



**A9-0022/2022**

8.2.2022

# RELATÓRIO

sobre a ingerência estrangeira em todos os processos democráticos na União Europeia, incluindo a desinformação  
(2020/2268(INI))

Comissão Especial sobre a Ingerência Estrangeira em Todos os Processos Democráticos na União Europeia, incluindo a Desinformação

Relatora: Sandra Kalniete

## ÍNDICE

|   | <b>Página</b> |
|---|---------------|
| PROPOSTA DE RESOLUÇÃO DO PARLAMENTO EUROPEU .....                                       | 3             |
| EXPOSIÇÃO DE MOTIVOS.....   | 59            |
| POSIÇÃO MINORITÁRIA DE CLARE DALY, EM NOME DO GRUPO THE LEFT.....                       | 68            |
| INFORMAÇÕES SOBRE A APROVAÇÃO NA COMISSÃO COMPETENTE QUANTO À<br>MATÉRIA DE FUNDO ..... | 69            |
| VOTAÇÃO NOMINAL.....  | 70            |

## PROPOSTA DE RESOLUÇÃO DO PARLAMENTO EUROPEU

### sobre a ingerência estrangeira em todos os processos democráticos na União Europeia, incluindo a desinformação (2020/2268(INI))

*O Parlamento Europeu,*

- Tendo em conta a Carta dos Direitos Fundamentais da União Europeia, nomeadamente os artigos 7.º, 8.º, 11.º, 12.º, 39.º, 40.º, 47.º e 52.º,
- Tendo em conta a Carta das Nações Unidas, nomeadamente os artigos 1.º e 2.º,
- Tendo em conta a Resolução 2131 (XX) da Assembleia Geral das Nações Unidas, de 21 de dezembro de 1965, intitulada «Declaração sobre a Inadmissibilidade da Intervenção nos Assuntos Internos dos Estados e a Proteção da sua Independência e Soberania»,
- Tendo em conta a Convenção para a Proteção dos Direitos Humanos e das Liberdades Fundamentais, nomeadamente os artigos 8.º, 9.º, 10.º, 11.º, 12.º, 13.º, 14.º, 16.º e 17.º, e o seu Protocolo, nomeadamente o artigo 3.º,
- Tendo em conta a sua resolução, de 23 de novembro de 2016, sobre a comunicação estratégica da UE para enfrentar a propaganda dirigida contra ela por terceiros<sup>1</sup> e a sua recomendação, de 13 de março de 2019, respeitante ao balanço do seguimento dado pelo SEAE dois anos após o relatório do PE sobre a comunicação estratégica da UE para enfrentar a propaganda dirigida contra ela por terceiros<sup>2</sup>,
- Tendo em conta a sua resolução, de 13 de junho de 2018, sobre ciberdefesa<sup>3</sup>,
- Tendo em conta a Comunicação Conjunta da Comissão e da Alta Representante da União para os Negócios Estrangeiros e a Política de Segurança, de 5 de dezembro de 2018, intitulada «Plano de Ação contra a Desinformação» (JOIN(2018)0036), e a Comunicação Conjunta da Comissão e da Alta Representante da União para os Negócios Estrangeiros e a Política de Segurança, de 14 de junho de 2019, intitulada «Relatório sobre a execução do Plano de Ação contra a Desinformação» (JOIN(2019)0012),
- Tendo em conta o documento de trabalho conjunto, de 23 de junho de 2021, referente ao quinto relatório intercalar sobre a aplicação do quadro comum de 2016 em matéria de luta contra as ameaças híbridas e da comunicação conjunta, de 2018, sobre aumentar a resiliência e reforçar a capacidade de enfrentar ameaças híbridas (SWD(2021)0729),
- Tendo em conta o Plano de Ação para a Democracia Europeia (COM(2020)0790),
- Tendo em conta a Comunicação da Comissão, de 3 de dezembro de 2020, intitulada «Os

---

<sup>1</sup> JO C 224 de 27.6.2018, p. 58.

<sup>2</sup> JO C 23 de 21.1.2021, p. 152.

<sup>3</sup> JO C 28 de 27.1.2020, p. 57.

meios de comunicação social da Europa na Década Digital: plano de ação para apoiar a recuperação e a transformação» (COM(2020)0784),

- Tendo em conta o pacote do ato legislativo sobre os serviços digitais,
- Tendo em conta a sua resolução, de 20 de outubro de 2021, sobre os meios de comunicação social da Europa na Década Digital: plano de ação para apoiar a recuperação e a transformação<sup>4</sup>,
- Tendo em conta o Código de Conduta sobre Desinformação, de 2018, e as Orientações de 2021 relativas ao reforço do Código de Conduta sobre Desinformação (COM(2021)0262), bem como as recomendações para o novo Código de Conduta sobre Desinformação emitidas pelo Grupo de Reguladores Europeus dos Serviços de Comunicação Social Audiovisual em outubro de 2021,
- Tendo em conta o Relatório Especial n.º 09/2021 do Tribunal de Contas Europeu, intitulado «Desinformação na UE: fenómeno combatido, mas não controlado»,
- Tendo em conta a proposta de diretiva do Parlamento Europeu e do Conselho relativa à resiliência das entidades críticas, apresentada pela Comissão em 16 de dezembro de 2020 (COM(2020)0829), e a proposta de anexo à diretiva,
- Tendo em conta o Regulamento (UE) 2019/452 do Parlamento Europeu e do Conselho, de 19 de março de 2019, que estabelece um regime de análise dos investimentos diretos estrangeiros na União<sup>5</sup> (Regulamento Análise dos IDE) e as Orientações de março de 2020 sobre o Regulamento Análise dos IDE (C(2020)1981),
- Tendo em conta a Comunicação Conjunta da Comissão e do Alto Representante da União para os Negócios Estrangeiros e a Política de Segurança, de 16 de dezembro de 2020, intitulada «Estratégia de cibersegurança da UE para a década digital» (JOIN(2020)0018),
- Tendo em conta os artigos da Comissão do Direito Internacional sobre a responsabilidade dos Estados por atos ilícitos a nível internacional,
- Tendo em conta a proposta de diretiva do Parlamento Europeu e do Conselho relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União e que revoga a Diretiva (UE) 2016/1148, apresentada pela Comissão em 16 de dezembro de 2020 (COM(2020)0823),
- Tendo em conta o conjunto de instrumentos da UE para a cibersegurança das redes 5G, de março de 2021,
- Tendo em conta o Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e

---

<sup>4</sup> Textos Aprovados, P9\_TA(2021)0428.

<sup>5</sup> JO L 79 I de 21.3.2019, p. 1.

comunicação e que revoga o Regulamento (UE) n.º 526/2013<sup>6</sup>,

- Tendo em conta os estudos, os *briefings* e as análises aprofundadas solicitadas pela Comissão Especial sobre a Ingerência Estrangeira em Todos os Processos Democráticos na União Europeia, incluindo a Desinformação (INGE),
  - Tendo em conta a audição de Frances Haugen, de 8 de novembro de 2021, organizada pela sua Comissão do Mercado Interno e da Proteção dos Consumidores, em associação com outras comissões,
  - Tendo em conta a sua resolução, de 7 de outubro de 2021, sobre o estado das capacidades de ciberdefesa da UE<sup>7</sup>,
  - Tendo em conta os Objetivos de Desenvolvimento Sustentável (ODS) das Nações Unidas, especialmente o ODS n.º 16, que visa promover sociedades pacíficas e inclusivas para o desenvolvimento sustentável,
  - Tendo em conta o discurso sobre o Estado da União de 2021 e a carta de intenções,
  - Tendo em conta o relatório do Secretário-Geral das Nações Unidas, de 10 de setembro de 2021, intitulado «A nossa agenda comum»,
  - Tendo em conta a Comunicação Conjunta da Comissão e do Alto Representante da União para os Negócios Estrangeiros e a Política de Segurança, de 10 de junho de 2020, intitulada «Combater a desinformação sobre a COVID-19: repor a verdade dos factos» (JOIN(2020)0008),
  - Tendo em conta a decisão do Conselho, de 15 de novembro de 2021, de alterar o seu regime de sanções contra a Bielorrússia, a fim de alargar os critérios de designação a pessoas e entidades que organizam ou contribuem para ataques híbridos e para a instrumentalização de seres humanos pelo regime bielorrusso,
  - Tendo em conta a sua decisão, de 18 de junho de 2020, sobre a constituição, as competências, a composição numérica e a duração do mandato da Comissão Especial sobre a Ingerência Estrangeira em Todos os Processos Democráticos na União Europeia, incluindo a Desinformação<sup>8</sup>, adotada nos termos do artigo 207.º do seu Regimento,
  - Tendo em conta o artigo 54.º do seu Regimento,
  - Tendo em conta o relatório da Comissão Especial sobre a Ingerência Estrangeira em Todos os Processos Democráticos na União Europeia, incluindo a Desinformação (A9-0022/2022),
- A. Considerando que a ingerência estrangeira constitui uma grave violação dos valores e princípios universais em que a União se funda, tais como a dignidade humana, a liberdade, a igualdade, a solidariedade, o respeito pelos direitos humanos e pelas

---

<sup>6</sup> JO L 151 de 7.6.2019, p. 15.

<sup>7</sup> Textos Aprovados, P9\_TA(2021)0412.

<sup>8</sup> JO C 362 de 8.9.2021, p. 186.

liberdades fundamentais, a democracia e o Estado de direito;

- B. Considerando que a ingerência estrangeira, a manipulação de informações e a desinformação constituem uma violação das liberdades fundamentais de expressão e de informação, tal como estabelecidas no artigo 11.º da Carta dos Direitos Fundamentais da União Europeia, e põem em perigo estas liberdades, para além de comprometerem os processos democráticos na UE e nos seus Estados-Membros, nomeadamente a realização de eleições livres e justas; que o objetivo da ingerência estrangeira é distorcer e representar falsamente os factos, inflacionar artificialmente argumentos unilaterais, desacreditar a informação para degradar o discurso político e, em última análise, minar a confiança no sistema eleitoral e, por conseguinte, no próprio processo democrático;
- C. Considerando que qualquer ação contra a manipulação da informação e a ingerência estrangeira deve, ela própria, respeitar as liberdades fundamentais de expressão e de informação; que a Agência dos Direitos Fundamentais da União Europeia (FRA) desempenha um papel fundamental na avaliação do respeito pelos direitos fundamentais, incluindo o artigo 11.º da Carta dos Direitos Fundamentais, a fim de evitar ações desproporcionadas; que os intervenientes que levam a cabo campanhas de ingerência estrangeira e de manipulação da informação abusam dessas liberdades em seu benefício e que, por conseguinte, é fundamental intensificar a luta preventiva contra a ingerência estrangeira e a manipulação da informação, uma vez que a democracia depende da tomada de decisões informadas por parte das pessoas;
- D. Considerando que existem provas de que intervenientes estatais e não estatais estrangeiros mal-intencionados e autoritários, como a Rússia e a China, entre outros, utilizam a manipulação da informação e outras táticas de ingerência para interferir nos processos democráticos da UE; que estes ataques, que fazem parte de uma estratégia de guerra híbrida e constituem uma violação do direito internacional, induzem em erro e enganam os cidadãos e afetam o seu comportamento eleitoral, amplificam os debates fraturantes, dividem, polarizam e exploram as vulnerabilidades das sociedades, promovem o discurso de ódio, agravam a situação dos grupos vulneráveis, que são mais suscetíveis de se tornar vítimas da desinformação, deturpam a integridade das eleições e dos referendos democráticos, alimentam a desconfiança nos governos nacionais, nas autoridades públicas e na ordem democrática liberal e têm por objetivo desestabilizar a democracia europeia e, por conseguinte, constituem uma grave ameaça para a segurança e a soberania da UE;
- E. Considerando que a ingerência estrangeira representa um padrão de comportamento que ameaça, ou afeta negativamente, os valores, os processos democráticos, os processos políticos, a segurança dos Estados e dos cidadãos e a capacidade para fazer face a situações excecionais; que essa ingerência tem um caráter manipulador e é levada a cabo e financiada de forma intencional e coordenada; que os responsáveis por essa ingerência, incluindo os seus intermediários dentro e fora do seu próprio território, podem ser intervenientes estatais ou não estatais e são frequentemente assistidos nas suas atividades de ingerência estrangeira por cúmplices políticos nos Estados-Membros que retiram vantagens políticas e económicas do favorecimento de estratégias estrangeiras; que o recurso, por parte de intervenientes estrangeiros, a intermediários nacionais e a sua cooperação com aliados nacionais dilui a fronteira entre a ingerência externa e interna;

- F. Considerando que as táticas de ingerência estrangeira assumem diversas formas, incluindo desinformação, supressão de informação, manipulação de plataformas de redes sociais e dos seus algoritmos, condições e sistemas publicitários, ciberataques, operações de pirataria e divulgação para aceder às informações dos eleitores e interferir na legitimidade do processo eleitoral, ameaças e assédio contra jornalistas, investigadores, políticos e membros de organizações da sociedade civil, donativos e empréstimos encobertos a partidos políticos, a campanhas que favorecem candidatos específicos, a organizações e a meios de comunicação social, organizações e meios de comunicação social falsos ou que defendem determinados interesses, captação e cooptação de elites, dinheiro sujo, identidades falsas, pressão no sentido de «autocensura», exploração abusiva de narrativas históricas, religiosas ou culturais, pressão sobre estabelecimentos de ensino e instituições culturais, controlo sobre infraestruturas essenciais e exercício de pressão sobre nacionais estrangeiros residentes na UE, instrumentalização de migrantes e espionagem; que estas táticas são frequentemente combinadas entre si para produzir maior impacto;
- G. Considerando que a manipulação de informações e a propagação da desinformação podem servir os interesses económicos dos intervenientes estatais e não estatais e dos seus intermediários e criar dependências económicas que podem ser exploradas para fins políticos; que, num mundo de competitividade internacional não cinética, a ingerência estrangeira pode ser um instrumento privilegiado para desestabilizar e enfraquecer os seus homólogos visados, ou para reforçar a sua própria vantagem competitiva através da criação de canais de influência, dependências da cadeia de abastecimento, chantagem ou coerção; que a desinformação está a causar danos económicos diretos e indiretos que não têm sido sistematicamente avaliados;
- H. Considerando que as informações erradas são comprovadamente informações falsas que não se destinam a causar danos, ao passo que a desinformação consiste em informações falsas ou enganadoras que são comprovadamente produzidas, apresentadas ou divulgadas de modo intencional para causar danos, provocar um efeito potencialmente perturbador na sociedade, enganando o público, ou para obter benefícios económicos de forma intencional;
- I. Considerando que é necessário chegar a acordo sobre definições e metodologias comuns e granulares na UE para melhorar a compreensão comum das ameaças e desenvolver normas adequadas da UE para uma melhor imputação e resposta; que o Serviço Europeu para a Ação Externa (SEAE) realizou um trabalho considerável neste domínio; que tais definições devem oferecer proteção contra a ingerência estrangeira e garantir o respeito pelos direitos humanos; que é da maior importância promover a cooperação com parceiros que partilham as mesmas ideias, nas instâncias internacionais competentes, relativamente a definições comuns em matéria de ingerência estrangeira, a fim de estabelecer normas e padrões internacionais; que a UE deve assumir a liderança no que respeita ao estabelecimento de regras internacionais claras para a imputação de ingerência estrangeira;

### ***Necessidade de uma estratégia coordenada contra a ingerência estrangeira***

- J. Considerando que as tentativas de ingerência estrangeira em todo o mundo estão a aumentar em número e grau de sofisticação e a tornar-se mais sistémicas, com base na

utilização generalizada da inteligência artificial (IA) e na erosão da imputabilidade;

- K. Considerando que cabe à UE e aos seus Estados-Membros defender todos os cidadãos e infraestruturas, bem como os seus sistemas democráticos, contra tentativas de ingerência estrangeira; que, no entanto, a UE e os seus Estados-Membros parecem não dispor de meios adequados e suficientes para prevenir, detetar, imputar, combater e sancionar melhor estas ameaças;
- L. Considerando a falta generalizada de sensibilização de muitos decisores políticos e cidadãos em geral para a realidade destas questões, que pode contribuir involuntariamente para criar novas vulnerabilidades; que a questão das campanhas de desinformação não esteve no topo da agenda dos decisores políticos europeus; que as audições e o trabalho da Comissão Especial INGE contribuíram para o reconhecimento público e a contextualização destas questões, tendo enquadrado com êxito o debate europeu sobre a ingerência estrangeira; que os esforços duradouros de desinformação estrangeira já contribuíram para o surgimento de ingerência de origem interna;
- M. Considerando que um controlo transparente em tempo real do estado de ingerência estrangeira por organismos institucionais e analistas e verificadores de factos independentes, a coordenação eficaz das suas ações e o intercâmbio de informações são cruciais para a tomada de medidas adequadas, não só no intuito de facultar informações sobre os ataques mal-intencionados em curso como também para os combater; que deve igualmente dar-se atenção ao chamado «levantamento da sociedade», identificando os domínios mais vulneráveis e suscetíveis à manipulação estrangeira e à desinformação, e enfrentando as causas dessas vulnerabilidades;
- N. Considerando que a principal prioridade da defesa da UE, ou seja, a resiliência e a preparação dos cidadãos da UE face à ingerência estrangeira e à manipulação da informação, exige uma abordagem de longo prazo que mobilize a sociedade no seu conjunto, começando pelo nível de ensino e aumentando a sensibilização para os problemas numa fase inicial;
- O. Considerando que é necessário cooperar e coordenar os diferentes níveis administrativos e setores entre os Estados-Membros, a nível da UE e com parceiros que partilham as mesmas ideias, bem como com a sociedade civil e o setor privado, para identificar vulnerabilidades, detetar ataques e neutralizá-los; que é urgente fazer corresponder as medidas de segurança nacional à perceção das ameaças;

***Reforçar a resiliência através do conhecimento situacional, da literacia mediática e informacional, do pluralismo dos meios de comunicação social, do jornalismo independente e da educação***

- P. Considerando que o conhecimento da situação, sistemas democráticos sólidos, um Estado de direito forte, uma sociedade civil dinâmica e instrumentos de alerta precoce e de avaliação de ameaças constituem os primeiros passos para combater a manipulação da informação e a ingerência; que, apesar de todos os progressos realizados em matéria de sensibilização para a ingerência estrangeira, muitas pessoas – nomeadamente os decisores políticos e funcionários públicos que trabalham nos domínios potencialmente visados – ainda não estão cientes dos riscos potenciais associados à ingerência estrangeira nem sabem como os abordar;



- Q. Considerando que os meios de informação independentes de elevada qualidade e caracterizados por um financiamento sustentável e transparente e um jornalismo profissional são essenciais para garantir a liberdade, o pluralismo da comunicação social e o Estado de direito e que, por conseguinte, são um pilar da democracia e o melhor antídoto contra a desinformação; que alguns intervenientes estrangeiros tiram partido da liberdade dos meios de comunicação social ocidentais para disseminar a desinformação; que os meios de comunicação social profissionais e o jornalismo tradicional, enquanto fonte de informação de qualidade, enfrentam tempos difíceis na era digital; que a educação e a formação para um jornalismo de qualidade, dentro e fora da UE, são necessárias para garantir análises jornalísticas de valor e elevados padrões editoriais; que a UE deve continuar a apoiar o jornalismo no contexto digital; que a comunicação baseada em dados científicos deve desempenhar um papel importante;
- R. Considerando que os meios de comunicação social de serviço público com independência editorial são essenciais e insubstituíveis na prestação de serviços de informação de elevada qualidade e imparciais ao público em geral e que devem ser protegidos contra a captação maligna e reforçados enquanto pilar fundamental da luta contra a desinformação;
- S. Considerando que, na análise da ingerência estrangeira, as diferentes partes interessadas e instituições recorrem a metodologias e definições divergentes, todas elas apresentando graus de inteligibilidade diferentes, e que essas diferenças podem obstar à comparabilidade do acompanhamento, da análise e da avaliação do nível de ameaça, o que dificulta a ação conjunta; que são necessárias uma definição e uma metodologia da UE para melhorar a análise comum das ameaças;
- T. Considerando que, para abordar adequadamente o problema, é necessário que a terminologia centrada nos conteúdos, como as notícias falsas ou enganosas, as informações erradas e a desinformação, seja complementada por terminologia centrada no comportamento; que esta terminologia deve ser harmonizada e cuidadosamente utilizada;
- U. Considerando que a formação em literacia mediática e digital e a sensibilização, tanto de crianças como de adultos, constituem ferramentas importantes para tornar os cidadãos mais resilientes às tentativas de ingerência no espaço de informação e para evitar a manipulação e a polarização; que, em geral, as sociedades com um elevado nível de literacia mediática são mais resilientes à ingerência estrangeira; que os métodos de trabalho jornalísticos, como o jornalismo construtivo, podem contribuir para reforçar a confiança dos cidadãos no jornalismo;
- V. Considerando que a manipulação da informação pode assumir muitas formas, como a propagação de desinformação e de notícias completamente falsas, a distorção de factos, de narrativas e de representações de opinião, a supressão de determinadas informações ou opiniões, a informação tirada do seu contexto, a manipulação dos sentimentos das pessoas, a promoção do discurso de ódio, a promoção de algumas opiniões à custa de terceiros e o assédio contra pessoas no intuito de as silenciar e oprimir; que um dos objetivos da manipulação da informação é criar caos, a fim de incentivar a perda de confiança dos cidadãos nos antigos e novos «guardiães» em matéria de informação; que a linha que separa a liberdade de expressão e a promoção do discurso de ódio e da

desinformação é bastante ténue e que a liberdade de expressão não deve ser utilizada de forma abusiva;

