



Documento de sessão

B9-0467/2023

20.11.2023

PROPOSTA DE RESOLUÇÃO

apresentada na sequência de uma declaração da Comissão

nos termos do artigo 132.º, n.º 2, do Regimento

sobre a falta de acompanhamento legislativo por parte da Comissão da
Resolução da Comissão de Inquérito PEGA
(2023/2988(RSP))

**Dominik Tarczyński, Ryszard Antoni Legutko, Anna Fotyga, Elżbieta
Kruk, Beata Mazurek, Beata Kempa, Waldemar Tomaszewski**
em nome do Grupo ECR

Resolução do Parlamento Europeu sobre a falta de acompanhamento legislativo por parte da Comissão da Resolução da Comissão de Inquérito PEGA (2023/2988(RSP))

O Parlamento Europeu,

- Tendo em conta o Tratado da União Europeia, nomeadamente o artigo 4.º, n.º 2,
- Tendo em conta o Tratado sobre o Funcionamento da União Europeia (TFUE),
- Tendo em conta o Regulamento (UE) 2021/821 do Parlamento Europeu e do Conselho, de 20 de maio de 2021, que cria um regime da União de controlo das exportações, corretagem, assistência técnica, trânsito e transferências de produtos de dupla utilização¹ («Regulamento Dupla Utilização»),
- Tendo em conta a Decisão (PESC) 2019/797 do Conselho, de 17 de maio de 2019, relativa a medidas restritivas contra os ciberataques que constituem uma ameaça para a União ou os seus Estados-Membros², com a redação que lhe foi dada pela Decisão (PESC) 2021/796 do Conselho, de 17 de maio de 2021³,
- Tendo em conta a Decisão 95/167/CE, Euratom, CECA do Parlamento Europeu, do Conselho e da Comissão, de 6 de março de 1995, relativa às formas de exercício do direito de inquérito do Parlamento Europeu⁴,
- Tendo em conta a Decisão (UE) 2022/480 do Parlamento Europeu, de 10 de março de 2022, sobre a criação de uma comissão de inquérito para investigar a utilização do *software* espião de vigilância Pegasus e equivalentes e que define o objeto do inquérito, bem como as competências, a composição numérica e a duração do mandato da comissão⁵,
- Tendo em conta a Carta das Nações Unidas e os Princípios Orientadores das Nações Unidas sobre Empresas e Direitos Humanos,
- Tendo em conta a Avaliação da Ameaça da Criminalidade Grave e Organizada de 2021 da Europol intitulada «A Corrupting Influence: The Infiltration and Undermining of Europe’s Economy and Society by Organised Crime» (Uma influência corruptora: a infiltração e o enfraquecimento da economia e da sociedade europeias pela criminalidade organizada),
- 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

¹ JO L 206 de 11.6.2021, p. 1.

² JO L 129 I de 17.5.2019, p. 13.

³ JO L 174 I de 18.5.2021, p. 1.

⁴ JO L 78 de 6.4.1995, p. 1.

⁵ JO L 98 de 25.3.2022, p. 72.

cidadãos da UE e na cooperação transatlântica no domínio da justiça e dos assuntos internos⁶, nomeadamente as suas recomendações relativas ao reforço da segurança informática nas instituições, nos órgãos e nos organismos da UE,

