Parlamento Europeu
2014-2019

Documento de sessão

B8-0162/2019

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))

Helmut Scholz, Kostadinka Kuneva, Martina Michels, Eleonora Forenza, Stelios Kouloglou, Dimitrios Papadimoulis
em nome do Grupo GUE/NGL

B8-0162/2019

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 o Relatório sobre a Economia da Informação de 2017, intitulado «Digitalização, Comércio e Desenvolvimento», publicado pela Conferência das Nações Unidas sobre Comércio e Desenvolvimento (CNUCED/IER/2017),

– Tendo em conta o Relatório sobre Comércio e Desenvolvimento de 2018, intitulado «Poder, Plataformas e Ilusão do Livre Comércio», publicado pela Conferência das Nações Unidas sobre Comércio e Desenvolvimento (CNUCED/TDR/2018),

– 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 sua resolução de 12 de março de 2014 sobre o programa de vigilância da Agência Nacional de Segurança dos EUA (NSA), os organismos de vigilância em diversos Estados-Membros e o seu impacto nos direitos fundamentais dos cidadãos da UE e na cooperação transatlântica no domínio da justiça e dos assuntos internos[3],

– Tendo em conta a proposta da Comissão 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 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 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 C 378 de 9.11.2017, p. 104.

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

– 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 a conectividade à Internet para o crescimento, a competitividade e a coesão: a sociedade europeia a gigabits e 5G[5],

– 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)[6],

– 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[7],

– Tendo em conta o Programa Europa Digital,

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

A. Considerando que a UE e os seus Estados-Membros necessitam de um plano de investimento público para desenvolver capacidades de ponta nos setores de alta tecnologia, como a cibersegurança, as TIC, a IA e a economia digital; considerando que foram concebidas várias estratégias da UE, que, no entanto, não foram aplicadas na íntegra;

B. Considerando que é necessário garantir um desenvolvimento digital justo e, ao mesmo tempo, melhorar as condições de vida à escala mundial;

C. Considerando que algumas empresas privadas digitais e de TI, principalmente dos Estados Unidos e da China, continuam a criar monopólios no mercado digital, o que lhes confere o poder de estabelecer normas internacionais e de não exercer as suas responsabilidades sociais;

D. Considerando que a rede 5G será uma das tecnologias-chave das futuras infraestruturas digitais, alargando a possibilidade de ligação de vários dispositivos às redes (Internet das coisas, etc.), e proporcionará novas possibilidades de aplicações em muitos domínios, como os transportes, a mobilidade, a energia, a saúde, as finanças, as telecomunicações, a economia digital e a inteligência artificial;

E. Considerando que podem ser exploradas vulnerabilidades nas redes 5G para comprometer os sistemas de TI, que são suscetíveis de causar danos muito graves aos cidadãos e às suas vidas, bem como às economias nacionais e europeia; considerando

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

que é tecnicamente possível a utilização pelos fornecedores de tecnologia de componentes das tecnologias da rede 5G para violar a privacidade dos dados dos cidadãos, das empresas e das instituições; considerando que é necessária uma abordagem baseada na análise dos riscos em matéria de contratos públicos e de concessão de licenças;

F. Considerando que apenas um número limitado de empresas fornece equipamento técnico 5G;

G. Considerando que empresas de vários países terceiros têm a possibilidade de causar problemas à segurança dos Estados-Membros, uma vez que podem ter acesso a dados pessoais e controlar a infraestrutura digital de muitos setores e serviços estratégicos, e podem igualmente proporcionar acesso aos dados aos serviços nacionais de informações;

H. Considerando que as revelações de Edward Snowden demonstraram que houve um abuso sistemático das redes de comunicação europeias e uma violação maciça do direito dos cidadãos à privacidade dos dados no caso do programa PRISM da Agência Nacional de Segurança dos EUA (NSA) e, no passado, pelo Quartel-General de Comunicações do Governo do Reino Unido (GCHQ);

I. Considerando que as agências de informações do governo dos EUA alegaram que o equipamento da Huawei constitui uma ameaça para a segurança nacional, mas não apresentaram quaisquer provas nesse sentido; considerando que a Huawei é um concorrente económico de várias grandes empresas dos EUA;

J. Considerando que, devido à cadeia de abastecimento mundial de tecnologias de TIC, qualquer proibição da utilização da tecnologia chinesa pode ser prejudicial para as empresas e os operadores europeus, uma vez que irá perturbar o fornecimento de equipamento, aumentar os custos para os operadores da UE e os seus clientes, atrasar a implantação de serviços 5G da próxima geração nos próximos anos e afetar potencialmente as redes existentes;

K. Considerando que a cibersegurança deve ser abordada a nível multilateral para dar lugar a uma resposta forte e coordenada;

L. Considerando que os fornecedores não devem ser tratados de forma diferente em função do seu país de origem, devendo, pelo contrário, ser tratados com base no compromisso e nas garantias que oferecem no tocante à salvaguarda do direito dos cidadãos da UE à privacidade dos dados e à prevenção da espionagem e do envelhecimento da tecnologia;

1. Solicita à Comissão e aos Estados-Membros que desenvolvam uma estratégia e planos de investimento público destinados a reduzir a dependência da Europa de tecnologia estrangeira no domínio da cibersegurança, das TIC, da IA e da economia digital;

2. Considera que os Estados-Membros devem basear as suas decisões relativas ao acesso de empresas de países terceiros a serviços futuros de telecomunicações e 5G nas competências técnicas e numa avaliação de riscos adequada, bem como nos compromissos e garantias dessas empresas no tocante à salvaguarda do direito dos cidadãos da UE à privacidade dos dados e à prevenção da espionagem e do

envelhecimento da tecnologia, e não na pressão política da Administração dos EUA;

3. Solicita à Comissão e aos Estados-Membros que trabalhem em prol de um sistema multilateral de governação em matéria de cibersegurança que vise o estabelecimento de um quadro regulamentar e político das Nações Unidas neste domínio; congratula-se com o lançamento do Índice Global de Cibersegurança das Nações Unidas pela União Internacional das Telecomunicações das Nações Unidas (UIT);

4. Solicita à Comissão e aos Estados-Membros que apliquem integralmente os mecanismos de cooperação introduzidos pela Diretiva Segurança das Redes e da Informação;

5. Solicita à Comissão e aos Estados-Membros que apliquem devidamente o Regulamento Cibersegurança e que se coordenem estreitamente a este respeito;

6. Observa que o fortalecimento do mandato da Agência da União Europeia para a Segurança das Redes e da Informação (ENISA) reforçaria a certificação da cibersegurança e considera que a ENISA poderia desempenhar um papel crucial na análise das ameaças à cibersegurança;

7. Recorda que todas as empresas que fornecem tecnologias e serviços na UE devem cumprir a legislação da UE e dos Estados-Membros e são responsáveis por quaisquer infrações à legislação em matéria de proteção de dados e de cibersegurança;

8. Considera necessário realizar uma avaliação de impacto ambiental rigorosa e independente sobre os eventuais efeitos negativos das tecnologias 5G na saúde humana;

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