- W. Considerando que o Azerbaijão, a China, a Turquia e a Rússia, entre outros, visaram especificamente jornalistas e opositores radicados na União Europeia, como o atestam os casos do bloguista e opositor azerbaijano Mahammad Mirzali, em Nantes, e do jornalista turco Erk Acarer, em Berlim;
- X. Considerando que existem provas concretas de que os processos democráticos da UE estão a ser visados e afetados por campanhas de desinformação que põem em causa os ideais democráticos e os direitos fundamentais; que a desinformação relacionada com temas como, por exemplo, o género, as pessoas LGBTIQ+, a saúde e os direitos sexuais e reprodutivos e as minorias é uma forma de desinformação que ameaça os direitos humanos, compromete os direitos digitais e políticos, bem como a segurança dos seus alvos, e semeia a discórdia e a falta de união entre os Estados-Membros; que, durante as campanhas eleitorais, os candidatos do sexo feminino tendem a ser desproporcionalmente visados por narrativas sexistas, o que desencoraja as mulheres de participarem nos processos democráticos; que os responsáveis por estas campanhas de desinformação sob o pretexto da promoção de valores «tradicionais» ou «conservadores», formam alianças estratégicas com parceiros locais para obter acesso a informações locais, e, segundo consta, recebem milhões de euros em financiamento estrangeiro;
- Y. Considerando que, além das instituições estatais, dos jornalistas, dos líderes de opinião e do setor privado, todo e qualquer setor da sociedade e indivíduo tem um papel importante a desempenhar para identificar e travar a propagação da desinformação e alertar as pessoas que, no seu meio, se encontrem em risco; que a sociedade civil, o meio académico e os jornalistas já contribuíram em grande medida para aumentar a sensibilização do público e a resiliência societal, nomeadamente em cooperação com os homólogos de países parceiros;
- Z. Considerando que as organizações da sociedade civil que representam as vozes das minorias e as organizações de defesa dos direitos humanos em toda a Europa continuam a ser subfinanciadas, apesar de desempenharem um papel crucial na sensibilização e no combate à desinformação; que as organizações da sociedade civil devem dispor de recursos adequados para desempenharem o seu papel na limitação do impacto da ingerência estrangeira;
- AA. Considerando que é importante beneficiar de um acesso fácil e oportuno a informações baseadas em factos e provenientes de fontes fidedignas quando a desinformação começa a propagar-se;
- AB. Considerando que é necessário detetar rapidamente os ataques de ingerência estrangeira e as tentativas de manipulação da informação, a fim de os combater; que a análise de informações da UE e o conhecimento da situação dependem da vontade dos Estados-Membros de partilhar informações; que a Presidente da Comissão propôs que se considere a criação de um centro comum de conhecimento da situação da UE; que a prevenção e medidas proativas, incluindo a desmistificação prévia e um ecossistema de informações são, demonstram ser muito mais eficazes do que os esforços subsequentes

de verificação de factos e de desmistificação, que revelam ter um alcance inferior ao da desinformação original; que a UE e os seus Estados-Membros não dispõem atualmente de capacidades suficientes para adotar tais medidas; que os novos instrumentos analíticos baseados em IA, como o Debunk.eu lituano, podem ajudar a detetar ataques, partilhar conhecimentos e informar o público;

- AC. Considerando que a desinformação prospera num ambiente de narrativas fracas ou fragmentadas a nível nacional ou da UE e em debates polarizados e emocionais, explorando pontos fracos e preconceitos existentes na sociedade e entre indivíduos; que a desinformação distorce o debate público em torno de eleições e de outros processos democráticos e pode dar azo a que os cidadãos tenham dificuldade em fazer escolhas informadas;

### ***Ingerência estrangeira através da utilização de plataformas em linha***

- AD. Considerando que as plataformas em linha são suscetíveis de constituir instrumentos facilmente acessíveis e a preços aceitáveis para quem manipula informação ou interfere de outra forma, nomeadamente através do ódio e do assédio, dos danos causados ao bom estado e à segurança das nossas comunidades em linha, do silenciamento de opositores, da espionagem ou da propagação da desinformação; que o seu funcionamento demonstrou incentivar opiniões polarizadas e extremas em detrimento de informações baseadas em factos; que as plataformas têm os seus próprios interesses e podem não ser neutras no que respeita ao tratamento da informação; que algumas plataformas em linha beneficiam em grande medida do sistema que amplifica a divisão, o extremismo e a polarização; que o espaço em linha se tornou tão importante para a nossa democracia como o espaço físico, pelo que necessita de regras correspondentes;
- AE. Considerando que as plataformas aceleraram e exacerbaram a propagação de informações erradas e desinformação de forma inédita e desafiante; que as plataformas em linha controlam o fluxo de informação e de publicidade em linha, concebem e utilizam algoritmos para controlar estes fluxos e que as plataformas não são transparentes, não dispõem de procedimentos apropriados para verificar a identidade dos seus utilizadores, utilizam terminologia pouco clara e vaga e que é escassa ou nula a informação partilhada pelas plataformas no que diz respeito à conceção, utilização e impacto dos algoritmos em causa; que a componente viciante dos algoritmos das plataformas em linha criou um grave problema de saúde pública que tem de ser resolvido; que as plataformas em linha devem ser responsáveis pelos efeitos nocivos dos seus serviços, uma vez que algumas plataformas estavam cientes das falhas dos seus algoritmos – em particular o seu papel na difusão de conteúdos divisivos – mas não as abordaram, a fim de maximizar os lucros, como revelado por autores de denúncias;
- AF. Considerando que existem campanhas de ingerência e de manipulação da informação que visam todas as medidas contra a propagação da COVID-19, nomeadamente a vacinação na UE, e que as plataformas em linha não coordenaram esforços para limitar estas campanhas e podem inclusivamente ter contribuído para a sua propagação; que essa desinformação pode ser fatal, ao dissuadir as pessoas de se vacinarem ou ao promover tratamentos falsos; que a pandemia exacerbou a luta sistémica entre a democracia e o autoritarismo, incitando os intervenientes estatais e não estatais autoritários, como a China e a Rússia, a aplicarem uma vasta gama de instrumentos explícitos e encobertos na sua tentativa de desestabilizar os seus homólogos

democráticos; que os «Facebook Papers» revelaram a incapacidade da plataforma para combater a desinformação relacionada com as vacinas, nomeadamente em língua inglesa; que a situação é ainda pior no caso da desinformação relacionada com as vacinas noutras línguas; que esta questão diz respeito a todas as plataformas;

- AG. Considerando que numerosos vendedores registados na UE vendem menções de «gosto», seguidores, comentários e partilhas inautênticos a todo e qualquer interveniente que pretenda aumentar artificialmente a sua visibilidade em linha; que é impossível identificar casos em que esses serviços são utilizados para fins legítimos, ao passo que as utilizações nocivas incluem a manipulação de eleições e de outros processos democráticos, o fomento de burlas, a publicação de críticas negativas dos produtos dos concorrentes, a defraudação de anunciantes e a criação de um público falso que é utilizado para moldar a conversa, fazer ataques pessoais e sobrevalorizar artificialmente determinados pontos de vista que, de outro modo, não seriam tidos em conta; que os regimes estrangeiros, como a Rússia e a China, utilizam estas ferramentas em linha em larga escala para influenciar o debate público nos países europeus; que a desinformação pode desestabilizar a democracia europeia;
- AH. Considerando que as plataformas sociais, os dispositivos digitais e as aplicações recolhem e armazenam enormes quantidades de dados pessoais muito pormenorizados e, amiúde, sensíveis, sobre cada utilizador; que esses dados podem ser utilizados para prever tendências comportamentais, reforçar o preconceito cognitivo e orientar a tomada de decisões; que esses dados são explorados para fins comerciais; que fugas de dados ocorrem repetidamente, em detrimento da segurança das vítimas dessas fugas, e que os dados podem ser vendidos no mercado negro; que as bases de dados podem constituir minas de ouro para intervenientes mal-intencionados que têm na mira grupos ou pessoas individuais;
- AI. Considerando que, em geral, as plataformas são concebidas para garantir que a escolha da opção de não partilhar dados seja pouco intuitiva, complexa e morosa em comparação com a escolha da opção de partilhar dados;
- AJ. Considerando que as plataformas em linha se inserem na maioria dos aspetos que caracterizam as nossas vidas e que a disseminação de informação nas plataformas pode ter um enorme impacto no nosso pensamento e comportamento, por exemplo, quando estão em causa preferências e comportamentos de voto, escolhas económicas e sociais, bem como a escolha das fontes de informação, e que estas escolhas decisivas de importância pública são atualmente, de facto, condicionadas pelos interesses comerciais de empresas privadas;
- AK. Considerando que os mecanismos de curadoria de algoritmos e outras componentes das plataformas de redes sociais são concebidos para maximizar o índice de participação; que tem sido repetidamente relatado que estas componentes fomentam a polarização e a radicalização dos conteúdos, promovem conteúdos discriminatórios e mantêm os utilizadores em comunidades que partilham as mesmas ideias; que tal leva à radicalização gradual dos utilizadores das plataformas, bem como ao condicionamento e à poluição dos processos de debate coletivo, e não à proteção dos processos democráticos e dos indivíduos; que as ações descoordenadas das plataformas conduziram a discrepâncias nas suas ações e permitiram a propagação da desinformação

entre plataformas; que o modelo de negócio que consiste em fazer dinheiro através da disseminação de informações polarizadas e da conceção de algoritmos torna as plataformas um alvo fácil para a manipulação por parte de intervenientes hostis estrangeiros; que as plataformas de redes sociais podem ser concebidas de forma diferente, de modo a promover uma esfera pública em linha mais saudável;

- AL. Considerando que a criação de materiais áudio e audiovisuais falsificados está a tornar-se cada vez mais fácil com o aparecimento de tecnologias acessíveis e de fácil utilização, e que a propagação desses materiais é um problema que está a aumentar exponencialmente; que, no entanto, atualmente, 90 % da investigação se destina ao desenvolvimento de falsificações e apenas 10 % à sua deteção;
- AM. Considerando que os sistemas de autorregulação, como o Código de Conduta sobre Desinformação de 2018, conduziram a melhorias; que, no entanto, depender da boa vontade das plataformas não é viável nem eficaz e produziu poucos dados significativos sobre o seu impacto global; que, além disso, as plataformas tomaram medidas individuais de grau e efeito variáveis, o que levou a «portas traseiras» através das quais os conteúdos podem continuar a espalhar-se por outras partes do mundo, apesar da sua remoção; que é necessário estabelecer um conjunto claro de regras e sanções para que o Código de Conduta produza efeitos suficientes no ambiente em linha;
- AN. Considerando que o Plano de Ação para a Democracia Europeia visa reforçar o Código de Conduta de 2018 e, em conjunto com o Regulamento Serviços Digitais, representa um afastamento em relação à abordagem de autorregulação e visa introduzir mais garantias e proteções para os utilizadores, aumentando a autonomia e ultrapassando a passividade no que respeita aos serviços oferecidos, bem como introduzindo medidas que exijam uma maior transparência e prestação de contas por parte das empresas e introduzindo mais obrigações para as plataformas;
- AO. Considerando que as atuais ações contra as campanhas de desinformação nas plataformas em linha não são eficazes nem dissuasivas e permitam que estas continuem a promover conteúdos discriminatórios e mal-intencionados;
- AP. Considerando que as plataformas dedicam consideravelmente menos recursos à gestão de conteúdos em línguas menos faladas, em comparação com os conteúdos em língua inglesa, e até mesmo aos conteúdos em línguas mais faladas do que o inglês;
- AQ. Considerando que os procedimentos de apresentação de queixa e de recurso das plataformas são geralmente inadequados;
- AR. Considerando que, nos últimos meses, vários intervenientes de grande envergadura acataram as regras de censura, por exemplo, durante as eleições legislativas russas de setembro de 2021, ocasião em que a Google e a Apple retiraram as aplicações de «votação inteligente» das suas lojas na Rússia;
- AS. Considerando que a falta de transparência quanto às escolhas algorítmicas efetuadas pelas plataformas torna, além disso, impossível confirmar as alegações das plataformas sobre o que fazem e o efeito das suas ações para combater a manipulação da informação e a ingerência; que existem discrepâncias entre o efeito declarado dos seus esforços nas autoavaliações anuais e a sua eficácia real, como demonstrado nos recentes «Facebook

Papers»;

- AT. Considerando que a natureza não transparente da publicidade direcionada conduz a quantidades maciças de publicidade em linha de marcas de renome, por vezes, até de instituições públicas, que acabam em sítios Web que incentivam o terrorismo, contêm discursos de ódio e desinformação, e financiam o crescimento desses sítios Web, sem o conhecimento ou o consentimento dos anunciantes;
- AU. Considerando que o mercado da publicidade em linha é controlado por um pequeno número de grandes empresas tecnológicas de anúncios que partilham o mercado entre si, sendo a Google e o Facebook os maiores operadores; que esta elevada concentração do mercado em algumas empresas está associada a um forte desequilíbrio de poder; que a existência de meios de comunicação social diversificados é ameaçada pela utilização de técnicas de caça-cliques e pelo poder deste número reduzido de intervenientes para determinar que conteúdos são monetizados e que conteúdos não o são, ainda que os algoritmos que utilizam não consigam distinguir a desinformação dos conteúdos noticiosos normais; que o mercado da publicidade direcionada é em grande medida pouco transparente; que as empresas tecnológicas de anúncios forcem as marcas a arcar com as culpas pela sua negligência na monitorização da colocação de anúncios;

### ***Infraestruturas críticas e setores estratégicos***

- AV. Considerando que a gestão das ameaças às infraestruturas críticas, mormente quando fazem parte de uma estratégia híbrida sincronizada e mal-intencionada, exige esforços coordenados e conjuntos entre todos os setores, a diferentes níveis – da UE, nacional, regional e local – e em vários momentos;
- AW. Considerando que a Comissão apresentou uma proposta de uma nova diretiva para reforçar a resiliência das entidades críticas que prestam serviços essenciais na UE que inclui uma lista proposta de diferentes tipos de infraestruturas críticas; que a lista dos serviços será integrada no anexo da diretiva;
- AX. Considerando que a crescente globalização da divisão do trabalho e das cadeias de produção deu origem a lacunas em matéria de fabrico e de competências em setores-chave em toda a União; que tal criou uma elevada dependência da UE das importações de muitos produtos essenciais e ativos primários provenientes do estrangeiro, que podem ter vulnerabilidades intrínsecas; que a resiliência da cadeia de abastecimento deve figurar entre as prioridades dos decisores da UE;
- AY. Considerando que os investimentos diretos estrangeiros (IDE) – de países terceiros e empresas estrangeiras – em setores estratégicos da UE, mas também em zonas vizinhas, como os Balcãs Ocidentais, em particular a aquisição de estruturas críticas pela China, têm sido motivo de preocupação crescente nos últimos anos, tendo em conta a importância cada vez maior da correlação entre comércio e segurança; que estes investimentos representam um risco de criação de dependências económicas e de perda de conhecimentos em setores industriais e de produção essenciais;
- AZ. Considerando que a autonomia estratégica aberta da UE exige o controlo das infraestruturas estratégicas europeias; que a Comissão e os Estados-Membros manifestaram uma preocupação crescente com a segurança e o controlo das tecnologias

e infraestruturas na Europa;

### ***Ingerência estrangeira durante processos eleitorais***

- BA. Considerando que os intervenientes mal-intencionados que procuram interferir nos processos eleitorais tiram partido da abertura e do pluralismo das nossas sociedades como uma vulnerabilidade estratégica para atacar os processos democráticos e a resiliência da UE e dos seus Estados-Membros; que é no contexto dos processos eleitorais que a ingerência estrangeira se torna mais perigosa, à medida que os cidadãos voltam a mostrar interesse e estão mais envolvidos na participação política convencional;
- BB. Considerando que a natureza distinta da ingerência estrangeira nos processos eleitorais e a utilização de novas tecnologias neste contexto, bem como os seus efeitos potenciais, representam ameaças particularmente perigosas para a democracia; que a ingerência estrangeira nos processos eleitorais vai muito além da «guerra de informação» nas redes sociais, favorecendo candidatos específicos para piratear e visar bases de dados e obter acesso à informação dos eleitores inscritos, interferindo diretamente no funcionamento normal, na competitividade e na legitimidade do processo eleitoral; que a ingerência estrangeira visa criar dúvidas, incerteza e desconfiança e não só alterar o resultado das eleições, mas também deslegitimar todo o processo eleitoral;

### ***Financiamento encoberto de atividades políticas por intervenientes e doadores estrangeiros***

- BC. Considerando que um conjunto sólido de elementos de prova demonstra que os intervenientes estrangeiros têm interferido ativamente no funcionamento democrático da UE e dos seus Estados-Membros, nomeadamente durante os períodos eleitorais e em que decorrem referendos, através de operações de financiamento encobertas;
- BD. Considerando que, por exemplo, a Rússia, a China e outros regimes autoritários injetaram mais de 300 milhões de dólares em 33 países para interferir nos processos democráticos, e que outros países, como o Irão e a Venezuela, e intervenientes do Médio Oriente e da extrema-direita dos EUA também estiveram envolvidos em atividades de financiamento encoberto; que esta tendência está claramente a aumentar exponencialmente; que metade dos casos em que tal ocorreu diz respeito a ações levadas a cabo pela Rússia na Europa; que a corrupção e o branqueamento de capitais ilícitos são uma fonte de financiamento político de países terceiros autoritários;
- BE. Considerando que os instrumentos de comunicação social criados por doadores estrangeiros de forma não transparente se tornaram altamente eficazes, atraindo um grande número de seguidores e incentivando a participação;
- BF. Considerando que as operações em causa financiam partidos extremistas, populistas e antieuropeus e determinados partidos e indivíduos ou movimentos que procuram agravar a fragmentação societal e minar a legitimidade das autoridades públicas europeias e nacionais; que tal contribuiu para aumentar o alcance destes partidos e movimentos;
- BG. Considerando que a Rússia procura estabelecer contacto com partidos, indivíduos e movimentos, a fim de utilizar o pessoal das instituições da UE para legitimar posições

russas e governos por procuração, exercer pressão no sentido do levantamento de sanções e mitigar as consequências do isolamento internacional; que partidos como o *Freiheitliche Partei Österreichs* austríaco, o *Rassemblement National* francês e o *Legha Nord* italiano assinaram acordos de cooperação com o Rússia Unida, o partido de Vladimir Putin, e são atualmente acusados pelos meios de comunicação social de estar dispostos a aceitar financiamento político da Rússia; que outros partidos europeus, como o *Alternative für Deutschland* (AfD) alemão, o *Fidesz* e o *Jobbik* húngaros, e o partido Brexit do Reino Unido, também mantêm alegadamente um contacto estreito com o Kremlin e que, além disso, o AfD e o *Jobbik* foram «observadores eleitorais» nas eleições controladas pelo Kremlin, por exemplo, em Donetsk e Lugansk, na Ucrânia Oriental, para acompanhar e legitimar as eleições patrocinadas pela Rússia; que os contactos estreitos e regulares entre funcionários russos e representantes de um grupo de separatistas catalães em Espanha, bem como entre funcionários russos e o maior doador privado da campanha «Brexit Vote Leave», devem ser objeto de uma investigação aprofundada, tendo em conta que fazem parte da estratégia mais ampla da Rússia de aproveitar todas as oportunidades para manipular a retórica, a fim de promover a desestabilização;