- Tendo em conta o relatório da Comissão de Inquérito para Investigar a Utilização do *Software* Espião de Vigilância Pegasus e Equivalentes (A9-0189/2023),
 - Tendo em conta a sua recomendação ao Conselho e à Comissão, de 15 de junho de 2023, na sequência da investigação de alegadas infrações ou má administração na aplicação do Direito da União relacionadas com a utilização do *software* espião de vigilância Pegasus e equivalentes⁷,
 - Tendo em conta o artigo 132.º, n.º 2, do seu Regimento,
- A. considerando que as recomendações propostas pela Comissão Parlamentar de Inquérito para Investigar a Utilização do *Software* Espião de Vigilância Pegasus e Equivalentes («Comissão PEGA») se baseiam no seu relatório sobre o uso e abuso de *software* espião nos países da UE;
 - B. Considerando que a única prova de vigilância foi frequentemente o testemunho de instituições (e iniciativas) com reputação questionável e ligações políticas, como o Projeto Pegasus (suspeito de ter ligações com Edward Snowden), o CitizenLab (uma organização com um perfil claramente de esquerda) e a IA (que ficou desacreditada devido a um relatório pró-russo sobre a situação na Ucrânia);
 - C. Considerando que o *software* espião explora vulnerabilidades nos sistemas operativos dos telemóveis inteligentes para instalar *software* malicioso; que, devido à sua estrutura, o *software* espião torna muito difícil detetar a sua utilização; que é quase impossível rastrear as fontes dessa vigilância, o que torna quaisquer conclusões especulativas;
 - D. Considerando que o relatório da Comissão PEGA é tendencioso e trata os países de forma desigual, condenando, por vezes, as mesmas soluções que considera adequadas noutros momentos;
 - E. Considerando que as recomendações da comissão, devido ao seu vasto âmbito de aplicação, dizem respeito a questões relacionadas com o Tratado da UE, ultrapassando, assim, o mandato da Comissão PEGA;
 - F. Considerando que, nos termos dos Tratados, as questões de segurança nacional continuam a ser da competência exclusiva dos Estados-Membros;
 - G. Considerando que as recomendações visam privar os Estados-Membros da sua liberdade de agir em questões de segurança nacional;
 - H. Considerando que os Estados-Membros se opõem profundamente (e justificadamente) a qualquer tentativa de limitar as suas competências;
 - I. Considerando que os países da UE estão em risco devido ao *software* espião de países

⁶ JO C 378 de 9.11.2017, p. 104.

⁷ Textos Aprovados, P9_TA(2023)0244.

terceiros, que pode ser utilizado tanto pelos serviços destes países como pelos seus próprios serviços;

- J. Considerando que as regras relativas à exportação de *software* espião e de produtos de dupla utilização podem ter de ser reforçadas;
 - K. Considerando que existe um sério risco de vigilância de *software* espião de altos responsáveis políticos e funcionários da UE, incluindo os comissários;
 - L. Considerando que o *software* espião cai frequentemente nas mãos de grupos criminosos;
 - M. Considerando que os conhecimentos sobre as vulnerabilidades dos sistemas informáticos são comercializados, ilegal e diretamente, entre as partes ou através de intermediários; que os intervenientes não estatais e as organizações criminosas estão envolvidos neste comércio;
 - N. Considerando que a investigação da Comissão PEGA mostra que os Estados-Membros devem desenvolver o seu próprio *software* espião independente para fins de defesa e de luta contra a criminalidade organizada;
 - O. Considerando que as disposições dos Tratados devem estabelecer os limites para o debate de propostas de regulamentação do *software* espião;
1. Realça que o relatório e as recomendações da Comissão PEGA não foram o resultado de uma avaliação sólida da situação, mas sim o resultado de um ponto de vista específico e politicamente motivado, não foi desprovido de preconceitos e estereótipos;
 2. Observa que, pelo menos em parte, o relatório e as recomendações foram elaborados no contexto do próximo processo eleitoral ou em curso na Polónia, na Grécia e em Espanha;
 3. Realça que os autores do relatório e das recomendações utilizaram fontes pouco fiáveis e tendenciosas, que distorceram a descrição da situação;
 4. Chama a atenção para a falta de equilíbrio e de critérios iguais na descrição da situação em cada país, o que suscita dúvidas quanto à fiabilidade das recomendações;
 5. Considera que as recomendações da Comissão PEGA ultrapassam o seu mandato e a sua esfera de competência e que, por conseguinte, não se pode esperar que os Estados-Membros e a Comissão as apliquem;
 6. Considera igualmente que a essência das alterações propostas é incompatível com o espírito (e muitas vezes com as disposições individuais) dos Tratados e que, por conseguinte, as recomendações devem ser encaradas como um meio de exercer pressão no debate em curso sobre a alteração dos Tratados;
 7. Está firmemente convicto de que as questões de segurança nacional devem continuar a ser da competência exclusiva dos Estados-Membros e que qualquer tentativa de interferir nestas questões a nível da UE - através de uma regulamentação pormenorizada do *software* espião ou da fixação de limites às questões de segurança nacional -

constitui um ataque aos direitos dos Estados-Membros consagrados nos Tratados;

