Parlamento Europeu
2014-2019

Documento de sessão

B8-0155/2019

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 as ameaças à segurança relacionadas com a crescente presença tecnológica da China na UE e as eventuais medidas a nível da UE para as reduzir
(2019/2575(RSP))

Luděk Niedermayer, Angelika Niebler, Ivo Belet, Paul Rübig
em nome do Grupo PPE

B8-0155/2019

Resolução do Parlamento Europeu sobre as ameaças à segurança no contexto do aumento da presença tecnológica da China na UE e possíveis medidas a tomar a nível da UE para as reduzir
(2019/2575(RSP))

O Parlamento Europeu,

– 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[1],

– 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[2],

– Tendo em conta a Diretiva 2013/40/UE do Parlamento Europeu e do Conselho, de 12 de agosto de 2013, relativa a ataques contra os sistemas de informação e que substitui a Decisão-Quadro 2005/222/JAI do Conselho[3],

– Tendo em conta a proposta da Comissão de um 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 proposta da Comissão de regulamento do Parlamento Europeu e do Conselho, de 12 de setembro de 2018, 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 a adoção da nova Lei Nacional de Informações pelo Congresso Nacional do Povo da República Popular da China, em 28 de junho de 2017,

– Tendo em conta as declarações do Conselho e da Comissão, de 13 de fevereiro de 2019, sobre as ameaças à segurança relacionadas com o aumento da presença tecnológica da China na UE e as eventuais medidas a tomar a nível da UE para a sua redução,

– Tendo em conta a adoção, pelo governo australiano, das «Reformas da segurança no setor das telecomunicações», com efeitos desde 18 de setembro de 2018,

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

[1] JO L 321 de 17.12.2018, p. 36
[2] JO L 194 de 19.7.2016, p. 1
[3] JO L 218 de 14.8.2013, p. 8.

um quadro para a análise de investimentos diretos estrangeiros na União Europeia[4],

– Tendo em conta as suas resoluções sobre as relações UE-China, em particular a resolução de 12 de setembro de 2018 sobre o estado das relações UE-China[5],

– Tendo em conta a comunicação da Comissão, de 14 de setembro de 2016, intitulada «5G para a Europa: um Plano de Ação» (COM(2016)0588),

– Tendo em conta a sua Resolução, de 1 de junho de 2017, sobre conetividade à Internet para o crescimento, a competitividade e a coesão: a sociedade europeia a gigabits e 5G[6],

– Tendo em conta o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)[7],

– Tendo em conta o Regulamento (UE) n.º 1316/2013 do Parlamento Europeu e do Conselho, de 11 de dezembro de 2013, que institui o Mecanismo Interligar a Europa, que altera o Regulamento (UE) n.º 913/2010 e revoga os Regulamentos (CE) n.º 680/2007 e (CE) n.º 67/2010[8],

– Tendo em conta a proposta da Comissão de um regulamento do Parlamento Europeu e do Conselho que cria o programa Europa Digital para o período de 2021-2027 (COM(2018)0434),

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

A. Considerando que a UE deve dinamizar a sua agenda de cibersegurança, a fim de tirar pleno partido do potencial de se tornar líder no domínio da cibersegurança e utilizar este estatuto em benefício da sua indústria;

B. Considerando que podem ser exploradas vulnerabilidades nas redes 5G para comprometer os sistemas de TI que poderão causar danos muito graves às economias, tanto a nível nacional como europeu; que é necessária uma abordagem baseada na análise de risco para toda a cadeia de valor, a fim de minimizar os riscos;

C. Considerando que a rede 5G será a espinha dorsal da nossa infraestrutura digital, aumentando a possibilidade de ligar vários dispositivos às redes (Internet das coisas, etc.), e trará novas vantagens e oportunidades à sociedade e às empresas em muitos domínios, incluindo os setores críticos da economia, nomeadamente os transportes, a energia, a saúde, as finanças, as telecomunicações, a defesa, o espaço e a segurança;

D. Considerando que a criação de um mecanismo adequado de resposta aos desafios em matéria de segurança daria à UE a oportunidade de tomar medidas ativas no contexto do

[4] Textos Aprovados, P8_TA(2019)0121.
[5] Textos Aprovados, P8_TA(2018)0343.
[6] JO C 307 de 30.8.2018, p. 144.
[7] JO L 119 de 4.5.2016, p. 1.
[8] JO L 348 de 20.12.2013, p. 129.

estabelecimento de normas relativas às redes 5G;

E. Considerando que foram manifestados receios relativamente aos fornecedores de equipamentos de países terceiros que poderão representar um risco de segurança para a UE devido à legislação do seu país de origem, especialmente após a adoção da Lei da Segurança do Estado chinesa, que prevê a obrigação de todos os cidadãos, empresas e outras entidades cooperarem com o Estado para salvaguardar a segurança deste; que não há qualquer garantia de que estas obrigações não sejam objeto de aplicação extraterritorial e que as reações aos regulamentos chineses variam em alguns países, desde avaliações de segurança até à proibição pura e simples;