- BH. Considerando que o Grupo de Estados contra a Corrupção (GRECO) do Conselho da Europa e a Comissão de Veneza já formularam recomendações abrangentes para reduzir a possibilidade de ingerência de intervenientes estrangeiros através do financiamento político;
- BI. Considerando que as leis eleitorais, em particular as disposições relativas ao financiamento de atividades políticas, não estão suficientemente bem coordenadas a nível da UE e que, por conseguinte, permitem que intervenientes estrangeiros recorram a métodos de financiamento opacos; que a definição jurídica de donativos políticos é demasiado restrita, permitindo que haja contribuições em espécie estrangeiras na União Europeia;
- BJ. Considerando que, em alguns Estados-Membros, a publicidade política em linha não está sujeita às regras aplicáveis à publicidade política fora de linha; que existe uma grave falta de transparência na publicidade política em linha, o que impossibilita os reguladores de aplicar limites de despesa e impedir fontes de financiamento ilegais, com consequências potencialmente desastrosas para a integridade dos nossos sistemas eleitorais;
- BK. Considerando que a falta de transparência do financiamento cria um ambiente propício à corrupção, que acompanha frequentemente o financiamento e os investimentos estrangeiros;
- BL. Considerando que o Regulamento (UE, Euratom) n.º 1141/2014 do Parlamento Europeu e do Conselho, de 22 de outubro de 2014, relativo ao estatuto e ao financiamento dos partidos políticos europeus e das fundações políticas europeias<sup>9</sup> está a ser revisto com vista a alcançar um maior nível de transparência em termos de financiamento das atividades políticas;
- BM. Considerando que o papel das fundações políticas tem vindo a crescer nos últimos anos,

---

<sup>9</sup> JO L 317 de 4.11.2014, p. 1.



na maioria dos casos, desempenhando um papel positivo na política e no reforço da democracia, mas, em alguns casos, tornando-se um veículo mais imprevisível para formas de financiamento mal-intencionadas e de ingerência indireta;

BN. Considerando que as tecnologias modernas e os ativos digitais, como as criptomoedas, são utilizados para encobrir transações financeiras ilegais para intervenientes políticos e partidos políticos;

### ***Cibersegurança e resiliência contra ciberataques***

BO. Considerando que a ocorrência de ciberataques e de incidentes com recurso a meios informáticos liderados por intervenientes estatais e não estatais hostis tem vindo a aumentar nos últimos anos; que múltiplos ciberataques, como as campanhas mundiais de ciberescagem personalizada por correio eletrónico dirigidas às estruturas estratégicas de armazenamento de vacinas e os ciberataques contra a Agência Europeia de Medicamentos (EMA), a Autoridade Bancária Europeia, o Parlamento norueguês e muitos outros, apontaram para grupos de piratas informáticos apoiados pelo Estado, predominantemente associados aos governos russo e chinês;

BP. Considerando que a União Europeia está empenhada em aplicar no ciberespaço o direito internacional em vigor, em particular a Carta das Nações Unidas; que intervenientes estrangeiros mal-intencionados estão a explorar a ausência de um quadro jurídico internacional sólido no ciberespaço;

BQ. Considerando que os Estados-Membros reforçaram a sua cooperação no domínio da ciberdefesa no âmbito da cooperação estruturada permanente (CEP), inclusive através da constituição de equipas de resposta rápida a ciberataques; que o Programa Europeu de Desenvolvimento Industrial no domínio da Defesa (PEDID) incluía informações, comunicações seguras e ciberdefesa nos seus programas de trabalho; que a atual capacidade para fazer face a ciberameaças é limitada devido à escassez de recursos humanos e financeiros, por exemplo, em estruturas críticas como os hospitais; que a UE se comprometeu a investir 1,6 mil milhões de euros, a título do Programa Europa Digital<sup>10</sup>, na capacidade de resposta e no desenvolvimento de instrumentos de cibersegurança para as administrações públicas, as empresas e os particulares, bem como a desenvolver a cooperação público-privada;

BR. Considerando que as lacunas e a fragmentação a nível das capacidades e estratégias da UE no ciberespaço estão a tornar-se um problema cada vez maior, tal como salientado pelo Tribunal de Contas Europeu<sup>11</sup>; que o conjunto de instrumentos de ciberdiplomacia da UE, criado em maio de 2019, demonstrou o valor acrescentado de uma resposta diplomática conjunta da UE às ciberatividades mal-intencionadas; que, em 30 de julho de 2020, o Conselho decidiu, pela primeira vez, impor medidas restritivas contra pessoas, entidades e organismos responsáveis por diversos ciberataques ou neles envolvidos;

BS. Considerando que intervenientes estatais estrangeiros têm recorrido a programas de vigilância em grande escala e ilícitos, como o Pegasus, para perseguir jornalistas,

<sup>10</sup> <https://www.consilium.europa.eu/pt/policies/cybersecurity/>

<sup>11</sup>

[https://www.eca.europa.eu/Lists/ECADocuments/BRP\\_CYBERSECURITY/BRP\\_CYBERSECURITY\\_PT.pdf](https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_PT.pdf)

ativistas dos direitos humanos, académicos, funcionários públicos e políticos, nomeadamente chefes de Estado europeus; que alguns Estados-Membros também recorreram ao *software* espião de vigilância;

### ***Proteção dos Estados-Membros, instituições, agências, delegações e missões da UE***

- BT. Considerando que o carácter descentralizado e multinacional das instituições da UE, incluindo as suas missões e operações, é um alvo cada vez maior e é explorado por intervenientes estrangeiros mal-intencionados que pretendem semear a discórdia na UE; que, em geral, não existe uma cultura de segurança nas instituições da UE, apesar do facto de serem alvos evidentes; que o Parlamento, enquanto instituição democraticamente eleita da UE, enfrenta desafios específicos; que vários casos revelaram que as instituições da UE parecem vulneráveis à infiltração estrangeira; que deve ser garantida a segurança do pessoal da UE;
- BU. Considerando que é necessário adotar, com carácter prioritário, procedimentos de gestão de crises sólidos e coerentes; que deve ser oferecida formação adicional, a fim de melhorar o grau de preparação do pessoal;
- BV. Considerando que os ciberataques visaram recentemente várias instituições da UE, o que sublinha a necessidade de uma forte cooperação interinstitucional em termos de deteção, monitorização e partilha de informações durante os ciberataques e/ou com vista a preveni-los, inclusive durante as missões e operações no âmbito da política comum de segurança e defesa (PCSD); que a UE e os seus Estados-Membros devem organizar exercícios conjuntos com regularidade, com vista a identificar pontos fracos e a adotar as medidas necessárias;

### ***Ingerência por parte de intervenientes mundiais através da captação de elites, diásporas nacionais, universidades e eventos culturais***

- BW. Considerando que vários políticos, incluindo antigos políticos e funcionários públicos europeus que ocuparam posições de destaque são contratados ou cooptados – em troca dos seus conhecimentos e em detrimento dos interesses dos cidadãos da UE e dos seus Estados-Membros – por empresas públicas ou privadas estrangeiras controladas por Estados autoritários;
- BX. Considerando que alguns países são particularmente ativos no domínio da captação e cooptação de elites, em particular a Rússia e a China, mas também a Arábia Saudita e outros países do Golfo, tal como sucedeu, por exemplo, com o antigo chanceler alemão, Gerhard Schröder, com o antigo primeiro-ministro da Finlândia, Paavo Lipponen, que se juntaram à Gazprom para acelerar o processo de candidatura aos projetos Nord Stream 1 e 2, com a antiga ministra dos Negócios Estrangeiros da Áustria, Karin Kneissl, nomeada membro do conselho de administração da Rosneft, com o antigo primeiro-ministro francês, François Fillon, nomeado membro do conselho de administração de Zarubejneft, com o antigo primeiro-ministro francês, Jean-Pierre Raffarin, ativamente empenhado na promoção dos interesses chineses em França, com o antigo comissário Štefan Füle, que trabalhou para a CEFC China Energy, com o antigo primeiro-ministro finlandês, Esko Aho, que pertence atualmente ao conselho de administração do banco estatal russo Sberbank, com o antigo ministro francês das Relações com o Parlamento, Jean-Marie Le Guen, que é atualmente membro do

conselho de administração da Huawei France, ou com o antigo primeiro-ministro belga, Yves Leterme, que foi nomeado vice-presidente do fundo de investimento chinês ToJoy, e com muitos outros antigos políticos e altos funcionários que atualmente ocupam cargos idênticos;

- BY. Considerando que as estratégias de representação dos grupos de interesses económicos podem estar associadas a objetivos de ingerência estrangeira; que, de acordo com o relatório da OCDE sobre a representação dos grupos de interesses no século XXI<sup>12</sup>, apenas os EUA, a Austrália e o Canadá dispõem de regras que cobrem a influência estrangeira; que existe uma séria falta de regras juridicamente vinculativas e uma aplicação insatisfatória do registo de grupos de interesses da UE, o que faz com que seja praticamente impossível controlar as atividades de representação dos grupos de interesses com origem em países terceiros; que é atualmente impossível controlar os esforços de representação dos grupos de interesses desenvolvidos nos Estados-Membros, que influenciam a legislação e a política externa através do Conselho Europeu; que as regras em matéria de representação dos grupos de interesses na UE se centram principalmente no contacto presencial e não têm em conta todo o ecossistema dos diferentes tipos de representação dos grupos de interesses existente em Bruxelas; que países como a China e a Rússia, mas também o Catar, os Emirados Árabes Unidos e a Turquia, investiram fortemente em atividades de representação dos grupos de interesses em Bruxelas;
- BZ. Considerando que a tentativa de instrumentalizar os grupos vulneráveis, incluindo as minorias e as diásporas nacionais que vivem em território da UE, representa um elemento importante das estratégias de ingerência estrangeira;
- CA. Considerando que diferentes intervenientes estatais, como os governos russo e chinês e, em menor grau, o Governo turco, têm tentado aumentar a sua influência através da criação e do recurso, nos Estados-Membros, a institutos culturais, estabelecimentos de ensino (nomeadamente através de subvenções e bolsas de estudo) e institutos religiosos, num esforço estratégico para desestabilizar a democracia europeia e expandir o controlo sobre a Europa Oriental e Central; que a Rússia já invocou a existência de uma situação supostamente difícil da sua minoria nacional como desculpa para intervir diretamente em países terceiros;
- CB. Considerando que existem provas de manipulação de informação em linha e ingerência russa em muitas democracias liberais em todo o mundo, incluindo, mas não exclusivamente, no referendo sobre o Brexit no Reino Unido e nas eleições presidenciais em França e nos EUA, bem como através da prestação de apoio prático a partidos extremistas, populistas e antieuropeus e a determinados partidos e indivíduos em toda a Europa, incluindo, mas não exclusivamente, em França, na Alemanha, em Itália e na Áustria; que é necessário aumentar o apoio à investigação e à educação para se compreender a influência exata da ingerência estrangeira no âmbito de acontecimentos específicos, como o Brexit e a eleição do Presidente Trump em 2016;
- CC. Considerando que as redes Sputnik e RT, controladas pelo Estado russo e estabelecidas no Ocidente, em combinação com meios de comunicação social ocidentais total ou

---

<sup>12</sup> Organização de Cooperação e de Desenvolvimento Económicos, *Lobbying in the 21st Century: Transparency, Integrity and Access*, 2021, Publicações da OCDE, Paris, disponível em: <https://doi.org/10.1787/c6d8eff8-en>

parcialmente detidos por entidades singulares ou coletivas russas ou chinesas, desenvolvem atividades de desinformação contra democracias liberais; que a Rússia recorre ao revisionismo histórico, procurando reescrever a história dos crimes soviéticos e promover a nostalgia soviética junto da população suscetível na Europa Central e Oriental; que as emissoras nacionais da Europa Central e Oriental têm dificuldade em competir com os conteúdos televisivos em russo, financiados pelo Governo russo; que existe um risco de desequilíbrio na cooperação entre os meios de comunicação social chineses e estrangeiros, atendendo ao facto de os meios de comunicação social chineses serem a voz do Partido Comunista Chinês dentro e fora do país;

- CD. Considerando a abertura de mais de 500 centros Confúcio em todo o mundo, incluindo cerca de 200 na Europa, e que os Institutos Confúcio e as Salas de Aula Confúcio são utilizados pela China como instrumento de ingerência na UE; que a liberdade académica é seriamente restringida nos Institutos Confúcio; que as universidades e os programas de ensino são objeto de um enorme financiamento estrangeiro, nomeadamente da China e do Catar, como acontece com o *campus* da Universidade de Fudan, em Budapeste;
- CE. Considerando que a UE não dispõe atualmente do conjunto de ferramentas necessário para dar resposta à captação de elites e para combater a criação de canais de influência, inclusive nas instituições da UE; que continua a verificar-se, a nível da UE, uma escassez de capacidades de conhecimento da situação e de instrumentos de contrainformação, existindo uma forte dependência da disponibilidade dos intervenientes nacionais para partilhar informações;

#### ***Dissuasão, imputação e contramedidas coletivas, incluindo sanções***

- CF. Considerando que a UE e os seus Estados-Membros não dispõem atualmente de um regime específico de sanções relacionadas com ingerências estrangeiras e campanhas de desinformação orquestradas por intervenientes estatais estrangeiros, o que significa que estes intervenientes podem legitimamente presumir que as suas campanhas de desestabilização da UE não terão de enfrentar quaisquer consequências;
- CG. Considerando que a imputação clara da desinformação e dos ataques de propaganda, nomeadamente através da identificação pública dos perpetradores, dos respetivos patrocinadores e dos objetivos visados, a par da medição dos efeitos desses ataques no público-alvo, constituem os primeiros passos para garantir uma defesa eficaz contra tais ações;
- CH. Considerando que a UE deve reforçar os seus instrumentos de dissuasão e os instrumentos que lhe permitem imputar estes ataques e classificá-los como lesivos ou não do direito internacional, com o objetivo de estabelecer um regime de sanções eficaz, de molde a que os intervenientes estrangeiros mal-intencionados tenham de pagar o preço das suas decisões e arcar com as consequências; que poderá não ser suficiente visar pessoas individuais; que podem ser utilizados outros instrumentos, designadamente medidas comerciais, para proteger os processos democráticos europeus contra ataques híbridos patrocinados por intervenientes estatais; que as medidas de dissuasão devem ser aplicadas de forma transparente e ser devidamente justificadas; que os ataques híbridos são calibrados de modo a ficarem deliberadamente abaixo do limiar estabelecido no artigo 42.º, n.º 7, do Tratado da União Europeia e no artigo 5.º do

Tratado do Atlântico Norte;

### ***Cooperação mundial e multilateralismo***

- CI. Considerando que as ações mal-intencionadas orquestradas por intervenientes estatais e não estatais estrangeiros estão a afetar muitos países parceiros democráticos em todo o mundo; que os aliados democráticos dependem da sua capacidade de unir forças numa resposta coletiva;
- CJ. Considerando que os países dos Balcãs Ocidentais em fase de adesão à UE estão a ser atingidos de forma particularmente dura por ataques sob a forma de ingerência estrangeira e de campanhas de desinformação com origem na Rússia, na China e na Turquia, como as campanhas de ingerência da Rússia durante o processo de ratificação do Acordo de Prespa na Macedónia do Norte; que a pandemia de COVID-19 foi ainda mais explorada pela China e pela Rússia nos Balcãs Ocidentais para desestabilizar estes países e desacreditar a UE; que se espera que os países candidatos e potencialmente candidatos adiram às iniciativas da UE para combater a ingerência estrangeira;
- CK. Considerando que continua a não haver um entendimento comum, bem como definições comuns, entre parceiros e aliados que partilham as mesmas ideias quanto à natureza das ameaças em causa; que o Secretário-Geral das Nações Unidas apela à elaboração de um código de conduta global para promover a integridade da informação pública; que a Conferência sobre o Futuro da Europa é uma plataforma importante para os debates relacionados com a matéria;
- CL. Considerando que é necessária uma cooperação global e multilateral e apoio entre parceiros que partilham as mesmas ideias para lidar com a ingerência estrangeira mal-intencionada; que outras democracias, como a Austrália e Taiwan, desenvolveram competências avançadas e estratégias; que Taiwan está na linha da frente da luta contra a manipulação da informação, principalmente proveniente da China; que o êxito do sistema taiwanês se deve à cooperação entre todos os ramos do Governo, mas também com ONG independentes especializadas na verificação de factos e na literacia mediática e com plataformas de redes sociais como o Facebook, bem como à promoção da literacia mediática de todas as gerações, à desmistificação da desinformação e à redução da propagação de mensagens manipuladoras; que a Comissão Especial INGE realizou uma missão oficial de três dias a Taiwan para debater a desinformação e a ingerência eleitoral estrangeira;

### ***Necessidade de uma estratégia coordenada da UE contra a ingerência estrangeira***

1. Manifesta profunda preocupação com o número e o grau de sofisticação crescentes das ingerências estrangeiras e das tentativas de manipulação da informação dirigidas contra todos os aspetos do funcionamento democrático da União Europeia e dos seus Estados-Membros, que são predominantemente levadas a cabo pela Rússia e pela China;
2. Insta a Comissão a propor, e os legisladores e os Estados-Membros a apoiarem, uma estratégia multidimensional, coordenada e transetorial, bem como recursos financeiros adequados, a fim de dotar a UE e os seus Estados-Membros de capacidades prospetivas e políticas de resiliência adequadas e de instrumentos de dissuasão que lhes permitam enfrentar todas as ameaças híbridas e ataques orquestrados por intervenientes estatais e

não estatais estrangeiros; considera que uma tal estratégia deve assentar no seguinte:

- a) terminologias e definições comuns, uma metodologia única, avaliações e avaliações de impacto *ex post* da legislação adotada até à data, um sistema de informações partilhado e a compreensão, a monitorização, incluindo capacidades de alerta precoce, e o conhecimento da situação das questões em jogo,
  - b) políticas concretas que permitam reforçar a resiliência dos cidadãos da UE, em consonância com os valores democráticos, nomeadamente através do apoio à sociedade civil,
  - c) capacidades adequadas para lidar com situações de perturbação e capacidades de defesa,
  - d) respostas diplomáticas e dissuasivas, incluindo um conjunto de instrumentos da UE para combater a ingerência estrangeira e as tentativas de exercer influência, incluindo operações híbridas, através de medidas adequadas, como, por exemplo, a imputação e a identificação dos perpetradores, sanções e contramedidas, e parcerias mundiais para o intercâmbio de práticas e a promoção de normas internacionais de comportamento responsável dos Estados;
3. Sublinha que todas as medidas destinadas a prevenir, detetar, imputar, combater e sancionar as ingerências estrangeiras devem ser concebidas de tal forma, que respeitem e promovam os direitos fundamentais, nomeadamente a capacidade dos cidadãos da UE de comunicar de forma segura, anónima e não censurada, sem interferências indevidas por parte de quaisquer intervenientes estrangeiros;
4. Considera que uma tal estratégia deve seguir uma abordagem baseada no risco, que tenha em conta a sociedade e o governo na sua totalidade, abrangendo, em particular, os seguintes domínios:
- a) o reforço da resiliência da UE através de um conhecimento situacional, da literacia mediática e informacional, do pluralismo dos meios de comunicação social, do jornalismo independente e da educação,
  - b) a ingerência estrangeira através da utilização de plataformas em linha,
  - c) as infraestruturas críticas e os setores estratégicos,
  - d) a ingerência estrangeira durante processos eleitorais,
  - e) o financiamento encoberto de atividades políticas por intervenientes e doadores estrangeiros,
  - f) a cibersegurança e a resiliência contra ciberataques,
  - g) a proteção dos Estados-Membros, instituições, agências, delegações e missões da UE,
  - h) a ingerência por parte de intervenientes mundiais através da captação de elites, diásporas nacionais, universidades e eventos culturais,

- i) a dissuasão, a imputação e as contramedidas coletivas, incluindo sanções,
  - j) a cooperação mundial e o multilateralismo;
5. Insta, em particular, a UE e os seus Estados-Membros a aumentarem os recursos e meios atribuídos às organizações e organismos em toda a Europa e a nível mundial – tais como grupos de reflexão e verificadores de factos – incumbidos de acompanhar e sensibilizar para a gravidade das ameaças, nomeadamente a desinformação; destaca o papel crucial da UE num sentido estratégico mais lato; apela ao reforço da capacidade prospetiva e da interoperabilidade da UE e dos seus Estados-Membros, a fim de assegurar uma preparação sólida para prever, prevenir e aplacar a manipulação da informação e a ingerência estrangeira, reforçar a proteção dos seus interesses estratégicos e infraestruturas e participar na cooperação e coordenação multilaterais, de molde a alcançar um entendimento comum da questão nas instâncias internacionais pertinentes; insta o Conselho dos Negócios Estrangeiros a debater regularmente assuntos relacionados com a ingerência estrangeira;
  6. Manifesta a sua preocupação com a falta flagrante de sensibilização, em particular do público em geral e dos funcionários públicos, para a gravidade das ameaças atualmente colocadas pelos regimes autoritários estrangeiros e por outros intervenientes mal-intencionados, que visam todos os níveis e setores da sociedade europeia com o objetivo de minar os direitos fundamentais e a legitimidade das autoridades públicas, de aumentar a fragmentação política e social e, em alguns casos, causando inclusivamente situações que podem pôr em perigo a vida dos cidadãos da UE;
  7. Manifesta a sua preocupação com a falta de normas e de medidas adequadas e suficientes para imputar os atos de ingerência estrangeira e dar resposta aos mesmos, o que resulta numa fórmula atrativa para os intervenientes mal-intencionados, composta por baixos custos, baixos riscos e uma elevada recompensa, tendo em conta que o risco de serem castigados pelos seus atos é atualmente reduzidíssimo;
  8. Insta a Comissão a incluir, se for caso disso, uma perspetiva de manipulação da informação e de ingerência estrangeira na avaliação de impacto *ex ante* levada a cabo antes da apresentação de novas propostas, com vista a integrar o combate à manipulação da informação e à ingerência estrangeira na elaboração de políticas da UE; exorta o SEAE e a Comissão a procederem com regularidade a uma análise da resiliência e a avaliarem a evolução das ameaças e o seu impacto na legislação e nas políticas em vigor;
  9. Insta a Comissão a analisar as instituições nacionais recentemente criadas, como o coordenador nacional de combate às ingerências estrangeiras estabelecido na Austrália, o comité de segurança da Finlândia que assiste o Governo e os ministérios, a agência para as situações de emergência civil, a nova agência de defesa psicológica e o Centro Nacional da China instituídos na Suécia, a nova agência nacional francesa, Viginum, o centro nacional de cibersegurança lituano e o grupo de trabalho de Taiwan para a coordenação interagências no domínio da desinformação, a fim de ver o que podemos aprender com essas boas práticas e de determinar em que medida é possível aplicar uma ideia semelhante a nível da UE; convida a Comissão a apoiar a partilha de informações e de boas práticas entre os Estados-Membros neste domínio; sublinha a importância de

uma abordagem e de instrumentos proativos, incluindo a comunicação estratégica como atividade principal para executar as políticas da UE e dos Estados-Membros através de palavras e ações; insta a Comissão a oferecer formação adequada no domínio da ciência de dados e a criar um organismo único de supervisão no seio da Comissão em matéria de manipulação de informações;

