanto à segurança desta tecnologia, especialmente no que diz respeito aos riscos de poluição eletromagnética para a saúde humana e o ambiente;

D. Considerando que a cibersegurança das redes 5G constitui um novo e complexo desafio, devido à natureza virtualizada e descentralizada da 5G e à sua cadeia de valor fragmentada e altamente especializada, desde a produção à distribuição, abrangendo também a instalação, a configuração, o funcionamento, a manutenção e as atualizações de software; considerando que a UE tem de colmatar o défice em termos de cibersegurança nas suas infraestruturas críticas nos setores das telecomunicações, da energia, dos transportes, da saúde, da defesa e da segurança, entre outros;

E. Considerando que a garantia de redes 5G seguras é uma tarefa que não pode ser efetuada isoladamente por fabricantes ou operadores de redes, mas que requer uma ação coordenada e eficaz por parte de todas as autoridades nacionais e internacionais pertinentes;

F. Considerando que a UE tem potencial para liderar o desenvolvimento de tecnologias de cibersegurança, proporcionando apoio às empresas europeias neste setor e promovendo todas as alterações na cadeia de valor que possam reduzir a dependência da UE em relação à tecnologia estrangeira;

G. Considerando que a UE tem vindo a desenvolver um conjunto de medidas para assegurar a cibersegurança, incluindo a Diretiva SRI e o Regulamento Cibersegurança, que devem ser aplicadas rapidamente e continuamente acompanhadas, a fim de garantir que continuem a ser eficazes ao longo das atualizações e revisões necessárias;

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

H. Considerando que a presença crescente de fornecedores de tecnologia chineses e de outros países terceiros se tornou evidente no mercado da 5G da UE, nomeadamente empresas públicas ou empresas que não oferecem transparência;

I. Considerando que a reciprocidade é uma das formas mais eficazes de progredir no sentido de condições de concorrência equitativas a nível mundial;

J. Considerando que as empresas estrangeiras têm de lidar com as discrepâncias existente nas normas da UE em matéria de proteção de dados entre o Regulamento Geral sobre a Proteção de Dados e diferentes requisitos previstos nas legislações nacionais;

K. Considerando que a UE e a China estão a negociar um acordo global em matéria de investimento desde 2013; considerando que o acordo proposto contribuiria para resolver questões de acesso ao mercado, estabelecer um quadro para a proteção dos investimentos e definir normas laborais e ambientais de base;

L. Considerando que surgiram provas, embora inconclusivas, sobre falhas de segurança nos equipamentos fornecidos por fornecedores de países terceiros, incluindo a China, que podem colocar em perigo os direitos individuais à vida privada e à proteção de informação sensível na UE;

1. Salienta que a implantação e a comercialização da 5G devem ser realizadas em conformidade com o princípio da precaução, antevendo todos os atores socioeconómicos os potenciais impactos em matéria de segurança e tomando precauções proporcionadas, incluindo a rápida divulgação de fatores que possam pôr em perigo a saúde pública ou o ambiente;

2. Salienta que os impactos sociais e económicos da 5G e das tecnologias que esta potencia, desde a Internet das coisas à inteligência artificial, devem ser cuidadosamente avaliados, devendo ser tomadas medidas para que a transição para a sociedade europeia a gigabits seja justa e equitativa para todos e se baseie na responsabilidade ética;

3. Insta a Comissão e os Estados-Membros a criarem um ambiente propício à inovação para que os vendedores da UE possam desenvolverem novos produtos, serviços e tecnologias, instando ainda que apoiem o empreendedorismo da UE no domínio da implantação e da comercialização de 5G segura, garantindo ao mesmo tempo que o seu potencial seja acessível a todas as empresas que participem na economia digital da UE, incluindo as pequenas e médias empresas;

4. Recorda que a cibersegurança é um dos principais desafios que a UE enfrenta atualmente e que um eventual fracasso neste domínio pode resultar numa violação da privacidade e dos direitos fundamentais dos consumidores e dos produtores da UE, comprometer seriamente a confiança dos cidadãos em produtos e serviços de TIC e, em última análise, causar graves prejuízos económicos; apela à criação de uma rede segura, por defeito e desde a conceção;

5. Insta a Comissão e os Estados-Membros a cooperarem estreitamente na aplicação da estratégia da UE para a cibersegurança e a conjugarem as medidas nacionais e da UE para minimizar o risco de falhas de segurança e de violações de dados em toda a cadeia de valor; considera que essas medidas podem incluir a certificação de cibersegurança da

UE, requisitos de configuração e procedimentos e práticas operacionais, bem como a promoção da ciber-higiene e da educação digital;

6. Considera que a Agência da UE para a Cibersegurança (Agência da União Europeia para a Segurança das Redes e da Informação – ENISA) tem um papel crucial a desempenhar na análise de eventuais ameaças resultantes das intervenções de fornecedores estrangeiros, incluindo a China, bem como na coordenação de uma abordagem comum aos Estados-Membros para fazer face às ameaças e aos ataques no domínio da cibersegurança;

7. Insta a Comissão e os Estados-Membros a implementarem rapidamente o pacote de medidas relativas à economia circular e a reforçarem a gestão das matérias-primas ao longo do ciclo de vida destas, bem como a impulsionarem a reciclagem dos resíduos, de modo a melhorar o acesso da UE a matérias-primas críticas, fundamentais para os produtos de alta tecnologia e as inovações emergentes;

8. Considera urgente abordar as eventuais ameaças à segurança da tecnologia resultantes da atual penetração no mercado da UE de vendedores estrangeiros, incluindo a China, adotando uma abordagem comum entre os Estados-Membros em matéria de segurança e proteção de dados;

9. Insta a Comissão e os Estados-Membros a analisarem e a controlarem a segurança dos sistemas de TIC nos quais estejam fortemente presentes tecnologias de países terceiros, nomeadamente através da realização de testes de resistência;

10. Salienta que os fornecedores de países terceiros não devem ser discriminados com base no seu país de origem, mas que, a fim de assegurar condições de concorrência equitativas, devem ser tidos em conta critérios como a transparência destas empresas, as normas de cibersegurança a que estão sujeitas e a existência de condições de reciprocidade para as empresas europeias no país de origem das suas contrapartes;

11. Salienta que os fornecedores e operadores chineses ou de outros países terceiros não podem, caso algum, ameaçar os direitos individuais garantidos pela legislação da UE, mesmo quando existam requisitos diferentes ao abrigo da legislação nacional no seu país de origem;

12. Solicita ao Conselho que aceite reiniciar os debates sobre a nova proposta revista da Comissão relativa ao procedimento que restringe o acesso de produtos estrangeiros ao mercado de contratos públicos da UE, em que não existe acesso recíproco;

13. Recorda a importância de prosseguir a melhoria do processo de negociação referente à cooperação regulamentar no domínio das tecnologias digitais com países terceiros e de assegurar uma maior participação dos mesmos em organismos internacionais de normalização;

14. Encarrega o seu Presidente de transmitir a presente resolução ao Conselho e à Comissão.