F. Considerando que, em dezembro de 2018, a autoridade nacional checa para a cibersegurança emitiu um alerta contra as ameaças de segurança que as tecnologias fornecidas pelas empresas chinesas Huawei e ZTE representavam; que, posteriormente, em janeiro de 2019, as autoridades fiscais checas excluíram a Huawei de um concurso que tinha como objetivo a criação de um portal fiscal;

G. Considerando que é necessária uma investigação aprofundada para esclarecer se os dispositivos envolvidos ou quaisquer outros dispositivos ou fornecedores representam riscos de segurança devido a características como as portas de acesso não autorizadas («backdoors») dos sistemas;

H. Considerando que as soluções devem ser coordenadas e abordadas a nível da UE, de modo a evitar diferentes níveis de segurança e potenciais lacunas na cibersegurança; que também é necessária uma coordenação a nível global para garantir uma resposta forte;

I. Considerando que aos benefícios do mercado único se junta a obrigação de cumprir as normas e o quadro jurídico da UE e que os fornecedores não deveriam ser tratados de forma diferente consoante o seu país de origem;

J. Considerando que o regulamento que estabelece um quadro para a análise de investimentos diretos estrangeiros na União Europeia, que deverá entrar em vigor até ao final de 2020, reforça a capacidade dos Estados-Membros para analisar o investimento estrangeiro com base na segurança e na ordem pública e institui um mecanismo de cooperação que permite que a Comissão e os Estados-Membros colaborem na avaliação que fazem dos riscos para a segurança, nomeadamente em matéria de cibersegurança, colocados por investimentos estrangeiros sensíveis, abrangendo também projetos e programas de interesse para a União, como as redes transeuropeias de telecomunicações e o programa Horizonte 2020;

1. Está convicto de que a União tem de assumir a liderança no domínio da cibersegurança através de uma abordagem comum baseada na utilização eficaz e eficiente dos conhecimentos especializados da UE, dos Estados-Membros e da indústria, uma vez que a existência de decisões nacionais díspares seria prejudicial para o mercado único digital;

2. Manifesta profunda preocupação face às recentes alegações, segundo as quais o equipamento 5G desenvolvido por empresas chinesas integra portas de acesso não autorizadas, o que permite aos fabricantes e às autoridades o acesso não autorizado a dados e a telecomunicações dos cidadãos e das empresas da UE;

3. Manifesta, igualmente, a sua preocupação com a possível existência de grandes vulnerabilidades no equipamento 5G destes fabricantes, caso viesse a ser instalado quando as redes 5G forem disponibilizadas nos próximos anos;

4. Sublinha que as implicações para a segurança das redes e dos equipamentos são semelhantes em todo o mundo e insta a UE a tirar lições da experiência acumulada, de modo a poder garantir as mais elevadas normas de cibersegurança; insta a Comissão a desenvolver uma estratégia que coloque a Europa numa posição de liderança no domínio da tecnologia de cibersegurança e que vise reduzir a dependência da Europa de tecnologia estrangeira neste domínio;

5. Insta os Estados-Membros a informarem a Comissão acerca das medidas nacionais que tencionem adotar nesta matéria, de molde a coordenar a resposta da União para garantir os mais elevados padrões de cibersegurança em toda a União e reitera a importância de evitar a introdução de medidas unilaterais desproporcionadas que fragmentariam o mercado único;

6. Reitera que as entidades que fornecem equipamentos ou serviços na UE, independentemente do seu país de origem, devem cumprir as obrigações em matéria de direitos fundamentais e a legislação da UE e dos Estados-Membros, incluindo o quadro jurídico aplicável à privacidade, à proteção de dados e à cibersegurança;

7. Insta a Comissão a avaliar a robustez do quadro jurídico da União, de modo a dar resposta aos receios de existência de equipamento vulnerável em setores estratégicos e infraestruturas de base; insta a Comissão a apresentar iniciativas, incluindo propostas legislativas, se for caso disso, a fim de sanar as eventuais lacunas detetadas em tempo oportuno, uma vez que a União está num processo permanente de identificação e resolução dos desafios em matéria de cibersegurança e de reforço da resiliência da cibersegurança na UE;

8. Insta os Estados-Membros que ainda não transpuseram integralmente a Diretiva (UE) 2016/1148 relativa à segurança das redes e da informação (Diretiva SRI) a fazerem-no sem demora, e exorta a Comissão a seguir de perto esta transposição para garantir que as suas disposições sejam aplicadas de forma adequada e que os cidadãos europeus beneficiem de melhor proteção contra as ameaças externas de segurança;

9. Exorta a Comissão e os Estados-Membros a assegurarem que os mecanismos de comunicação introduzidos pela Diretiva SRI sejam devidamente aplicados; observa que a Comissão e os Estados-Membros devem acompanhar cuidadosamente quaisquer incidentes de segurança ou reações inadequadas de fornecedores, a fim de colmatar as lacunas identificadas;

10. Insta a Comissão a ponderar a necessidade de alargar o âmbito de aplicação da diretiva a novos setores e serviços críticos que não sejam abrangidos por legislação específica, como, por exemplo, a infraestrutura de rede;