10. Manifesta a sua preocupação com o grande número de deficiências e lacunas existentes na legislação e nas políticas em vigor a nível da UE e a nível nacional que têm por objetivo detetar, prevenir e combater as ingerências estrangeiras;
11. Assinala que a UE está a financiar vários projetos e programas a longo prazo que colocam a tónica no combate à desinformação a nível tecnológico, jurídico, psicológico e informacional; exorta a Comissão a avaliar o impacto e a aplicabilidade de tais projetos e programas;
12. Insta a Comissão a criar um grupo de trabalho, liderado por Věra Jourová, enquanto Vice-Presidente da Comissão responsável pela pasta «Valores e Transparência», e dedicado ao exame da legislação e das políticas existentes, a fim de identificar lacunas que possam ser exploradas por intervenientes mal-intencionados, e exorta a Comissão a colmatar essas lacunas; salienta que essa estrutura deve cooperar com outras instituições da UE e com os Estados-Membros a nível nacional, regional e local e facilitar o intercâmbio de boas práticas; insta a Comissão e o SEAE a ponderarem a criação de um Centro Europeu para as Ameaças de Ingerência e a Integridade da Informação, dotado de recursos adequados e independente, com a missão de identificar, analisar e documentar as operações de manipulação da informação e as ameaças de ingerência contra a UE no seu conjunto, aumentar o conhecimento da situação, desenvolver um centro de conhecimentos especializados, tornando-se uma plataforma de coordenação com a sociedade civil, o setor empresarial, as instituições nacionais e da UE, e sensibilizar o público, nomeadamente através de relatórios periódicos sobre ameaças sistémicas; salienta que a criação provisória desse novo Centro Europeu para as Ameaças de Ingerência e a Integridade da Informação, independente e dotado de recursos adequados, deve contribuir para esclarecer e reforçar o papel da Divisão StratCom do SEAE e dos seus grupos de trabalho, enquanto organismos estratégicos do serviço diplomático da UE, e evitar a sobreposição de atividades; realça que o mandato da Divisão StratCom do SEAE deve centrar-se no desenvolvimento estratégico de políticas externas para combater as ameaças conjuntas existentes e emergentes, bem como para reforçar a cooperação com os parceiros internacionais neste domínio; assinala que a Divisão StratCom do SEAE pode prosseguir esse objetivo em estreita cooperação com o novo Centro Europeu para as Ameaças de Ingerência e a Integridade da Informação e o novo grupo de trabalho da Comissão;
13. Apela às instituições da UE e aos Estados-Membros para que habilitem a sociedade civil a desempenhar um papel ativo na luta contra a ingerência estrangeira; insta todos os níveis e setores da sociedade europeia a criarem mecanismos que tornem as organizações e os cidadãos mais resilientes à ingerência estrangeira, permitam detetar a tempo os ataques e combatê-los da forma mais eficiente possível, inclusive através da educação e da sensibilização, no respeito pelo quadro da UE para os direitos fundamentais e de uma forma transparente e democrática; destaca, neste contexto, as boas práticas e a abordagem que mobiliza toda a sociedade aplicadas por Taiwan; exorta



os decisores políticos a dotarem a sociedade civil de instrumentos adequados e de financiamento específico para estudar, expor e combater a influência estrangeira;

***Reforçar a resiliência da UE através do conhecimento situacional, da literacia mediática e da educação***

14. Salaria que as instituições da UE e os Estados-Membros necessitam de sistemas sólidos, robustos e interligados para detetar, analisar, acompanhar e fazer um levantamento dos incidentes em que intervenientes estatais e não estatais estrangeiros tentam interferir nos processos democráticos, para deste modo desenvolver um conhecimento situacional e uma compreensão clara do tipo de comportamentos que a UE e os seus Estados-Membros se veem na necessidade de dissuadir e combater; apela a uma investigação sociológica regular e à realização de sondagens para monitorizar a resiliência e a literacia mediática, bem como para compreender o apoio público e as perceções das narrativas de desinformação mais comuns;
15. Sublinha que é igualmente importante que as conclusões desta análise não sejam apenas acessíveis a grupos de especialistas em matéria de ingerência estrangeira, mas sejam partilhadas abertamente, tanto quanto possível, com o público em geral, especialmente com pessoas que desempenham funções sensíveis, para que todos estejam cientes dos padrões que caracterizam as ameaças e possam evitar os riscos;
16. Sublinha que, para adquirir um conhecimento da situação, é necessário desenvolver uma metodologia comum, dispor de capacidades de alerta precoce e de avaliação de ameaças, recolher provas sistematicamente e detetar a tempo manipulações do ambiente de informação, bem como desenvolver normas de atribuição técnica, por exemplo, no que se refere à autenticidade dos conteúdos, a fim de assegurar uma resposta eficaz;
17. Salaria a necessidade de a UE desenvolver, em cooperação com os Estados-Membros e trabalhando a nível multilateral nas instâncias internacionais pertinentes, uma definição concetual das ameaças de ingerência que a UE enfrenta; realça que uma tal definição deve refletir as táticas, as técnicas, os procedimentos e as ferramentas utilizados para descrever os padrões de comportamento dos perpetradores estatais e não estatais de ameaças a que assistimos atualmente; exorta a Comissão a envolver, no âmbito deste processo, a FRA da UE para garantir que nenhuma das definições concetuais contém noções ou preconceitos discriminatórios ou iníquos;
18. Destaca que a diplomacia pública e a comunicação estratégica são elementos fundamentais das relações externas e da proteção dos valores democráticos da UE; insta as instituições da UE a continuarem a desenvolver e a intensificar o importante trabalho da Divisão StratCom do SEAE, com os seus grupos de trabalho, o Centro de Situação e de Informações da UE (UE INTCEN) e a célula de fusão híbrida, a Direção de Informações do Estado-Maior da UE, o sistema de alerta rápido, a cooperação estabelecida a nível administrativo entre o SEAE, a Comissão e o Parlamento, a rede liderada pela Comissão contra a desinformação, o grupo de trabalho administrativo do Parlamento contra a desinformação e a cooperação em curso com a NATO, o G7, a sociedade civil e o setor privado no que diz respeito à melhor forma de cooperar em matéria de informação, análise, partilha de boas práticas e sensibilização para a manipulação da informação e a ingerência estrangeira; acolhe com agrado o Relatório

Especial n.º 09/2021 do Tribunal de Contas Europeu (TCE), intitulado «Desinformação na UE: fenómeno combatido, mas não controlado»; solicita ao SEAE e à Comissão que publiquem um calendário pormenorizado para a aplicação das recomendações do TCE;

19. Realça que é necessário redobrar continuamente os esforços no sentido de acompanhar a situação e de os intensificar muito antes da realização de eleições, de referendos ou de outros processos políticos importantes na Europa;
20. Insta os Estados-Membros a tirarem pleno partido destes recursos, partilhando informações pertinentes com o UE INTCEN e aumentando a sua participação no sistema de alerta rápido; entende que é necessário reforçar ainda mais a análise e a cooperação na UE e com a NATO em matéria de informação, aumentando, ao mesmo tempo, a transparência e responsabilização democrática dessa cooperação, inclusive mediante a partilha de informações com o Parlamento;
21. Congratula-se com a ideia avançada pela Presidente da Comissão, Ursula von der Leyen, no sentido de criar um Centro Comum de Conhecimento da Situação para melhorar a prospetiva estratégica e a autonomia estratégica aberta da UE, embora aguarde esclarecimentos adicionais relativamente à sua criação e missão; destaca que um centro desta natureza exigiria uma cooperação ativa com os serviços competentes da Comissão, do SEAE, do Conselho, do Parlamento e das autoridades nacionais; reitera, no entanto, a importância de evitar a duplicação de trabalho e a sobreposição com as estruturas existentes da UE;
22. Recorda a necessidade de dotar o SEAE de um mandato reforçado e claramente definido e dos recursos necessários para permitir à Divisão de Comunicações Estratégicas e Análise de Informações, com os seus grupos de trabalho, monitorizar e fazer face à manipulação da informação e ingerência por parte de intervenientes distintos das fontes estrangeiras atualmente abrangidas pelos três grupos de trabalho, e permitir-lhe também alargar a sua cobertura geográfica, seguindo para tal uma abordagem baseada no risco; apela urgentemente para que o SEAE mobilize capacidades suficientes para fazer face à manipulação da informação e ingerência que tem origem na China, nomeadamente através da criação de uma equipa específica para o Extremo Oriente; salienta ainda a necessidade de reforçar significativamente no SEAE, nos Estados-Membros e nas instituições da UE em geral os conhecimentos especializados e as capacidades linguísticas relativamente à China e a outras regiões estrategicamente importantes, bem como de recorrer a fontes de informação abertas, que são atualmente subutilizadas;
23. Frisa a importância de meios de comunicação social amplamente acessíveis, competitivos e pluralistas, dos jornalistas independentes, dos verificadores de factos e dos investigadores, assim como de um forte serviço público de comunicação social para um debate democrático aceso e livre; congratula-se com as iniciativas, como o Observatório Europeu dos Meios de Comunicação Digitais e o Fundo Europeu para a Democracia, que se destinam a reunir, formar e apoiar de outro modo organizações de jornalistas independentes, verificadores de factos e investigadores em toda a Europa e, em particular, nas regiões mais ameaçadas; lamenta profundamente que o Observatório Europeu dos Meios de Comunicação Digitais não abranja os Estados bálticos; congratula-se, igualmente, com as iniciativas destinadas a estabelecer indicadores

facilmente reconhecíveis de fiabilidade do jornalismo e da verificação de factos, como os que foram criados pelos Repórteres Sem Fronteiras; exorta a Comissão a combater a propriedade monopolista dos meios de comunicação social;

24. Louva a investigação indispensável e as numerosas iniciativas criativas e bem-sucedidas em matéria de literacia mediática e digital e de sensibilização levadas a cabo por pessoas individuais, escolas, universidades, organizações de meios de comunicação social, instituições públicas e organizações da sociedade civil;
25. Solicita que a UE e os Estados-Membros reservem o financiamento público da UE para verificadores de factos independentes, investigadores, meios de comunicação social e jornalistas de investigação de qualidade e ONG que pesquisem e investiguem a manipulação da informação e a ingerência, promovam a literacia mediática, digital e informacional e outros meios para capacitar os cidadãos e investiguem como medir de forma significativa a eficácia da formação em matéria de literacia mediática, digital e informacional, da sensibilização, da desmistificação e da comunicação estratégica;
26. Apela à tomada de medidas para reforçar os meios de comunicação social profissionais e pluralistas, garantindo que os editores recebam uma remuneração justa pela utilização dos seus conteúdos na Internet; sublinha que vários países em todo o mundo estão a tomar medidas para garantir que os meios de comunicação social disponham de recursos financeiros adequados; insta novamente à criação de um fundo permanente da UE para os meios de informação e regozija-se, neste contexto, com a Iniciativa «News», incluindo as novas possibilidades de financiamento para o setor dos meios de comunicação social e a literacia mediática e informacional no âmbito do Programa Europa Criativa 2021-2027; observa, no entanto, que os fluxos de financiamento podem gerar dependências ou ter impacto na independência dos meios de comunicação social; salienta, a este respeito, a importância da transparência do financiamento dos meios de comunicação social; considera que a proteção do pluralismo dos meios de comunicação social depende da divulgação pública de informação não só sobre quem são os seus proprietários e doadores, mas também sobre quem os controla ou lhes fornece conteúdos e sobre quem paga pelos conteúdos jornalísticos;
27. Realça a necessidade de elaborar e disponibilizar ao público análises, relatórios de incidentes e avaliações das ameaças públicas baseadas em informações a respeito da manipulação da informação e da ingerência; sugere, por conseguinte, a criação de uma base de dados à escala da UE sobre incidentes de ingerência estrangeira comunicados pelas autoridades da UE e dos Estados-Membros; sublinha que as informações sobre estes incidentes podem ser partilhadas, se for caso disso, com as organizações da sociedade civil e o público, em todas as línguas da UE;
28. Solicita a todos os Estados-Membros que – desde o ensino na primeira infância até à educação de adultos, passando pela formação de professores e investigadores – incluam nos seus programas curriculares a literacia mediática e digital, bem como a educação sobre a democracia, os direitos fundamentais, a história recente, os assuntos mundiais, o pensamento crítico e a participação pública; exorta a Comissão e os Estados-Membros a aumentarem o apoio ao ensino da história e à investigação sobre o impacto da ingerência estrangeira e do totalitarismo passado na sociedade em geral e, mais especificamente, nos acontecimentos democráticos em grande escala;

29. Apela às instituições da UE e aos Estados-Membros, a todos os níveis administrativos, para que identifiquem os setores suscetíveis de ser alvo de tentativas de ingerência e a preverem regularmente formação e exercícios para o pessoal que trabalha nos setores em causa sobre a forma de detetar e evitar tentativas de ingerência, e sublinha que tais esforços beneficiariam da existência de um formato normalizado estabelecido pela UE; recomenda que sejam igualmente ministrados módulos de formação abrangentes a todos os funcionários públicos; congratula-se, a este respeito, com a formação facultada aos deputados e ao pessoal pela administração do Parlamento; recomenda que esta formação continue a ser aperfeiçoada;
30. Destaca a necessidade de sensibilizar para a ingerência estrangeira em todos os estratos sociais; congratula-se com as iniciativas tomadas pelo SEAE, pela Comissão e pela administração do Parlamento, tais como a realização de ações de formação e de sensibilização para jornalistas, professores, influenciadores, estudantes, pessoas idosas e visitantes, tanto fora de linha como em linha, em Bruxelas e nos Estados-Membros, e recomenda que estas continuem a ser desenvolvidas;
31. Insta os Estados-Membros, a administração da UE e as organizações da sociedade civil a partilharem as boas práticas no domínio da formação e sensibilização em matéria de literacia mediática e informacional, conforme requer a Diretiva Serviços de Comunicação Social Audiovisual<sup>13</sup>; insta a Comissão a organizar estes intercâmbios em cooperação com o Grupo de Peritos em Literacia Mediática; realça que a diretiva revista deve ser rápida e devidamente aplicada pelos Estados-Membros;
32. Exorta as instituições da UE a elaborarem um Código de Ética que forneça orientações às autoridades públicas e aos representantes políticos sobre a utilização das plataformas de redes sociais; considera necessário promover uma utilização responsável de tais plataformas de redes sociais para combater a manipulação e as informações erradas com origem na esfera pública;
33. Insta a UE e os seus Estados-Membros a implementarem programas adaptados de sensibilização e literacia mediática e informacional, inclusivamente para as diásporas e as minorias, e insta a Comissão a criar um sistema de fácil partilha de material em línguas minoritárias, a fim de reduzir os custos de tradução e chegar ao maior número possível de pessoas; insta as regiões e os municípios a assumirem um papel de proa, uma vez que é importante chegar às zonas rurais e a todos os grupos demográficos;
34. Salaria que a resposta essencial a tentativas de ingerência estrangeira consiste na defesa dos principais grupos-alvo a que estas se dirigem; frisa a necessidade de ações específicas, através de um quadro jurídico harmonizado da UE, contra a propagação da desinformação e do discurso de ódio sobre questões relacionadas com o género, as pessoas LGBTIQ+, as minorias e os refugiados; exorta a Comissão a desenvolver e executar estratégias que impeçam o financiamento de indivíduos e grupos que manipulam a informação ou participam ativamente na manipulação da informação visando frequentemente os grupos e temas acima mencionados, a fim de dividir a sociedade; apela à realização de campanhas de comunicação positivas sobre estas

---

<sup>13</sup> Diretiva 2010/13/UE do Parlamento Europeu e do Conselho, de 10 de março de 2010, relativa à coordenação de certas disposições legislativas, regulamentares e administrativas dos Estados-Membros respeitantes à oferta de serviços de comunicação social audiovisual (JO L 95 de 15.4.2010, p. 1).

- questões e frisa a necessidade de uma formação sensível à dimensão de género;
35. Reconhece que os ataques e campanhas de desinformação baseados no género são frequentemente utilizados no âmbito de uma estratégia política mais ampla para prejudicar a igualdade de participação nos processos democráticos e visam especialmente as mulheres e as pessoas LGBTIQ+; salienta que a desinformação sobre as pessoas LGBTIQ+ alimenta o ódio, tanto em linha como fora de linha, e coloca em risco a vida dessas pessoas; apela à realização de investigação sobre a desinformação em linha numa perspetiva interseccional e ao controlo das mudanças que as plataformas estão a efetuar para combater as campanhas de desinformação relativa ao género em linha; apela a que seja prestada maior atenção à desinformação relativa ao género mediante a criação de sistemas de alerta precoce através dos quais as campanhas de desinformação relativa ao género possam ser identificadas e denunciadas;
  36. Insta a Comissão a apresentar uma estratégia global de literacia mediática e informacional que coloque uma ênfase especial na luta contra a manipulação da informação;
  37. Saúda a criação de um grupo de peritos para combater a desinformação e promover a literacia digital através da educação e da formação, cujo trabalho se centrará, designadamente, no pensamento crítico, na formação de professores, em esforços de desmistificação prévia, desmistificação e verificação de factos e no envolvimento dos estudantes; insta a Comissão a partilhar os resultados do trabalho deste grupo de peritos e a dar seguimento às suas conclusões;
  38. Sublinha a importância da comunicação estratégica no combate às narrativas antidemocráticas mais comuns; apela a que a UE melhore a sua comunicação estratégica, de modo a aumentar o seu alcance junto dos cidadãos e no estrangeiro; salienta que todas as organizações democráticas têm de defender a democracia e salvaguardar o Estado de direito e têm a responsabilidade comum de dialogar com os cidadãos através das suas línguas e plataformas preferidas;
  39. Insta os Estados-Membros a garantirem a eficácia das campanhas de comunicação públicas relacionadas com a pandemia de COVID-19, de modo a difundir informações precisas e oportunas para combater as informações erradas, sobretudo no que se refere às vacinas;
  40. Manifesta profunda preocupação com a disseminação de propaganda estatal estrangeira, proveniente essencialmente de Moscovo e Pequim, assim como de Ancara, que é traduzida para as línguas locais, por exemplo, em conteúdos nos meios de comunicação social patrocinados pela rede televisiva RT, pelas agências noticiosas Sputnik e Anadolu, pela operadora de radiodifusão CCTV, pelo tabloide *Global Times*, pela agência noticiosa Xinhua, pelo canal de televisão TRT World ou pelo Partido Comunista Chinês, apresentados sob a forma de jornalismo e distribuídos com os jornais; defende que estes canais não podem ser considerados verdadeiros meios de comunicação social, não devendo, por isso, gozar dos direitos e proteções concedidas a tais meios; manifesta igualmente a sua preocupação com a forma como estas narrativas se propagaram, tornando-se verdadeiros produtos jornalísticos; salienta a necessidade de aumentar a sensibilização para as campanhas de desinformação da Rússia e da China,

que têm por objetivo pôr em causa os valores democráticos e dividir a UE, atendendo a que constituem a principal fonte de desinformação na Europa; exorta a Comissão a iniciar um estudo sobre normas mínimas aplicáveis aos meios de comunicação social, como base para a possível revogação de licenças em caso de infração; solicita à Comissão que incorpore as conclusões do estudo em legislação futura, como uma possível lei sobre a liberdade dos meios de comunicação social; faz notar que os intervenientes responsáveis pela ingerência estrangeira podem falsamente apresentar-se como jornalistas; entende que, nesses casos, deve ser possível sancionar essa pessoa ou organização, por exemplo, através da sua identificação pública, da sua exclusão de eventos de imprensa ou da revogação da sua acreditação de profissional da comunicação social;

41. Manifesta profunda preocupação com os ataques, o assédio, a violência e as ameaças contra jornalistas, defensores dos direitos humanos e outras pessoas que denunciam casos de ingerência estrangeira, o que também pode comprometer a sua independência; solicita à Comissão que apresente sem demora propostas concretas e ambiciosas relativas à segurança de todas estas pessoas, incluindo um instrumento de combate às ações judiciais estratégicas contra a participação pública (SLAPP) e apoio económico, jurídico e diplomático, tal como anunciado no Plano de Ação para a Democracia Europeia; saúda, neste contexto, a Recomendação (UE) 2021/1534 da Comissão, de 16 de setembro de 2021, relativa à garantia de proteção, segurança e capacitação dos jornalistas e outros profissionais da comunicação social na União Europeia<sup>14</sup>; exorta os Estados-Membros a protegerem eficazmente os jornalistas e outros profissionais da comunicação social com recurso a instrumentos legislativos e não legislativos;
42. Salaria a necessidade de envolver os decisores locais e regionais responsáveis por decisões estratégicas em domínios que se insiram no âmbito das respetivas competências, tais como as infraestruturas, a cibersegurança, a cultura e a educação; sublinha que, muitas vezes, os políticos e as autoridades locais e regionais podem identificar os desenvolvimentos numa fase precoce e salienta que o conhecimento local é frequentemente necessário para determinar e aplicar contramedidas adequadas;
43. Insta a Comissão e os Estados-Membros a estabelecerem canais de comunicação e a criarem plataformas nas quais as empresas, as ONG e os particulares, incluindo os membros das diásporas, possam comunicar casos em que sejam vítimas de manipulação da informação ou de ingerência; insta os Estados-Membros a apoiarem as pessoas que são vítimas de ataques, que têm conhecimento de tais ataques ou que se encontram sob pressão;

#### ***Ingerência estrangeira através da utilização de plataformas em linha***

44. Acolhe favoravelmente a proposta de revisão do Código de Conduta sobre Desinformação e as propostas relativas a um Regulamento Serviços Digitais e um Regulamento Mercados Digitais, bem como outras medidas relacionadas com o Plano de Ação para a Democracia Europeia, como instrumentos potencialmente eficazes para fazer face à ingerência estrangeira; recomenda que a última leitura destes textos tenha em conta os aspetos apresentados na parte remanescente da presente secção;

---

<sup>14</sup> JO L 331 de 20.9.2021, p. 8.