8. Salienta que, embora o *software* espião represente muitas ameaças, nomeadamente às liberdades cívicas e aos direitos humanos, a sua utilização é, em alguns casos, indispensável; considera que tal se aplica principalmente aos serviços de informação, à defesa nacional e à luta contra a criminalidade organizada; destaca, além disso, que, em tempos de conflitos híbridos, é impossível delimitar claramente as áreas acima referidas;
9. Considera, por conseguinte, que a utilização de *software* espião pelos serviços dos Estados-Membros deve ser limitada ao mínimo e que as decisões nesta matéria devem ser sempre tomadas pelos Estados-Membros soberanos, uma vez que todos dispõem de sistemas democráticos, sistemas jurídicos e instituições capazes de combater eventuais abusos;
10. Alerta para o facto de todas as propostas da Comissão para aplicar as recomendações propostas pela Comissão PEGA virem a encontrar, certamente, uma forte resistência do Conselho, uma vez que os Estados-Membros as considerarão um ataque aos seus direitos e competências;
11. Observa que basear as alterações jurídicas propostas nas recomendações nas disposições do Título V, Capítulo 4, do TFUE significa, na prática, a necessidade de alcançar a unanimidade entre os Estados-Membros, o que parece totalmente irrealista;
12. Partilha, no entanto, as preocupações da Comissão PEGA quanto aos riscos associados à utilização de *software* espião de origem estrangeira, especialmente de países terceiros; considera que a melhor solução para este problema será que os Estados-Membros desenvolvam as suas próprias tecnologias de *software* espião - sob o controlo dos seus serviços e no âmbito da sua própria legislação;
13. Partilha, além disso, as preocupações quanto à exportação de *software* espião da UE para países terceiros; destaca que a regulamentação relativa às exportações (incluindo a exportação dos chamados bens de dupla utilização) pode ser reforçada e deve ser devidamente aplicada e supervisionada;
14. Considera que uma melhor regulamentação a nível da UE sobre a importação de *software* espião e de produtos de dupla utilização (por exemplo, para impedir a sua aquisição por grupos criminosos) parece justificar-se, mas é extremamente difícil de aplicar e fazer cumprir;
15. Realça a necessidade de aumentar o nível de proteção contra o *software* espião para os altos responsáveis políticos e funcionários europeus; chama a atenção para as ameaças decorrentes de uma eventual vigilância dos principais políticos e funcionários europeus por potências estrangeiras, especialmente durante a atual guerra de agressão russa contra a Ucrânia;
16. Salienta os grandes riscos associados à utilização de *software* espião por intervenientes não estatais; insta os Estados-Membros a acompanharem de perto o comércio de *software* espião e destaca que a assistência da Europol pode ser utilizada neste domínio, especialmente para a dimensão transfronteiriça desta questão;

17. Opõe-se firmemente, ao mesmo tempo, a qualquer tentativa de conferir à Europol o poder de agir sem o conhecimento e o consentimento dos Estados-Membros e, por conseguinte, de os ignorar; recorda que o papel da Europol deve consistir em prestar apoio em termos de coordenação;
18. Recomenda, em conclusão, que a Comissão adote uma abordagem muito cautelosa relativamente às recomendações da Comissão PEGA; salienta a necessidade de ter em conta o contexto político destas recomendações, a sua incompatibilidade parcial com os Tratados e a sua impraticabilidade parcial, tanto por razões jurídicas como políticas;
19. Encarrega a sua Presidente de transmitir a presente resolução ao Conselho, à Comissão e aos governos e parlamentos dos Estados-Membros.