11. Saúda e apoia o acordo alcançado sobre o Regulamento Cibersegurança e o reforço do mandato da Agência da UE para a Cibersegurança (ENISA), a fim de melhor apoiar os Estados-Membros na luta contra as ameaças e os ataques à cibersegurança;

12. Recorda que a cibersegurança exige normas de segurança elevadas; apela à criação de uma rede segura, por defeito e desde a conceção; exorta os Estados-Membros, juntamente com a Comissão, a explorarem todos os meios disponíveis para garantir um elevado nível de segurança;

13. Insta a Comissão a mandatar a ENISA para que dê prioridade ao desenvolvimento de um sistema de certificação para o equipamento 5G, a fim de garantir que a implantação da tecnologia 5G na União cumpra as mais elevadas normas de segurança e seja resistente a «backdoors» ou a grandes vulnerabilidades que comprometeriam a segurança das redes de telecomunicações da União e dos serviços dependentes; recomenda que se confira especial atenção aos processos, produtos e programas informáticos de uso corrente que, por uma mera questão de escala, têm um impacto importante no quotidiano dos cidadãos e na economia;

14. Congratula-se vivamente com as propostas relativas a centros de competências em cibersegurança e a uma rede de centros de coordenação nacionais, destinada a ajudar a UE a manter e a desenvolver as capacidades tecnológicas e industriais em cibersegurança necessárias para salvaguardar o seu mercado único digital;

15. Reitera a sua posição relativamente ao Programa Europa Digital, que impõe requisitos de segurança e a fiscalização, pela Comissão, das entidades estabelecidas na UE mas controladas a partir de países terceiros, em particular no que se refere a ações relacionadas com a cibersegurança;

16. Insta os Estados-Membros a zelarem por que as instituições públicas e as empresas privadas encarregadas de garantir o bom funcionamento das redes de infraestruturas críticas, como as telecomunicações, a energia, os sistemas de saúde e os sistemas sociais, procedam a avaliações de riscos pertinentes tendo em conta as ameaças à segurança especificamente associadas às características técnicas do sistema em causa ou à dependência de fornecedores externos de tecnologias de hardware e software;

17. Recorda que o atual quadro jurídico para as telecomunicações exige que os Estados-Membros se certifiquem de que os operadores de telecomunicações respeitem a integridade e a disponibilidade das redes de comunicações eletrónicas públicas; salienta que, de acordo com o Código Europeu das Comunicações Eletrónicas, os Estados-Membros dispõem de todos os poderes necessários para investigar e aplicar uma vasta gama de medidas corretivas em caso de não conformidade dos produtos presentes no mercado da UE;

18. Insta a Comissão e os Estados-Membros a tornarem o aspeto da segurança um elemento obrigatório em todos os procedimentos de adjudicação de contratos públicos para as infraestruturas importantes, tanto a nível da UE como a nível nacional;

19. Insta a Comissão e os Estados-Membros a reforçarem a transparência e a segurança através do desenvolvimento de processos de adjudicação de contratos multifaseados para a infraestrutura de TIC, o que permitiria efetuar uma distinção entre os concursos relativos à arquitetura destes sistemas, à sua produção, ao seu funcionamento e à sua manutenção, e distinguir os diferentes fornecedores de tecnologia;

20. Recorda aos Estados-Membros a obrigação que lhes incumbe por força do direito penal

da UE de imporem sanções, nomeadamente multas ou coimas, contra pessoas singulares que cometam infrações penais, tais como ataques contra sistemas de informação, interferência ilegal no sistema, interferência ilegal nos dados e interceção ilegal de dados; salienta que os Estados-Membros devem também recorrer à possibilidade de imposição de outras sanções contra estas entidades jurídicas, como a interdição temporária ou definitiva do exercício de atividades comerciais;

21. Espera que as autoridades nacionais de proteção de dados, assim como a Autoridade Europeia para a Proteção de Dados, investiguem exaustivamente os indícios de violação de dados por parte de fornecedores externos e imponham multas e sanções adequadas, em conformidade com a legislação europeia em matéria de proteção de dados;

22. Congratula-se com a próxima entrada em vigor de um regulamento que estabelece um quadro para a análise dos investimentos diretos estrangeiros por razões de segurança e de ordem pública e sublinha que este regulamento estabelece, pela primeira vez, uma lista de áreas e fatores, incluindo as comunicações e a cibersegurança, que são relevantes para a segurança e a ordem pública a nível da UE;

23. Reitera a necessidade de a UE apoiar a cibersegurança em toda a cadeia de valor, desde a investigação até à utilização e implantação de tecnologias essenciais, divulgar informações pertinentes e promover a ciber-higiene e um plano de estudos sobre cibersegurança, e considera que o programa Europa Digital será um instrumento eficaz para o efeito, entre outras medidas;

24. Insta a Comissão e os Estados-Membros a tomarem as medidas necessárias, incluindo sistemas de investimento robustos, a fim de criar um ambiente propício à inovação na UE, que seja acessível a todas as empresas da economia digital da UE, incluindo as pequenas e médias empresas (PME); apela ainda no sentido de que esse ambiente permita que os fornecedores europeus desenvolvam novos produtos, serviços e tecnologias, promovendo assim a sua competitividade;

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