45. Salienta que a liberdade de expressão não deve ser erradamente interpretada como liberdade para participar em atividades em linha consideradas ilegais fora de linha, como o assédio, o discurso de ódio, a discriminação racial, o terrorismo, a violência, a espionagem e as ameaças; sublinha que as plataformas devem não só respeitar a lei do país em que operam, mas também cumprir as suas condições, especialmente as que digam respeito aos conteúdos nocivos em linha; solicita às plataformas que intensifiquem os esforços no sentido de impedir o reaparecimento de conteúdos ilegais idênticos aos que foram identificados como ilegais e removidos;
46. Sublinha que é necessário, acima de tudo, continuar a estudar o crescimento da desinformação e da ingerência estrangeira em linha e que a legislação da UE assegure um aumento considerável e significativo da transparência, do controlo e da responsabilização no que se refere às operações das plataformas em linha e ao acesso aos dados por parte dos requerentes legítimos de acesso, em particular quando se trata de algoritmos e publicidade em linha; solicita às empresas de redes sociais que mantenham bibliotecas de anúncios publicitários;
47. Apela à adoção de regulamentação e de medidas que obriguem as plataformas, especialmente as que apresentam um risco sistémico para a sociedade, a contribuir para reduzir a manipulação da informação e a ingerência, por exemplo, através da utilização de rótulos que indiquem os verdadeiros autores a quem as contas pertencem, da limitação do alcance de contas que sejam regularmente utilizadas para difundir desinformação ou que incumpram regularmente as condições da plataforma, da suspensão e, se necessário e com base em legislação clara, eliminação de contas inautênticas utilizadas em campanhas de ingerência coordenadas ou da desmonetização de sítios de difusão de desinformação, do estabelecimento de medidas de atenuação dos riscos de interferência decorrentes dos efeitos dos seus algoritmos, modelos de publicidade, sistemas de recomendação e tecnologias de IA, e da sinalização dos conteúdos de desinformação, tanto nas publicações como nos comentários; recorda que estas medidas devem ser aplicadas de forma transparente e responsável;
48. Insta a Comissão a ter plenamente em conta a nota de orientação do Conselho da Europa sobre boas práticas para a adoção de quadros jurídicos e processuais eficazes para os mecanismos de autorregulação e de correção da moderação de conteúdos, adotada em junho de 2021;
49. Apela a uma aplicação completa e eficaz do Regulamento Geral sobre a Proteção de Dados<sup>15</sup>, que limite a quantidade de dados que as plataformas podem armazenar sobre os utilizadores e o período de tempo durante o qual estes dados podem ser utilizados, especialmente no caso das plataformas e aplicações que utilizam dados muito privados e/ou sensíveis, nomeadamente nos domínios do envio de mensagens, da saúde, das finanças, das aplicações de marcação de encontros e dos pequenos grupos de discussão; solicita que as plataformas consideradas controladores de acesso se abstenham de combinar os dados pessoais de que dispõem com dados pessoais obtidos no âmbito de outros serviços por elas oferecidos ou de serviços prestados por terceiros, a fim de tornar igualmente fácil para os utilizadores dar ou retirar o seu consentimento

---

<sup>15</sup> 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 (JO L 119 de 4.5.2016, p. 1).

relativamente ao armazenamento e partilha de dados e permitir-lhes escolher se querem ver outros anúncios publicitários personalizados em linha; saúda todos os esforços no sentido de proibir as técnicas de microdirecionamento de publicidade política, em particular, mas não exclusivamente, as que se baseiam em dados pessoais sensíveis, como a origem étnica, as convicções religiosas ou a orientação sexual, e solicita à Comissão que pondere a possibilidade de alargar a proibição do microdirecionamento à publicidade temática;

50. Solicita regras vinculativas da UE que exijam que as plataformas cooperem com as autoridades competentes para efetuar testes regulares ao seus sistemas e identificar, avaliar e atenuar os riscos de manipulação da informação e de ingerência e as vulnerabilidades inerentes à utilização dos seus serviços, incluindo a forma como a conceção e a gestão dos seus serviços contribuem para esses riscos; solicita regras vinculativas da UE que obriguem as plataformas a criar sistemas para monitorizar a forma como os seus serviços são utilizados, nomeadamente permitindo ver em tempo real as publicações mais atuais e populares por país, a fim de detetar casos de manipulação da informação e de ingerência e de sinalizar às autoridades competentes os casos em que haja suspeitas de ingerência, bem como para aumentar os custos para os intervenientes que fazem vista grossa a tais atividades facilitadas pelos seus sistemas;
51. Insta as plataformas em linha a preverem recursos adequados para prevenir ingerências estrangeiras prejudiciais e assegurar aos moderadores de conteúdos melhores condições de trabalho, apoio psicológico e uma remuneração justa; insta as plataformas de redes sociais de grande dimensão a apresentarem relatórios pormenorizados por país sobre os recursos consagrados à verificação de factos, às atividades de investigação, à moderação de conteúdos, incluindo as capacidades humanas e de IA em línguas individuais, e à colaboração com a sociedade civil local; sublinha a necessidade de estas plataformas intensificarem os seus esforços para combater a desinformação em mercados de menor dimensão e comercialmente menos rentáveis na UE;
52. Insta as plataformas de redes sociais a respeitarem plenamente a igualdade de todos os cidadãos da UE, independentemente da língua utilizada na conceção dos seus serviços, ferramentas e mecanismos de monitorização, bem como nas medidas para uma maior transparência e um ambiente em linha mais seguro; salienta que tal se refere não só a todas as línguas nacionais e regionais oficiais, mas também às línguas de diásporas importantes na UE; sublinha que estes serviços devem também ser acessíveis a pessoas com deficiência auditiva;
53. Apela a uma rotulagem clara e legível das falsificações profundas, tanto para os utilizadores das plataformas, como nos metadados do conteúdo, por forma a melhorar a sua rastreabilidade por parte de investigadores e verificadores de factos; regozija-se, a este respeito, com as iniciativas destinadas a melhorar a autenticidade e a rastreabilidade dos conteúdos, tais como o desenvolvimento de marcas de água e de normas de autenticidade e a introdução de normas globais;
54. Solicita que sejam regulamentados os serviços que oferecem ferramentas e serviços de manipulação das redes sociais, como o aumento do alcance das contas ou dos conteúdos através da participação artificial ou de perfis inautênticos; sublinha que esta regulamentação deve basear-se numa avaliação exaustiva das práticas atuais e dos riscos



associados e deve impedir que estes serviços sejam utilizados por intervenientes mal-intencionados para fins de ingerência política;

55. Frisa a necessidade de transparência por parte dos anunciantes no que diz respeito à pessoa singular ou coletiva real que está por detrás das contas e conteúdos em linha; insta as plataformas a criarem mecanismos para detetar e suspender, em particular, as contas inautênticas associadas a operações de influência coordenadas; sublinha que estas práticas não devem interferir na capacidade de manter o anonimato em linha, que é fundamental para proteger jornalistas, ativistas, comunidades marginalizadas e pessoas em posições vulneráveis (por exemplo, autores de denúncias, dissidentes e opositores políticos de regimes autocráticos), e devem permitir a existência de contas satíricas e humorísticas;
56. Sublinha que uma maior responsabilidade pela remoção de conteúdos não deve conduzir à remoção arbitrária de conteúdos legais; recomenda prudência em relação à suspensão total de contas de pessoas reais ou à utilização maciça de filtros automáticos; regista com preocupação as decisões arbitrárias das plataformas de eliminar as contas de representantes eleitos; salienta que estas contas só devem ser eliminadas com base em legislação clara e assente em valores democráticos, enquadrada na política empresarial e aplicada através de um controlo democrático independente, e que deve existir um processo totalmente transparente que preveja o direito de recurso;
57. Solicita regras vinculativas que exijam que as plataformas criem canais de comunicação facilmente acessíveis e eficazes para pessoas ou organizações que pretendam denunciar conteúdos ilegais, situações de incumprimento das condições, casos de desinformação, ingerência estrangeira ou manipulação da informação, se for caso disso, conferindo às pessoas objeto de acusação o direito de responderem antes de serem tomadas medidas restritivas, e permitindo o estabelecimento de processos de consulta ou de recurso imparciais, transparentes, céleres e acessíveis para as vítimas de conteúdos publicados em linha, para as pessoas que denunciaram conteúdos e para as pessoas ou organizações afetadas pela decisão de rotular, restringir a visibilidade, desativar ou suspender contas ou de restringir o acesso às receitas de publicidade; recomenda que as plataformas de redes sociais designem um ponto de contacto específico para cada Estado-Membro e criem grupos de trabalho para todas as eleições importantes em cada Estado-Membro;
58. Apela à adoção de regras legislativas que assegurem a transparência em relação aos utilizadores e ao público em geral, como a obrigação de as plataformas criarem arquivos públicos e facilmente pesquisáveis de anúncios em linha – que incluam informações sobre o público-alvo dos anúncios e a identidade das pessoas que pagaram por esses anúncios, bem como os conteúdos moderados e eliminados –, estabelecerem medidas autorreguladoras e facultarem um acesso abrangente e significativo a informações sobre a conceção, a utilização e o impacto dos algoritmos às autoridades nacionais competentes, investigadores habilitados associados a instituições académicas, meios de comunicação social, organizações da sociedade civil e organizações internacionais que representem o interesse público; considera que os parâmetros destas bibliotecas devem ser harmonizados para permitir análises entre plataformas e reduzir os encargos administrativos das plataformas;
59. Apela ao fim dos modelos de negócio que dependem do incentivo a que as pessoas

passem mais tempo nas plataformas, fornecendo lhes conteúdos cativantes; insta os legisladores e as plataformas a garantirem, através do recurso a moderadores humanos e auditores externos, que os algoritmos não promovam conteúdos ilegais, extremistas, discriminatórios ou conducentes à radicalização, oferecendo antes aos utilizadores uma pluralidade de perspetivas, bem como a privilegiarem e promoverem os factos e conteúdos de base científica, em particular no que respeita a questões sociais importantes como a saúde pública e as alterações climáticas; entende que os sistemas de classificação viciantes e baseados na participação representam uma ameaça sistémica para a nossa sociedade; exorta a Comissão a abordar a questão atual dos incentivos de preço, que levam a que anúncios altamente direcionados com conteúdos divisionistas tenham frequentemente preços muito mais baixos para o mesmo número de visualizações do que anúncios menos direcionados com conteúdos socialmente integradores;

60. Solicita que os algoritmos sejam modificados com o objetivo de parar de promover os conteúdos provenientes de contas e canais inautênticos que conduzem artificialmente à propagação da manipulação nociva de informações por parte de intervenientes estrangeiros; apela à modificação dos algoritmos para que estes não promovam conteúdos divisionistas e que incitem à raiva; frisa a necessidade de a UE adotar medidas que exijam legalmente às empresas de redes sociais que previnam, tanto quanto possível, a amplificação da desinformação, uma vez detetada; salienta que as plataformas devem enfrentar consequências, caso não cumpram a obrigação de remover os conteúdos que promovem a desinformação;
61. Destaca a necessidade de uma fase de testes melhorada e de uma análise sistemática das consequências dos algoritmos, nomeadamente da forma como estes moldam o discurso público e influenciam os resultados políticos, bem como da forma como é atribuída prioridade aos conteúdos; sublinha que uma tal análise deve igualmente centrar-se na questão de saber se as plataformas conseguem assegurar as garantias dadas nas respetivas condições e se dispõem de salvaguardas suficientes para impedir comportamentos inautênticos coordenados em grande escala de manipular os conteúdos exibidos nas suas plataformas;
62. Considera alarmante o valor médio de 65 milhões de euros em receitas de publicidade que revertem todos os anos para cerca de 1 400 sítios Web de desinformação que visam os cidadãos da UE<sup>16</sup>; realça que a publicidade em linha, por vezes até de instituições públicas, é exibida em sítios Web mal-intencionados sem o consentimento, ou inclusivamente o conhecimento, dos anunciantes em causa, acabando por financiar estes sítios que promovem o discurso de ódio e a desinformação; observa que cinco empresas, incluindo a Google Ads, pagam 97 % destas receitas de publicidade e são responsáveis pela seleção dos sítios Web dos editores constantes do seu inventário e, como tal, têm o poder de determinar os conteúdos que são monetizados e os que não o são; considera inaceitável que os algoritmos que atribuem os fundos publicitários sejam completamente ocultados do público; insta a Comissão a utilizar os instrumentos da política de concorrência e a legislação anti-trust para assegurar um mercado funcional e desmantelar este monopólio; apela a estes intervenientes para que evitem que sítios Web de desinformação sejam financiados através dos seus serviços de publicidade; felicita as

---

<sup>16</sup> [https://disinformationindex.org/wp-content/uploads/2020/03/GDI\\_Adtech\\_EU.pdf](https://disinformationindex.org/wp-content/uploads/2020/03/GDI_Adtech_EU.pdf)

organizações dedicadas à sensibilização para esta questão preocupante; sublinha que os anunciantes devem ter o direito de saber e de decidir onde os seus anúncios são exibidos e de saber quem foram os corretores que trataram os seus dados; solicita o estabelecimento de um processo de mediação que permita o reembolso dos anunciantes quando os anúncios forem colocados em sítios Web que promovam a desinformação;

63. Realça que a versão atualizada do Código de Conduta sobre Desinformação, o Regulamento Serviços Digitais, o Regulamento Mercados Digitais e outras medidas relacionadas com o Plano de Ação para a Democracia Europeia exigirão um mecanismo eficaz de análise, avaliação e aplicação de sanções após a sua adoção, de modo a avaliar regularmente a sua aplicação a nível nacional e da UE, a identificar e corrigir lacunas sem demora e a sancionar o cumprimento incorreto e o incumprimento dos compromissos; apela, neste contexto, à nomeação de coordenadores dos serviços digitais fortes e capazes em cada Estado-Membro, bem como à disponibilização de recursos suficientes para permitir que o braço de execução da Comissão desempenhe as atribuições previstas no Regulamento Serviços Digitais; salienta, além disso, a importância de garantir que as plataformas em linha sejam objeto de auditorias independentes certificadas pela Comissão; observa que, para garantir a independência dos auditores, estes não podem ser financiados por plataformas individuais;
64. Solicita, neste contexto, que sejam definidos indicadores-chave de desempenho (ICD) objetivos, através da correção, para garantir a verificabilidade das medidas tomadas pelas plataformas, bem como dos seus efeitos; sublinha que estes ICD devem incluir parâmetros específicos por país, tais como o público-alvo da desinformação, a participação (taxa de cliques, etc.), o financiamento de atividades de verificação de factos e de investigação no país, bem como a prevalência e a força das relações da sociedade civil no país;
65. Manifesta profunda preocupação com a falta de transparência na revisão do Código de Conduta sobre Desinformação, pois, o debate foi deixado em grande parte ao setor privado e à Comissão; lamenta que o Parlamento Europeu, em particular a Comissão Especial INGE, e outras partes interessadas fundamentais não tenham sido devidamente consultados durante o processo de revisão do Código de Conduta sobre Desinformação;
66. Lamenta que o Código de Conduta continue a insistir na autorregulação, uma vez que esta é insuficiente quando se trata de proteger o público contra as tentativas de ingerência e manipulação; manifesta a sua preocupação pelo facto de a versão atualizada do Código de Conduta sobre Desinformação poder não ser capaz de dar resposta aos desafios que se avizinham; manifesta a sua apreensão quanto à forma como as Orientações para reforçar o Código de Conduta sobre Desinformação se apoiam na proposta da Comissão relativa a um Regulamento Serviços Digitais; solicita que sejam tomadas rapidamente medidas para que o Código de Conduta preveja compromissos vinculativos para as plataformas, a fim de garantir a preparação da UE antes das próximas eleições autárquicas, regionais, nacionais e europeias;
67. Insta a UE a proteger e incentivar o diálogo no seio da comunidade tecnológica e o intercâmbio de informações sobre o comportamento e as estratégias das plataformas sociais; considera que só uma comunidade tecnológica aberta pode reforçar a opinião pública contra ataques, manipulações e ingerências; solicita que se estude a

possibilidade de criar um centro de partilha e análise de informações (ISAC) público-privado para a desinformação, cujos membros rastreiem, rotulem e partilhem informações sobre ameaças em termos de conteúdos de desinformação e sobre os respetivos agentes de divulgação, de acordo com uma classificação das ameaças; considera que este centro poderia informar o sistema de alerta rápido da UE e o mecanismo do G7 e beneficiaria também os intervenientes mais pequenos e com menos recursos; solicita também que se defina uma norma, a nível do setor, sobre desinformação no contexto dos serviços publicitários e dos serviços de monetização em linha, para desmonetizar os conteúdos nocivos, que seja igualmente utilizada pelos sistemas de pagamento em linha e pelas plataformas de comércio eletrónico e auditada por terceiros;

68. Salaria a necessidade de o Código poder funcionar como um instrumento eficaz até à entrada em vigor do Regulamento Serviços Digitais (RSD); considera que o Código deve antecipar algumas das obrigações do RSD e obrigar os signatários a aplicar uma série de disposições do RSD relativas ao acesso dos investigadores e das entidades reguladoras aos dados, bem como à transparência da publicidade, inclusive dos algoritmos e dos sistemas de recomendação; exorta os signatários a assegurarem a auditoria do cumprimento destas obrigações por um auditor independente e solicita a publicação dos relatórios de auditoria correspondentes;
69. Lamenta a falta de transparência do processo de controlo do cumprimento do Código, bem como o calendário da revisão do Código, que estará finalizada antes das conclusões da Comissão Especial INGE; observa que, no mínimo, as ordens do dia das reuniões, as notas finais e as listas de presenças devem ser divulgadas publicamente; exorta os signatários a prestarem declarações ao Parlamento relativas aos compromissos assumidos no âmbito do Código e à forma como cumpriram e cumprirão esses compromissos;
70. Considera que as entidades reguladoras independentes dos meios de comunicação social, como o Grupo de Reguladores Europeus dos Serviços de Comunicação Social Audiovisual, podem vir a desempenhar um papel crucial no controlo e na aplicação do Código;
71. Acolhe favoravelmente a proposta de criação de um grupo de trabalho prevista nas Orientações da Comissão para reforçar o Código de Conduta sobre Desinformação; insiste em que a Comissão convide representantes do Parlamento, das entidades reguladoras nacionais e de outras partes interessadas, incluindo a sociedade civil e a comunidade científica, a integrar esse grupo de trabalho;

### ***Infraestruturas críticas e setores estratégicos***

72. Considera que, dada a sua natureza interligada e transfronteiriça, as infraestruturas críticas são cada vez mais vulneráveis a interferências externas e entende que o quadro atualmente em vigor deve ser revisto; congratula-se, por conseguinte, com a proposta da Comissão relativa a uma nova diretiva para reforçar a resiliência das entidades críticas que prestam serviços essenciais na União Europeia;
73. Recomenda que os Estados-Membros mantenham a prerrogativa de identificar as entidades críticas, mas salienta que a coordenação a nível da UE é necessária,

designadamente, para:

- a) reforçar os canais de ligação e de comunicação utilizados por vários intervenientes, nomeadamente para a segurança geral das missões e operações da UE,
  - b) apoiar as autoridades competentes dos Estados-Membros através do Grupo para a Resiliência das Entidades Críticas, garantindo uma participação diversificada das partes interessadas e, em particular, a participação efetiva das pequenas e médias empresas (PME), das organizações da sociedade civil e dos sindicatos,
  - c) promover o intercâmbio de boas práticas, não só entre os Estados-Membros, mas também a nível regional e local, inclusivamente com os países dos Balcãs Ocidentais, e entre proprietários e operadores de infraestruturas críticas, nomeadamente através da comunicação interserviços, de molde a identificar os desenvolvimentos numa fase precoce e desenvolver contramedidas adequadas,
  - d) aplicar uma estratégia comum de resposta aos ciberataques contra infraestruturas críticas;
74. Recomenda que a lista de entidades críticas seja alargada de modo a incluir as infraestruturas eleitorais digitais e os sistemas educativos, dada a sua importância essencial para garantir o funcionamento e a estabilidade da UE e dos seus Estados-Membros a longo prazo, e que seja permitida flexibilidade no que diz respeito à decisão sobre o aditamento à lista de novos setores estratégicos a proteger;
75. Apela a uma abordagem global da UE para fazer face às ameaças híbridas aos processos eleitorais e melhorar a coordenação e a cooperação entre os Estados-Membros; insta a Comissão a avaliar de forma crítica a dependência das plataformas e da infraestrutura de dados no contexto das eleições; considera que existe uma falta de controlo democrático sobre o setor privado; apela a um maior controlo democrático das plataformas, incluindo o acesso adequado aos dados e aos algoritmos por parte das autoridades competentes;
76. Recomenda que as obrigações decorrentes da proposta de diretiva, incluindo as avaliações das ameaças, riscos e vulnerabilidades à escala da UE e por país, reflitam os mais recentes desenvolvimentos e fiquem a cargo do Centro Comum de Investigação em conjunto com o INTCEN do SEAE; salienta que são necessários recursos suficientes para estas instituições estarem em condições de realizar as análises mais avançadas, com um forte controlo democrático, o que não deve excluir uma avaliação prévia por parte da FRA para garantir o respeito pelos direitos fundamentais;
77. Considera que a UE e os seus Estados-Membros têm de disponibilizar alternativas de financiamento aos países dos Balcãs Ocidentais que são candidatos à adesão à UE e a outros países potencialmente candidatos nos quais países terceiros tenham utilizado os investimentos diretos estrangeiros (IDE) como instrumento geopolítico para aí aumentar a sua influência, se se pretender impedir que uma grande parte das infraestruturas críticas da UE e dos países candidatos fique na posse de países terceiros, como é o caso do porto do Pireu na Grécia e como acontece atualmente com os investimentos chineses em cabos submarinos nos mares Báltico e Mediterrâneo e no Ártico; regozija-se, por

consequente, com o Regulamento Análise dos IDE enquanto instrumento importante para coordenar as ações dos Estados-Membros em matéria de investimentos estrangeiros, e apela a um quadro regulamentar mais sólido e a uma aplicação mais rigorosa desse quadro para garantir que sejam bloqueados os IDE lesivos para a segurança da UE, tal como especificado no regulamento, e que sejam transferidas para as instituições da UE mais competências de análise dos IDE; apela ao abandono do princípio da proposta mais baixa nas decisões de investimento público; apela a todos os Estados-Membros que não disponham de mecanismos de análise dos investimentos para que adotem tais medidas; entende que o quadro deve estar mais bem interligado com análises independentes realizadas por institutos nacionais e da UE ou por outras partes interessadas, como grupos de reflexão, para fazer um levantamento dos fluxos de IDE e proceder à análise desses fluxos; entende que poderá também ser adequado incluir outros setores estratégicos no quadro, como a tecnologia 5G e outras tecnologias da informação e comunicação (TIC), para limitar a dependência da UE e dos seus Estados-Membros de fornecedores de alto risco; sublinha que esta abordagem deve aplicar-se igualmente aos países candidatos e potencialmente candidatos;

78. Está convicto de que a UE enfrenta mais desafios em resultado da sua falta de investimento no passado, que contribuiu para a sua dependência de fornecedores de tecnologia estrangeiros; recomenda que se protejam as cadeias de produção e de abastecimento de infraestruturas críticas e de material crítico na UE; entende que a evolução da UE no sentido de uma autonomia estratégica aberta e soberania digital é importante e é o caminho certo a seguir; salienta que a UE deverá utilizar novos instrumentos para reforçar a sua posição geopolítica, incluindo um instrumento antioerção; considera que o Regulamento Circuitos Integrados anunciado pela Comissão, que visa assegurar que as peças essenciais para a produção de circuitos integrados sejam fabricadas na UE, constitui um passo importante para limitar a dependência de países terceiros, como a China e os EUA; considera que o investimento na produção de circuitos integrados deve ser feito de forma coordenada em toda a União e com base numa análise do lado da procura, por forma a evitar uma corrida às subvenções públicas nacionais e a fragmentação do mercado único; exorta, por conseguinte, a Comissão a criar um fundo europeu específico para os semicondutores, que apoie a criação da mão de obra qualificada necessária e compense os custos de estabelecimento mais elevados de instalações de conceção e fabrico na UE; considera que Taiwan é um parceiro importante para impulsionar a produção de semicondutores na UE;
79. Apela a um maior desenvolvimento das redes europeias de infraestruturas de dados e de prestadores de serviços com normas de segurança europeias, como a GAIA-X, que é um passo importante para criar alternativas viáveis aos prestadores de serviços atuais e no sentido de uma economia digital aberta, transparente e segura; sublinha a necessidade de reforçar as PME e de evitar a cartelização do mercado da computação em nuvem; recorda que os centros de dados são infraestruturas críticas; manifesta a sua preocupação com a influência de países terceiros e das suas empresas no desenvolvimento da GAIA-X;
80. Sublinha que a integridade, disponibilidade e confidencialidade das redes públicas de comunicações eletrónicas, como as estruturas de base da Internet e os cabos submarinos de comunicações, têm um interesse vital para a segurança; insta a Comissão e os

Estados-Membros a prevenirem a sabotagem e a espionagem nessas redes de comunicação e a promoverem a utilização de normas de encaminhamento seguras e interoperáveis, a fim de garantir a integridade e a robustez das redes e serviços de comunicações eletrónicas, designadamente através da recente Estratégia Global Gateway;

81. Exorta a Comissão a propor medidas para criar um aprovisionamento seguro, sustentável e equitativo das matérias-primas utilizadas para produzir componentes e tecnologias críticas, incluindo baterias e equipamentos, a tecnologia 5G e tecnologias subsequentes, e produtos químicos e farmacêuticos, salientando simultaneamente a importância do comércio mundial, da cooperação internacional, no pleno respeito dos direitos dos trabalhadores, e do ambiente natural, e através da aplicação das normas internacionais em matéria social e de sustentabilidade no que diz respeito à utilização dos recursos; recorda a necessidade de conceder o financiamento necessário à investigação e ao desenvolvimento para encontrar substitutos adequados em caso de perturbação da cadeia de aprovisionamento;

### *Ingerência estrangeira durante processos eleitorais*

82. Apela a que a proteção do processo eleitoral no seu conjunto seja considerada uma questão essencial de segurança a nível da UE e a nível nacional, porquanto as eleições livres e justas estão no cerne do processo democrático; solicita à Comissão que desenvolva um quadro de resposta mais eficaz para combater a ingerência estrangeira nos processos eleitorais, que, entre outras medidas, deve consistir em canais de comunicação direta com os cidadãos;
83. Saliencia a necessidade de promover a resiliência da sociedade contra a desinformação durante os processos eleitorais, inclusive no setor privado e no meio académico, e de adotar uma abordagem holística através da qual esta ingerência deve ser combatida de forma constante, desde os programas de ensino nas escolas à integridade técnica e fiabilidade do voto, bem como através de medidas estruturais para combater a natureza híbrida dessa ingerência; apela, em particular, à adoção de um plano para preparar as eleições europeias de 2024, que deve incluir uma estratégia, formação e sensibilização dos partidos políticos europeus e do seu pessoal, bem como medidas de segurança reforçadas para prevenir a ingerência estrangeira;
84. Considera que as informações erradas e a desinformação através das redes sociais são um problema crescente para a integridade eleitoral; defende que as plataformas de redes sociais devem assegurar a aplicação e o bom funcionamento de políticas destinadas a proteger a integridade das eleições; considera alarmante a recente descoberta de que empresas privadas estão a ser contratadas por intervenientes mal-intencionados para interferirem em eleições, propagarem narrativas falsas e promoverem conspirações virais, principalmente nas redes sociais; apela a uma investigação aprofundada sobre a forma de combater o fenómeno de «contratação de desinformação», que está a tornar-se cada vez mais sofisticado e comum em todo o mundo;
85. Saliencia a extrema importância das missões de observação eleitoral na prestação de informações pertinentes e na formulação de recomendações específicas para tornar o sistema eleitoral mais resiliente e ajudar a combater a ingerência estrangeira nos

processos eleitorais; solicita que os processos eleitorais sejam melhorados e reforçados, uma vez que as missões de observação eleitoral são um instrumento fundamental na luta contra o crescente recurso a processos eleitorais desleais e fraudulentos por regimes não liberais que pretendem fazer-se passar por democráticos; destaca, neste contexto, a necessidade de reavaliar e atualizar os instrumentos e métodos utilizados na observação eleitoral internacional a fim de fazer face a novas tendências e ameaças, incluindo a luta contra falsos observadores eleitorais, o intercâmbio de boas práticas com parceiros que partilham as mesmas ideias e uma colaboração mais estreita com organizações internacionais pertinentes, como a Organização para a Segurança e a Cooperação na Europa (OSCE) e o Conselho da Europa, e com todos os intervenientes relevantes no âmbito da Declaração dos Princípios de Observação Eleitoral Internacional e do Código de Conduta do Observador Eleitoral Internacional; salienta que a participação de deputados ao Parlamento Europeu em missões de observação eleitoral não autorizadas compromete a credibilidade e a reputação do Parlamento Europeu; acolhe favoravelmente e recomenda a plena aplicação do procedimento do Grupo de Apoio à Democracia e de Coordenação Eleitoral para «casos de observação eleitoral individual não oficial por deputados ao Parlamento Europeu» (adotado em 13 de dezembro de 2018), que permite a exclusão dos deputados das delegações oficiais de observação eleitoral do Parlamento durante o mandato;

### ***Financiamento encoberto de atividades políticas por doadores estrangeiros***

86. Salienta que, embora continue a ser necessário compreender melhor os efeitos do financiamento encoberto de atividades políticas, por exemplo, sobre as tendências antidemocráticas na Europa, o financiamento estrangeiro de atividades políticas através de operações encobertas não deixa de representar uma grave violação da integridade do funcionamento democrático da UE e dos seus Estados-Membros, em particular durante os períodos eleitorais, violando, por conseguinte, o princípio da realização de eleições livres e justas; salienta, por conseguinte, que, em todos os Estados-Membros, devem ser consideradas ilegais quaisquer atividades encobertas financiadas por intervenientes estrangeiros que visem influenciar o processo da política europeia ou nacional; observa, a este respeito, que países como a Austrália adotaram legislação que proíbe a ingerência estrangeira na política;
87. Condena o facto de partidos extremistas, populistas e antieuropeus e determinados partidos e indivíduos estarem implicados nas tentativas de interferência nos processos democráticos da União e serem explicitamente cúmplices, e manifesta a sua apreensão pelo facto de estes partidos e indivíduos serem utilizados como porta-vozes da ingerência levada a cabo por intervenientes estrangeiros a fim de legitimar os seus governos autoritários; apela à clarificação total das relações políticas e económicas entre estes partidos e indivíduos e a Rússia; entende que estas relações são altamente inadequadas e condena a cumplicidade que, na prossecução de objetivos políticos, pode expor a UE e os seus Estados-Membros a ataques de potências estrangeiras;
88. Insta os Estados-Membros, aquando de uma maior harmonização das regulamentações nacionais, a proibirem os donativos estrangeiros e a colmatarem, em particular, as seguintes lacunas:
  - a) contribuições em espécie de intervenientes estrangeiros para partidos políticos,



fundações, pessoas que exercem cargos públicos ou funcionários eleitos, incluindo empréstimos financeiros concedidos por pessoas singulares ou coletivas estabelecidas fora da UE e do Espaço Económico Europeu (EEE) (exceto eleitores europeus), donativos anónimos acima de um determinado limiar e a ausência de limites de despesa para as campanhas políticas, o que permite que estas sejam influenciadas através de grandes donativos; os políticos, intervenientes ou partidos a quem tenha sido proposto e/ou que tenham aceite uma contribuição financeira ou em espécie por parte de um interveniente estrangeiro devem ser obrigados a notificar as autoridades competentes desse facto e esta informação deve, por seu turno, ser comunicada a nível da UE para permitir um controlo à escala da UE;

- b) testas de ferro com cidadania nacional<sup>17</sup>: a transparência dos doadores, sejam eles pessoas singulares ou coletivas, deve ser garantida através de declarações de conformidade que atestem o estatuto do doador e mediante a atribuição de maiores poderes de execução às comissões eleitorais; os donativos provenientes da UE que excedam um determinado limiar mínimo devem ser inscritos num registo oficial e público e estar associados a uma pessoa singular, devendo ser fixado um limite máximo para os donativos por parte de pessoas singulares e coletivas (e subsídios) a partidos políticos;
- c) empresas fictícias e filiais nacionais de empresas-mãe estrangeiras<sup>18</sup>: as empresas fictícias devem ser proibidas e devem ser estabelecidos requisitos mais sólidos para revelar as origens do financiamento através das empresas-mãe; o financiamento e os donativos a partidos políticos que excedam um determinado limiar devem ser registados num registo público e central com um nome e um endereço oficiais que possam ser associados a uma pessoa real, e os Estados-Membros devem recolher essas informações; insta a Comissão a assegurar que as autoridades dos Estados-Membros tenham o direito de investigar as origens do financiamento para verificar as informações das filiais nacionais e resolver o problema da insuficiência de dados nos registos nacionais, especialmente em situações em que é utilizada uma rede de empresas fictícias;
- d) terceiros e organizações sem fins lucrativos<sup>19</sup>, coordenadas por intervenientes estrangeiros e criadas com vista a influenciar os processos eleitorais: deve ser ponderada a possibilidade de se adotarem regras mais uniformes e de garantir a transparência em toda a UE para as organizações que tencionem financiar atividades políticas nos casos em que estas pretendam influenciar diretamente processos eleitorais como eleições ou campanhas para referendos; essas regras não deverão impedir as organizações sem fins lucrativos e terceiros de receberem financiamento para campanhas sobre questões específicas; as regras que garantem a transparência do financiamento ou dos donativos devem também aplicar-se às fundações políticas;

---

<sup>17</sup> Pessoa que doa, em seu próprio nome, o dinheiro de outrem a um partido político ou candidato.

<sup>18</sup> Esta lacuna abrange duas realidades diferentes: as empresas fictícias, que não exercem atividades comerciais reais e servem apenas para encobrir o financiamento, e as filiais nacionais de empresas-mãe estrangeiras utilizadas para canalizar fundos para a política.

<sup>19</sup> As organizações sem fins lucrativos e os terceiros não são obrigados a revelar a identidade dos seus doadores, mas estão autorizados a financiar partidos políticos e candidatos em vários Estados-Membros da UE.

- e) anúncios de teor político em linha, uma vez que não estão sujeitos às regras em matéria de publicidade na televisão, na rádio e na imprensa e geralmente não estão regulamentados a nível da UE: por conseguinte, é necessário proibir anúncios adquiridos por intervenientes de fora da UE e do EEE e garantir total transparência no que diz respeito à aquisição de anúncios de teor político em linha por intervenientes da UE; salienta a necessidade de assegurar uma transparência e uma responsabilização democrática muito maiores relativamente à utilização de algoritmos; congratula-se com o anúncio, pela Comissão, de uma nova proposta legislativa sobre a transparência dos conteúdos políticos patrocinados, tal como proposto no Plano de Ação para a Democracia Europeia, que deve ter por objetivo evitar uma manta de retalhos de 27 legislações nacionais em matéria de publicidade política em linha e permitirá garantir que os partidos da UE possam fazer campanha em linha antes das eleições europeias, limitando simultaneamente o risco de ingerência estrangeira e explorando quais as regras voluntariamente adotadas pelos partidos políticos em cada Estado-Membro e pelas principais plataformas de redes sociais que podem vir a constituir regras aplicáveis à escala da UE; insta os Estados-Membros a atualizarem as respetivas regulamentações nacionais em matéria de publicidade política, que não acompanharam a evolução constante no sentido de transformar o meio digital no principal meio de comunicação política; exorta a Comissão a propor uma forma de definir democraticamente a publicidade política temática, com vista a pôr termo a uma situação em que plataformas privadas com fins lucrativos decidem o que é ou não temático;
- f) controlo das despesas eleitorais, efetuado por auditores independentes, a quem devem ser disponibilizadas atempadamente informações sobre as despesas e os donativos, atenuando assim riscos como os conflitos de interesses e a representação dos grupos de interesses relacionados com o financiamento político; ao estabelecerem uma divulgação proativa, as instituições responsáveis pela regulamentação financeira devem ter um mandato claro, bem como a capacidade, os recursos e o poder legal para conduzir investigações e remeter processos para ação penal;
89. Insta, por conseguinte, a Comissão a analisar o financiamento encoberto na UE e a apresentar propostas concretas destinadas a colmatar todas as lacunas que permitem o financiamento opaco de partidos políticos e fundações políticas ou funcionários eleitos por fontes de países terceiros e a propor normas comuns da UE aplicáveis às leis eleitorais nacionais em todos os Estados-Membros; entende que os Estados-Membros devem ter por objetivo introduzir requisitos de transparência claros relativamente ao financiamento de partidos políticos, assim como a proibição dos donativos a partidos políticos e a políticos individuais provenientes de fora da UE e do EEE, com exceção dos eleitores europeus que vivem fora da UE e do EEE, e estabelecer uma estratégia clara em relação ao sistema de sanções; exorta a Comissão e os Estados-Membros a criarem uma autoridade da UE para controlos financeiros destinados a combater práticas financeiras ilícitas e ingerências da Rússia e de outros regimes autoritários; salienta a necessidade de proibir os donativos ou os financiamentos efetuados com recurso a tecnologias emergentes que são extremamente difíceis de rastrear; solicita aos Estados-Membros e à Comissão que atribuam mais recursos e mandatos mais fortes às agências de supervisão com vista a assegurar uma melhor qualidade dos dados;

90. Compromete-se a assegurar que todas as organizações sem fins lucrativos, grupos de reflexão, institutos e ONG que, no decurso dos trabalhos parlamentares, contribuam para o desenvolvimento da política da UE ou tenham um papel consultivo no processo legislativo sejam totalmente transparentes, independentes e isentos de conflitos de interesses no que respeita ao seu financiamento e à sua propriedade;
91. Acolhe com agrado a revisão em curso do Regulamento (UE, Euratom) n.º 1141/2014 relativo ao estatuto e ao financiamento dos partidos políticos europeus e das fundações políticas europeias; apoia todos os esforços para alcançar um maior grau de transparência no financiamento das atividades dos partidos políticos europeus e das fundações políticas europeias, em particular antes das eleições europeias de 2024, incluindo a proibição de todos os donativos provenientes de fora da UE e de fontes anónimas, com exceção das diásporas dos Estados-Membros da UE, bem como de donativos provenientes de fora da UE que não possam ser documentados por meio de contratos, acordos de serviço ou pagamento de quotas relacionadas com a filiação num partido político europeu, permitindo, no entanto, que membros de partidos nacionais que se encontrem fora da UE e do EEE paguem as suas quotas a partidos políticos europeus; exorta os partidos políticos europeus e nacionais a empenharem-se no combate à ingerência estrangeira e à propagação da desinformação, tornando-se signatários de uma Carta que preveja compromissos específicos a este respeito;
92. Salaria que a aplicação de muitas das recomendações do GRECO do Conselho da Europa e da Comissão de Veneza permitiria reforçar a imunidade do sistema político dos Estados-Membros e da União no seu conjunto face à influência financeira estrangeira;

### ***Cibersegurança e resiliência contra ciberataques***

93. Exorta as instituições da UE e os Estados-Membros a aumentarem rapidamente os investimentos nas cibercapacidades e cibercompetências estratégicas da UE, como a IA, a comunicação segura e a infraestrutura de dados e de computação em nuvem, para detetar, expor e combater a ingerência estrangeira a fim de melhorar a cibersegurança da UE, garantindo ao mesmo tempo o respeito pelos direitos fundamentais; exorta também a Comissão a aumentar o investimento no aprofundamento dos conhecimentos digitais e das competências técnicas da UE, por forma a compreender melhor os sistemas digitais utilizados em toda a UE; insta a Comissão a afetar recursos adicionais, humanos, materiais e financeiros, às capacidades de análise de ciberameaças, nomeadamente o INTCEN do SEAE, e à cibersegurança dos Estados-Membros e das instituições, órgãos e organismos da UE, nomeadamente a ENISA e a Equipa de Resposta a Emergências Informáticas para as instituições e agências da UE (CERT-UE); lamenta a falta de cooperação e harmonização em matéria de cibersegurança entre os Estados-Membros;
94. Acolhe favoravelmente as propostas da Comissão referentes a uma nova estratégia de cibersegurança e a uma nova diretiva relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União Europeia e que revoga a Diretiva (UE) 2016/1148<sup>20</sup> (SRI 2); recomenda que o resultado final dos trabalhos em curso sobre a proposta aborde as lacunas da Diretiva SRI de 2016, nomeadamente através do

---

<sup>20</sup> Proposta de diretiva do Parlamento Europeu e do Conselho relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União e que revoga a Diretiva (UE) 2016/1148 (COM(2020)0823).

reforço dos requisitos de segurança, do alargamento do seu âmbito de aplicação, da criação de um quadro para a cooperação europeia e a partilha de informações, do reforço das capacidades dos Estados-Membros em matéria de cibersegurança, do desenvolvimento da cooperação público-privada, da introdução de requisitos de execução mais rigorosos e da transformação da cibersegurança numa responsabilidade ao mais alto nível de gestão das entidades europeias que são vitais para a nossa sociedade; salienta a importância de alcançar um elevado nível comum de cibersegurança em todos os Estados-Membros, de molde a limitar os pontos fracos da cibersegurança conjunta da UE; sublinha a necessidade fundamental de assegurar a resiliência dos sistemas de informação e congratula-se, a este respeito, com a Rede de Organizações de Coordenação de Cibercrises (CyCLONe); incentiva uma maior promoção das medidas de reforço de capacidades da OSCE para o ciberespaço;

95. Regozija-se com a proposta da Comissão incluída na SRI2 de realização de avaliações coordenadas dos riscos de segurança das cadeias de aprovisionamento críticas, à semelhança do seu conjunto de instrumentos da UE para a tecnologia 5G, de forma a ter devidamente em conta os riscos associados, por exemplo, à utilização de *software* e *hardware* produzidos por empresas sob o controlo de Estados estrangeiros; exorta a Comissão a desenvolver normas e regras de concorrência mundiais para a tecnologia 6G, em consonância com os valores democráticos; insta a Comissão a promover intercâmbios entre as instituições da UE e as autoridades nacionais sobre os desafios, as boas práticas e as soluções relacionadas com as medidas do conjunto de instrumentos; entende que a UE deve investir mais nas suas capacidades no domínio das tecnologias 5G e pós-5G, a fim de reduzir a dependência de fornecedores estrangeiros;
96. Salienta que a cibercriminalidade não conhece fronteiras e insta a UE a intensificar os seus esforços internacionais para a combater eficazmente; assinala que a UE deve assumir a liderança na elaboração de um tratado internacional sobre cibersegurança que estabeleça normas internacionais em matéria de cibersegurança para combater a cibercriminalidade;
97. Acolhe com agrado o anúncio da elaboração de uma Diretiva Ciber-Resiliência que complemente uma política europeia de ciberdefesa, uma vez que os domínios do ciberespaço e da defesa estão estreitamente relacionados; solicita um maior investimento no reforço da coordenação e das capacidades europeias no domínio da ciberdefesa; recomenda que o reforço das cibercapacidades dos nossos parceiros seja promovido através de missões de formação da UE ou de cibermissões civis; sublinha a necessidade de harmonizar e normalizar a formação relacionada com o ciberespaço e apela a um financiamento estrutural da UE neste domínio;
98. Condena a utilização ilícita e em larga escala do *software* de vigilância Pegasus da empresa NSO Group Technologies por entidades estatais, nomeadamente de Marrocos, da Arábia Saudita, da Hungria, da Polónia, do Barém, dos Emirados Árabes Unidos e do Azerbaijão, contra jornalistas, defensores dos direitos humanos e políticos; recorda que o Pegasus é apenas um dos inúmeros exemplos de programas que são utilizados de forma abusiva por entidades estatais para fins de vigilância ilícita em larga escala visando cidadãos inocentes; condena igualmente outras operações de espionagem estatal dirigidas a políticos europeus; exorta a Comissão a elaborar uma lista de *software* ilícito de vigilância e a atualizar continuamente essa lista; apela à UE e aos Estados-Membros

para que utilizem esta lista para assegurar o dever de diligência em matéria de direitos humanos e o controlo adequado das exportações de tecnologia de vigilância europeia e de assistência técnica e das importações para os Estados-Membros que representam um risco claro para o Estado de direito; apela, além disso, à criação de um Laboratório de Cidadãos da UE, semelhante ao instituído no Canadá, composto por jornalistas, peritos em direitos humanos e peritos em engenharia inversa de *software* mal-intencionado, que se dedicaria a detetar e expor a utilização ilegal de *software* para fins de vigilância ilícita;

99. Insta a UE a adotar um quadro regulamentar sólido neste domínio, tanto a nível da UE como a nível internacional; saúda, neste contexto, a decisão do Gabinete da Indústria e da Segurança do Departamento do Comércio dos EUA de colocar na lista negra a empresa NSO Group Technologies, proibindo assim a empresa de receber tecnologias americanas;
100. Manifesta a sua preocupação pelo facto de a UE cooperar em questões judiciais e de aplicação da lei com países terceiros que estiveram envolvidos com a empresa NSO Group e que utilizam o *software* espião Pegasus para espiar cidadãos da UE; apela a salvaguardas adicionais e a um reforço do controlo democrático dessa cooperação;
101. Exorta a Comissão a analisar os investimentos da UE na empresa NSO Group Technologies e a adotar medidas específicas contra os Estados estrangeiros que utilizem *software* para espiar cidadãos da UE ou pessoas que beneficiem do estatuto de refugiado em países da UE;
102. Manifesta a sua preocupação pelo facto de jornalistas e ativistas da democracia poderem ser ilegalmente mantidos sob vigilância e assediados pelos regimes autoritários a que procuraram escapar, mesmo em território da UE, e considera que tal representa uma grave violação dos valores fundamentais da União e dos direitos fundamentais dos indivíduos, consagrados na Carta dos Direitos Fundamentais, na Convenção Europeia dos Direitos Humanos (CEDH) e no Pacto Internacional sobre os Direitos Cívicos e Políticos; lamenta a falta de apoio jurídico às vítimas deste *software* de espionagem;
103. Realça a necessidade urgente de reforçar o quadro legislativo, de modo a responsabilizar as pessoas que distribuem e utilizam de forma abusiva esse *software* para fins ilícitos e não autorizados; remete, em particular, para as sanções impostas em 21 de junho de 2021 a Alexander Shatrov, diretor-executivo de uma empresa bielorrussa que produz *software* de reconhecimento facial utilizado por um regime autoritário, por exemplo, para identificar manifestantes da oposição política; exorta a Comissão a impedir qualquer utilização ou financiamento na UE de tecnologias de vigilância ilegais; apela à UE e aos Estados-Membros para que colaborem com os governos dos países terceiros para pôr termo às práticas e à legislação repressivas em matéria de cibersegurança e de luta contra o terrorismo, sob um controlo democrático reforçado; apela a uma investigação, por parte das autoridades competentes da UE, sobre a utilização ilícita de *software* espião na UE e a exportação desse *software* a partir da UE, bem como sobre as repercussões nos Estados-Membros e países associados, incluindo os que participam em programas da UE, que adquiriram e utilizaram o *software* espião e a partir dos quais este foi exportado para visar ilegalmente jornalistas, defensores dos direitos humanos, advogados e políticos;

104. Apela a uma revisão ambiciosa da Diretiva Privacidade Eletrónica<sup>21</sup>, de molde a reforçar a confidencialidade das comunicações e dos dados pessoais aquando da utilização de dispositivos eletrónicos, sem reduzir o grau de proteção proporcionado pela diretiva e sem prejuízo da responsabilidade dos Estados-Membros de salvaguardar a segurança nacional; salienta que as autoridades públicas devem ser obrigadas a divulgar as vulnerabilidades que detem nos dispositivos informáticos; exorta a UE e os Estados-Membros a reforçarem a coordenação das suas ações com base na Diretiva relativa a ataques contra os sistemas de informação<sup>22</sup> a fim de garantir que o acesso ilegal aos sistemas de informação e a interceção ilegal sejam definidos como infrações penais e penalizados com as sanções adequadas; recorda que toda e qualquer violação da confidencialidade para fins de segurança nacional deve ser cometida legalmente e para fins explícitos e legítimos numa sociedade democrática, com base na estrita necessidade e proporcionalidade, tal como exigido pelo Tribunal Europeu dos Direitos Humanos (TEDH) e pelo Tribunal de Justiça da União Europeia;

#### ***Proteção dos Estados-Membros, instituições, agências, delegações e missões da UE***

105. Sublinha que as instituições, órgãos, organismos, delegações, missões, operações, redes, edifícios e pessoal da UE constituem um alvo para todos os tipos de ameaças e ataques híbridos por parte de intervenientes estatais estrangeiros, pelo que devem ser devidamente protegidos, prestando especial atenção aos ativos, instalações e atividades do SEAE no estrangeiro, assim como à segurança do pessoal da UE delegado em países não democráticos com regimes repressivos; solicita uma resposta estruturada a estas ameaças por parte das missões da PCSD, bem como um apoio mais concreto a essas missões através de uma comunicação estratégica; reconhece o aumento constante dos ataques patrocinados por intervenientes estatais contra as instituições, órgãos e organismos da UE, inclusive contra a EMA e as instituições e autoridades públicas dos Estados-Membros;
106. Apela a uma revisão exaustiva e periódica de todos os serviços, redes, equipamento e *hardware* das instituições, órgãos, organismos, delegações, missões e operações da UE, a fim de reforçar a sua resiliência às ameaças à cibersegurança e excluir programas e dispositivos potencialmente perigosos, como os desenvolvidos pelo Kaspersky Lab; exorta as instituições da UE e os Estados-Membros a garantirem uma orientação adequada e ferramentas seguras para o pessoal; frisa a necessidade de sensibilizar as instituições e as administrações para o recurso a redes e a serviços seguros, inclusivamente durante as missões; assinala as vantagens em matéria de confiança e segurança dos sistemas operativos de rede de fonte aberta, amplamente utilizados por agências militares e governamentais aliadas;
107. Destaca a importância de uma coordenação eficaz, oportuna e estreita entre as diferentes instituições, órgãos e organismos da UE especializados em cibersegurança, como a CERT-UE, cujas capacidades operacionais devem ser desenvolvidas, bem como a

---

<sup>21</sup> Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (JO L 201 de 31.7.2002, p. 37).

<sup>22</sup> 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 (JO L 218 de 14.8.2013, p. 8).

ENISA e a futura ciberunidade conjunta, que assegurará uma resposta coordenada a ameaças de cibersegurança em grande escala na UE; congratula-se com a atual cooperação estruturada entre a CERT-UE e a ENISA; congratula-se igualmente com a criação do grupo de trabalho da UE sobre ciberinformações no âmbito do UE INTCEN, com vista a promover a cooperação estratégica em matéria de informações; acolhe com agrado as recentes iniciativas dos Secretários-Gerais das instituições da UE no sentido de desenvolver regras comuns em matéria de informação e cibersegurança;

108. Aguarda com expectativa as duas propostas de regulamento da Comissão que estabelecem um quadro normativo para a segurança da informação e a cibersegurança em todas as instituições, órgãos e organismos da UE, e considera que esses regulamentos devem incluir o reforço das capacidades e da resiliência; insta a Comissão e os Estados-Membros a afetarem fundos e recursos adicionais à cibersegurança das instituições da UE a fim de dar resposta aos desafios de um cenário de ameaças em constante evolução;
109. Aguarda com expectativa o Relatório Especial do Tribunal de Contas Europeu sobre a Auditoria da Cibersegurança, previsto para o início de 2022;
110. Apela a uma investigação exaustiva dos casos denunciados de infiltração estrangeira entre o pessoal das instituições da UE; apela a uma análise e possível revisão dos procedimentos em matéria de recursos humanos, incluindo a seleção antes do recrutamento, a fim de colmatar as lacunas que permitem a infiltração estrangeira; insta os órgãos de direção do Parlamento a melhorarem os procedimentos de habilitação de segurança do pessoal e a apertarem as regras e os controlos de acesso às suas instalações, a fim de impedir que pessoas estreitamente ligadas a interesses estrangeiros tenham acesso a reuniões e informações confidenciais; exorta as autoridades belgas a analisarem e atualizarem o quadro nacional de combate à espionagem, a fim de permitir a deteção, a ação penal e a aplicação de sanções eficazes aos infratores; apela à tomada de medidas semelhantes nos outros Estados-Membros para proteger as instituições e organismos da UE no seu território;
111. Exorta todas as instituições da UE a sensibilizarem o seu pessoal através de formação e orientação adequadas a fim de prevenir, atenuar e combater os riscos de segurança em geral e de cibersegurança em particular; apela à formação obrigatória e regular em matéria de segurança e TIC para todo o pessoal (incluindo estagiários) e deputados ao Parlamento Europeu; solicita que seja feito um levantamento e avaliações regulares e específicas dos riscos de influência estrangeira nas instituições;
112. Destaca a necessidade de procedimentos adequados de gestão de crises para os casos de manipulação da informação, incluindo sistemas de alerta entre níveis administrativos e setores, a fim de assegurar a prestação de informações mútuas e impedir que a manipulação da informação se propague; regozija-se, a este respeito, com o Sistema de Alerta Rápido (SAR) e o procedimento de alerta rápido instituídos antes das eleições europeias de 2019 e com os procedimentos em vigor nas administrações da Comissão e do Parlamento para alertar para eventuais casos que afetem as instituições ou os processos democráticos da UE; solicita à administração da UE que reforce o seu controlo, nomeadamente mediante o estabelecimento de um repositório central e de um instrumento de rastreio de incidentes, e que desenvolva um conjunto de instrumentos

comum a ativar em caso de alerta SAR;

113. Solicita regras de transparência obrigatórias para as viagens oferecidas por países e entidades estrangeiros a funcionários das instituições da UE, incluindo deputados ao Parlamento Europeu, APA e assessores dos grupos políticos, bem como a funcionários nacionais, que obriguem à divulgação dos seguintes elementos: o nome do terceiro pagador, o custo da viagem e uma descrição dos motivos subjacentes à viagem; recorda que viagens organizadas desta natureza não podem ser consideradas delegações oficiais do Parlamento e solicita a aplicação de sanções rigorosas caso tal não seja respeitado; salienta que os grupos informais de amizade podem comprometer o trabalho dos órgãos oficiais do Parlamento, bem como lesar a sua reputação e a coerência das suas ações; insta os órgãos de direção do Parlamento a aumentarem a transparência e a responsabilização destes grupos, a aplicarem as regras em vigor e a tomarem as medidas necessárias quando estes grupos de amizade sejam utilizados de forma abusiva por países terceiros; solicita aos Questores que criem e mantenham um registo acessível e atualizado dos grupos de amizade e das declarações;

***Ingerência por parte de intervenientes mundiais através da captação de elites, diásporas nacionais, universidades e eventos culturais***

114. Condena todos os tipos de captação de elites e a técnica de cooptação de altos funcionários públicos e de antigos políticos da UE utilizada por empresas estrangeiras com ligações a governos ativamente envolvidos em ações de ingerência contra a UE, e lamenta a falta de instrumentos e de aplicação necessários para prevenir estas práticas; considera que a divulgação de informações confidenciais obtidas durante mandatos públicos ou no exercício de funções de funcionários públicos, em detrimento dos interesses estratégicos da UE e dos seus Estados-Membros, deve ter consequências legais e dar lugar à imposição de sanções severas, incluindo o despedimento imediato e/ou a inibição de recrutamento futuro pelas instituições; entende que as declarações de rendimentos e de propriedade dessas pessoas devem ser divulgadas ao público;
115. Insta a Comissão a incentivar e coordenar ações contra a captação de elites, nomeadamente complementando e aplicando, sem exceções, os períodos de incompatibilidade dos comissários da UE e dos altos funcionários da UE com um dever de comunicação de informações após esse período, a fim de pôr cobro à prática das «portas giratórias», e com regras estruturadas para combater a captação de elites a nível da UE; insta a Comissão a avaliar se os atuais requisitos de incompatibilidade continuam a adequar-se à sua finalidade; sublinha que os antigos políticos e funcionários da UE devem denunciar casos em que sejam contactados por um Estado estrangeiro a uma entidade de supervisão específica e beneficiar da proteção conferida aos autores de denúncias; insta todos os Estados-Membros a aplicarem e harmonizarem os períodos de incompatibilidade previstos para os seus dirigentes políticos e a assegurarem-se de que dispõem de medidas e sistemas que obriguem os funcionários públicos a declarar as suas atividades externas, empregos, investimentos, ativos e donativos ou benefícios substanciais que possam causar um conflito de interesses;
116. Manifesta a sua preocupação com as estratégias integradas de representação de grupos de interesses que combinam interesses industriais e objetivos políticos estrangeiros, em particular nos casos em que favorecem os interesses de um Estado autoritário; insta, por



consequente, as instituições da UE a reformularem o Registo de Transparência, nomeadamente através da introdução de regras de transparência mais rigorosas, do levantamento do financiamento estrangeiro para atividades de representação de grupos de interesses relacionadas com a UE e da garantia de uma entrada que permita identificar o financiamento proveniente de governos estrangeiros; apela a uma cooperação eficaz nesta matéria entre todas as instituições da UE; considera que o regime australiano de transparência da influência estrangeira é um exemplo de uma boa prática a seguir;

117. Solicita aos Estados-Membros que estudem a possibilidade de criar um regime de registo da influência estrangeira e um registo, gerido pelo governo, das atividades declaradas realizadas para um Estado estrangeiro ou em nome desse Estado, seguindo as boas práticas de outras democracias que partilham as mesmas ideias;
118. Manifesta a sua preocupação com as tentativas de controlo das diásporas que vivem em território da UE por parte de Estados autoritários estrangeiros; faz notar o papel fundamental desempenhado pela Frente Unida da China, um departamento diretamente dependente do Comité Central do Partido Comunista Chinês e que é responsável por coordenar a estratégia de ingerência externa da China através do controlo rigoroso dos cidadãos chineses e das empresas chinesas no estrangeiro; refere a experiência da Austrália e da Nova Zelândia em matéria de relações com a Frente Unida;
119. Condena veementemente os esforços do Kremlin no sentido de instrumentalizar as minorias nos Estados-Membros da UE, aplicando a chamada «política a favor dos compatriotas», em particular nos Estados bálticos e nos países da vizinhança oriental, como parte da estratégia geopolítica do regime de Putin, cujo objetivo é dividir as sociedades na UE, ao mesmo tempo que aplica o conceito de «mundo russo», destinado a justificar ações expansionistas por parte do regime; observa que muitas «fundações privadas», «empresas privadas», «organizações de meios de comunicação social» e «ONG» russas são detidas pelo Estado ou têm laços ocultos com o Estado russo; salienta que, no diálogo com a sociedade civil russa, é da maior importância distinguir entre as organizações que não têm influência do Estado russo e as que têm ligações ao Kremlin; recorda que existem também provas de ingerência e manipulação russas em muitas democracias liberais ocidentais, bem como de apoio ativo a forças extremistas e entidades radicais, que visam promover a desestabilização da União; observa que o Kremlin utiliza amplamente a cultura, incluindo a música popular, os conteúdos audiovisuais e a literatura como armas do seu ecossistema de desinformação; lamenta as tentativas da Rússia no sentido de não reconhecer plenamente a história dos crimes soviéticos e, em vez disso, introduzir uma nova narrativa russa;
120. Manifesta a sua preocupação com as tentativas do Governo turco de influenciar as pessoas de origem turca no intuito de utilizar a diáspora como meio para veicular as posições de Ancara e dividir as sociedades europeias, nomeadamente através da presidência para os turcos no estrangeiro e comunidades afins (YTB); condena as tentativas explícitas da Turquia de utilizar a sua diáspora na Europa para alterar o desenrolar das eleições;
121. Condena os esforços da Rússia no sentido de explorar as tensões étnicas nos Balcãs Ocidentais, de modo a agravar conflitos e dividir comunidades, o que pode conduzir a

uma desestabilização de toda a região; manifesta a sua preocupação com as tentativas da Igreja Ortodoxa em países como a Sérvia, o Montenegro e a Bósnia-Herzegovina, especialmente na República Sérvia, de promover a Rússia como protetor dos valores familiares tradicionais e fortalecer as relações entre o Estado e a igreja; considera alarmante que a Hungria e a Sérvia estejam a contribuir para os objetivos geopolíticos da China e da Rússia; recomenda o encetamento de diálogos com a sociedade civil dos Balcãs Ocidentais e o setor privado, a fim de coordenar os esforços de combate à desinformação na região, com ênfase na investigação e análise e na inclusão de conhecimentos especializados regionais; insta a Comissão a criar as infraestruturas necessárias para conceber respostas fundamentadas em dados às ameaças de desinformação a curto e a longo prazo nos Balcãs Ocidentais; insta o SEAE a adotar uma posição mais proativa, centrada no reforço, e não na defesa, da credibilidade da UE na região, alargando o controlo por parte da Divisão StratCom de modo a centrar a sua atenção nas ameaças transfronteiriças de desinformação provenientes dos países dos Balcãs Ocidentais e dos seus vizinhos;

122. Salaria a necessidade de a UE e os seus Estados-Membros reforçarem o apoio aos países parceiros da Europa Oriental, nomeadamente através da cooperação no reforço da resiliência do Estado e da sociedade à desinformação e à propaganda estatal russa, a fim de combater a estratégia de enfraquecimento e de fragmentação das suas sociedades e instituições;
123. Manifesta a sua apreensão perante a aplicação extraterritorial de medidas coercivas decorrentes da nova lei da segurança nacional relativa a Hong Kong e da lei chinesa relativa ao combate às sanções estrangeiras, conjugada com os acordos de extradição celebrados pela China com outros países, que lhe permitem levar a cabo ações de dissuasão em grande escala contra cidadãos não chineses críticos, como foi recentemente o caso de dois deputados dinamarqueses, e com as sanções de retaliação impostas pela China a cinco deputados ao Parlamento Europeu, à Subcomissão dos Direitos do Homem do Parlamento, a três deputados dos Estados-Membros da UE, ao Comité Político e de Segurança do Conselho da UE, a dois académicos europeus e a dois grupos de reflexão europeus na Alemanha e na Dinamarca, respetivamente; insta todos os Estados-Membros a resistirem e recusarem a extradição e, se for caso disso, a oferecerem proteção adequada às pessoas em causa, a fim de evitar potenciais violações dos direitos humanos;
124. Manifesta a sua preocupação com o número de universidades, escolas e centros culturais europeus envolvidos em parcerias com entidades chinesas, incluindo os Institutos Confúcio, que permitem o roubo de conhecimentos científicos e o exercício de um controlo rigoroso sobre todos os temas relacionados com a China no domínio da investigação e do ensino, o que constitui uma violação da proteção constitucional da liberdade e autonomia académicas, bem como da escolha das atividades culturais relacionadas com a China; manifesta a sua preocupação pelo facto de tais medidas poderem conduzir a uma perda de conhecimentos sobre questões relacionadas com a China, privando a UE das competências necessárias; manifesta a sua preocupação, nomeadamente, com o patrocínio, em 2014, da biblioteca chinesa do Colégio da Europa pelo Serviço de Informações do Conselho de Estado do Governo chinês<sup>23</sup>; manifesta

---

<sup>23</sup> <https://www.coleurope.eu/events/official-inauguration-china-library>

profunda preocupação com as tentativas da China de exercer pressão e censura, por exemplo, sobre o Museu de Nantes em relação à exposição sobre Genghis Kahn, inicialmente prevista para 2020<sup>24</sup>; exorta a Comissão a facilitar o intercâmbio de boas práticas entre os Estados-Membros, a fim de combater a ingerência estrangeira nos setores da cultura e da educação;

125. Manifesta a sua preocupação perante os casos de financiamento oculto da investigação realizada na Europa, incluindo as tentativas da China de caçar talentos mediante o plano «Thousand Talents» (Mil talentos) e das bolsas de estudo oferecidas pelos Institutos Confúcio, bem como a conjugação deliberada de projetos científicos militares e civis através da estratégia chinesa de fusão civil-militar; destaca as tentativas dos estabelecimentos de ensino superior chineses de assinar memorandos de entendimento com estabelecimentos parceiros na Europa, que contêm cláusulas que perpetuam a propaganda chinesa ou apoiam as posições e iniciativas políticas do Partido Comunista Chinês, como a iniciativa «Uma Cintura, uma Rota», contornando e comprometendo assim as posições oficiais assumidas pelos governos dos países em causa; solicita às instituições culturais, académicas e não governamentais que melhorem a transparência no que respeita à influência da China e apela a que divulguem quaisquer intercâmbios e compromissos com o Governo chinês e organizações conexas;
126. Condena a decisão do Governo húngaro de criar um polo da Universidade de Fudan e, ao mesmo tempo, encerrar a Universidade da Europa Central em Budapeste; manifesta a sua preocupação com a crescente dependência financeira das universidades europeias em relação à China e a outros Estados estrangeiros, atendendo ao risco de fluxos de dados sensíveis, tecnologias e resultados de investigação para Estados estrangeiros e às implicações que tal dependência pode ter na liberdade académica; salienta a importância da liberdade académica para combater a desinformação e as tentativas de exercer influência sobre a informação; incentiva estes estabelecimentos a realizarem avaliações pormenorizadas da vulnerabilidade antes de forjarem novas parcerias com entidades estrangeiras; salienta que o pessoal académico deve ser instruído a denunciar casos de financiamento encoberto ou influência através de uma linha direta específica e que as pessoas que denunciem tais situações devem beneficiar sempre da proteção conferida aos autores de denúncias; exorta a Comissão e os Estados-Membros a garantirem que o financiamento da investigação de interesse geopolítico nas universidades europeias provenha de fontes europeias; insta a Comissão a propor legislação para aumentar a transparência do financiamento das universidades, bem como das ONG e dos grupos de reflexão, designadamente através da declaração obrigatória de donativos, do dever de diligência no que respeita aos seus fluxos de financiamento e à divulgação do financiamento, das contribuições em espécie e das subvenções recebidas de partes estrangeiras; insta as autoridades dos Estados-Membros a adotarem regras eficazes sobre o financiamento estrangeiro dos estabelecimentos de ensino superior, incluindo limites máximos rigorosos e o requisito de comunicação de informações;
127. Sublinha que existem riscos semelhantes para a segurança e em termos de roubo de propriedade intelectual no setor privado, em que os trabalhadores podem ter acesso a tecnologias essenciais e a segredos comerciais; insta a Comissão e os Estados-Membros a incentivarem as instituições académicas e o setor privado a criar programas

---

<sup>24</sup> <https://www.chateaublanc.fr/expositions/fils-du-ciel-et-des-steppes/>

abrangentes de segurança e conformidade, incluindo análises de segurança específicas para novos contratos; observa que podem justificar-se limitações acrescidas aos sistemas e ao acesso à rede, bem como à habilitação de segurança de alguns dos professores ou trabalhadores do ramo da investigação e desenvolvimento de produtos críticos;

128. Observa que a Diretiva Cartão Azul UE<sup>25</sup> revista, que facilita a entrada na UE de migrantes qualificados de países terceiros, permite, por exemplo, às empresas chinesas e russas estabelecidas na Europa recrutar migrantes qualificados dos respetivos países; faz notar que tal pode tornar mais difícil para os Estados-Membros controlar o afluxo destes cidadãos, o que pode criar riscos de ingerência estrangeira;
129. Assinala o número crescente de Institutos Confúcio estabelecidos em todo o mundo e, em particular, na Europa; observa que o Centro para a Educação e a Cooperação Linguísticas, anteriormente conhecido como Sede do Instituto Confúcio, ou Hanban (Gabinete do Conselho Internacional do Ensino da Língua Chinesa), que é responsável pelo programa dos Institutos Confúcio, faz parte do sistema de propaganda do regime de partido único chinês; insta os Estados-Membros e a Comissão a apoiarem cursos independentes de língua chinesa, sem a participação do Estado chinês ou de organizações afiliadas; entende que o recém-criado Centro Nacional da China na Suécia pode ser um exemplo importante de como aumentar os conhecimentos independentes da China na Europa;
130. Considera, além disso, que os Institutos Confúcio servem como plataforma para promover os interesses económicos chineses, bem como para as atividades do serviço de informações chinês e para o recrutamento de agentes e espões; recorda que muitas universidades decidiram cessar sua cooperação com os Institutos Confúcio devido aos riscos de espionagem e ingerência chinesas, tal como fizeram as universidades de Düsseldorf em 2016, de Bruxelas (VUB e ULB) em 2019, e de Hamburgo em 2020, e todas as universidades da Suécia; apela a que mais universidades reflitam sobre a sua atual cooperação, a fim de garantir que esta não afeta a sua liberdade académica; insta os Estados-Membros a acompanharem de perto o ensino, a investigação e outras atividades dos Institutos Confúcio e, sempre que a alegada espionagem ou ingerência seja corroborada por provas claras, a tomarem medidas de execução para salvaguardar a soberania económica e política europeia, nomeadamente através da recusa de financiamento ou da revogação das licenças de institutos associados;
131. Observa que a ingerência estrangeira pode também passar pela influência sobre instituições religiosas e pela instrumentalização destas instituições, destacando-se a influência russa em igrejas ortodoxas, em particular na Sérvia, no Montenegro, na Bósnia-Herzegovina, especialmente na República Sérvia, na Geórgia e, até certo ponto, na Ucrânia, que inclusivamente causa divisões entre as populações locais, leva a que a história seja escrita de forma tendenciosa e promove uma agenda anti-UE, bem como a influência do Governo turco, através de mesquitas em França e na Alemanha, e da Arábia Saudita, através de mesquitas salafitas em toda a Europa, promovendo um islamismo radical; exorta a Comissão e os Estados-Membros a garantirem uma melhor

---

<sup>25</sup> Diretiva (UE) 2021/1883 do Parlamento Europeu e do Conselho, de 20 de outubro de 2021, relativa às condições de entrada e de residência de nacionais de países terceiros para efeitos de emprego altamente qualificado e que revoga a Diretiva 2009/50/CE do Conselho (JO L 382 de 28.10.2021, p. 1).

coordenação em matéria de proteção das instituições religiosas contra a ingerência estrangeira e a limitarem o financiamento e a aumentarem a transparência deste financiamento; insta os Estados-Membros a acompanharem de perto as atividades em instituições religiosas e, se for caso disso e com base em elementos de prova, a tomarem medidas, nomeadamente através da recusa de financiamento ou da revogação das licenças de instituições associadas;

132. Insta o SEAE a realizar um estudo sobre a prevalência e a influência de intervenientes estatais mal-intencionados em grupos de reflexão, universidades, organizações religiosas e instituições de comunicação social europeus; insta todas as instituições da UE e os Estados-Membros a colaborarem e a encetarem um diálogo sistemático com as partes interessadas e os peritos, a fim de determinar com precisão e monitorizar a influência estrangeira nas esferas cultural, académica e religiosa; apela a uma maior partilha de conteúdos entre os organismos de radiodifusão nacionais europeus, incluindo os dos países vizinhos;
133. Manifesta a sua preocupação com os relatos que dão conta de atividades de ingerência estrangeira visando os sistemas judiciais europeus; chama a atenção, em particular, para a execução de sentenças russas pelos tribunais europeus contra os opositores do Kremlin; insta os Estados-Membros a sensibilizarem os funcionários judiciais e a colaborarem com a sociedade civil para evitar abusos da cooperação judiciária internacional e dos órgãos jurisdicionais europeus por parte de governos estrangeiros; insta o SEAE a encomendar um estudo sobre a prevalência e a influência da ingerência estrangeira nos processos judiciais europeus; observa que, com base neste estudo, pode ser necessário propor alterações aos requisitos de transparência e de financiamento no âmbito dos processos judiciais;

#### ***Dissuasão, imputação e contramedidas coletivas, incluindo sanções***

134. Considera que os regimes de sanções recentemente criados pela UE, como as medidas restritivas contra os ciberataques que constituem uma ameaça para a União e os seus Estados Membros<sup>26</sup> e o regime global de sanções da UE em matéria de direitos humanos<sup>27</sup> (Lei Magnitsky da UE), adotados em 17 de maio de 2019 e 7 de dezembro de 2020, respetivamente, demonstraram o seu valor acrescentado ao dotarem a UE de instrumentos de dissuasão importantes; exorta a Comissão a apresentar uma proposta legislativa tendo em vista a adoção de um novo regime de sanções temáticas para combater atos graves de corrupção; recorda que as medidas restritivas contra os ciberataques e o regime de sanções em matéria de direitos humanos foram utilizados duas vezes, em 2020 e 2021, respetivamente; apela a que o regime de cibersanções se torne permanente e insta os Estados-Membros a partilharem todas as provas e informações recolhidas para e elaboração de listas de cibersanções;
135. Insta a UE e os seus Estados-Membros a adotarem medidas adicionais contra a ingerência estrangeira, incluindo as campanhas de desinformação em larga escala, as ameaças híbridas e a guerra híbrida, no pleno respeito das liberdades de expressão e de informação, nomeadamente através da criação de um regime de sanções; considera que tal deve incluir a introdução de um quadro de sanções transetorial e assimétrico, bem

---

<sup>26</sup> <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=OJ%3AL%3A2019%3A129I%3ATOC>.

<sup>27</sup> <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=OJ:L:2020:410I:TOC>.

como de sanções diplomáticas, proibições de viagem, congelamento de bens e retirada de autorizações de residência da UE a cidadãos estrangeiros e seus familiares associados a tentativas de ingerência estrangeira, que devem visar com a maior precisão possível os decisores e os organismos responsáveis por ações agressivas, evitando um ambiente de retaliação, nos termos do artigo 29.º do TUE e do artigo 215.º do Tratado sobre o Funcionamento da União Europeia (TFUE) (medidas restritivas) e firmemente integrados nos pilares da política externa e de segurança comum (PESC) e da PCSD; insta os Estados-Membros a tornarem a desinformação e a ingerência estrangeira e nacional um assunto permanente da agenda do Conselho dos Negócios Estrangeiros; exorta a UE a definir o que é um ato ilícito a nível internacional e a adotar limiares mínimos para o desencadeamento de contramedidas em resultado desta nova definição, o que deve ser acompanhado de uma avaliação de impacto, a fim de proporcionar segurança jurídica; observa que o Conselho deve poder decidir sobre as sanções relacionadas com a ingerência estrangeira por meio de votação por maioria, em vez de por unanimidade; entende que os países envolvidos em atividades de ingerência estrangeira e manipulação da informação com o objetivo de desestabilizar a situação na UE devem pagar o preço pelas suas decisões e arcar com as consequências económicas e diplomáticas e para a sua reputação; insta a Comissão e o Vice-Presidente da Comissão/Alto Representante da União para os Negócios Estrangeiros e a Política de Segurança a apresentarem propostas concretas a este respeito;

136. Insiste em que um regime de sanções, embora deva procurar salvaguardar os processos democráticos, os direitos humanos e as liberdades, tal como definidos nos Tratados, deve também prestar especial atenção ao impacto das sanções impostas nos direitos e liberdades fundamentais, a fim de respeitar a Carta dos Direitos Fundamentais, devendo ser transparente quanto aos motivos pelos quais é tomada a decisão de aplicar sanções; salienta a necessidade de uma maior clareza a nível da UE no que respeita ao âmbito e ao impacto das sanções contra pessoas associadas, tais como cidadãos da UE e empresas;
137. Considera que, embora a natureza destes ataques híbridos varie, o seu perigo para os valores, os interesses fundamentais, a segurança, a independência e a integridade da UE e dos seus Estados-Membros, bem como para o apoio à democracia e à sua consolidação, ao Estado de direito, aos direitos humanos, aos princípios do direito internacional e às liberdades fundamentais, pode ser substancial quer em termos da dimensão dos ataques, quer da sua natureza ou do seu efeito cumulativo; congratula-se com o facto de o Plano de Ação para a Democracia Europeia prever que a Comissão e o SEAE colaborem no desenvolvimento de um conjunto de instrumentos para combater a ingerência estrangeira e as tentativas de exercer influência, nomeadamente as operações híbridas e a imputação clara de ataques mal-intencionados por terceiros, incluindo países terceiros, contra a UE;
138. Salienta que a consciência de que certas ações de ingerência estrangeira estão a afetar seriamente os processos democráticos e a influenciar o exercício de direitos e deveres tem vindo a aumentar à escala internacional; assinala, a este respeito, as alterações adotadas em 2018 na lei australiana de alteração da lei sobre segurança nacional (espionagem e ingerência estrangeira), que visa criminalizar atividades encobertas e desonestas levadas a cabo por intervenientes estrangeiros que pretendem interferir nos processos políticos ou governamentais, afetar direitos e deveres ou apoiar as atividades

de informação de um governo estrangeiro, criando novas infrações como a «ingerência estrangeira intencional»;

139. Está ciente de que, nos termos do artigo 21.º, n.º 3, do TUE, a União deve assegurar a coerência entre os diferentes domínios da sua ação externa e entre estes e outras políticas, tal como definidos nos Tratados; faz notar, a este respeito, que a ingerência externa, como, por exemplo, a ameaça que representam os combatentes terroristas estrangeiros e os grupos que influenciam as pessoas que permanecem na UE, também foi combatida através da Diretiva (UE) 2017/541 do Parlamento Europeu e do Conselho, de 15 de março de 2017, relativa à luta contra o terrorismo<sup>28</sup>;
140. Sublinha que, para reforçar o seu impacto, as sanções devem ser impostas coletivamente, sempre que possível, com base na coordenação com parceiros que partilham as mesmas ideias, possivelmente envolvendo organizações internacionais e formalizando essa coordenação por meio de um acordo internacional, tendo igualmente em conta outros tipos de reações aos ataques; observa que os países candidatos e potencialmente candidatos devem também adotar estas sanções, a fim de se alinharem com a PESC da UE; regista o importante trabalho desenvolvido pela NATO no domínio das ameaças híbridas e recorda, a este respeito, o comunicado da reunião da NATO de 14 de junho de 2021, em que se reafirma que caberá ao Conselho do Atlântico Norte decidir, numa base casuística, em que circunstâncias um ciberataque deve suscitar a invocação do artigo 5.º do Tratado da NATO, e que as ciberatividades mal-intencionadas e cumulativas de grande alcance e impacto poderão, em determinadas circunstâncias, ser consideradas equivalentes a um ataque armado<sup>29</sup>; salienta que a UE e a NATO devem adotar uma abordagem mais prospetiva e estratégica no que respeita às ameaças híbridas, centrada nos motivos e objetivos dos adversários, devendo esclarecer em que casos a UE está mais bem equipada para lidar com uma ameaça, bem como as vantagens comparativas das suas capacidades; recorda que vários Estados-Membros da UE não são membros da NATO, embora cooperem com esta organização, por exemplo através do seu Programa Parceria para a Paz (PPP) e da Iniciativa de Interoperabilidade da Parceria (IIP); sublinha, por conseguinte, que qualquer cooperação entre a UE e a NATO não deve prejudicar a política de segurança e defesa dos Estados-Membros da UE não pertencentes à NATO, incluindo os que seguem políticas de neutralidade; salienta a importância da assistência mútua e da solidariedade, em conformidade com o artigo 42.º, n.º 7, do TUE e o artigo 222.º do TFUE, e insta a UE a elaborar cenários concretos para a ativação destes artigos em caso de hipotético ciberataque; insta a UE e todos os Estados-Membros a incorporarem esta questão noutros aspetos das suas relações com Estados responsáveis por ingerências e campanhas de desinformação, em particular a Rússia e a China;

### *Cooperação mundial e multilateralismo*

141. Reconhece que muitos países democráticos em todo o mundo se veem confrontados com operações de desestabilização semelhantes levadas a cabo por intervenientes estatais e não estatais estrangeiros;
142. Realça a necessidade de uma cooperação mundial e multilateral entre países que

---

<sup>28</sup> JO L 88 de 31.3.2017, p. 6.

<sup>29</sup> [https://www.nato.int/cps/en/natohq/news\\_185000.htm](https://www.nato.int/cps/en/natohq/news_185000.htm)

partilham as mesmas ideias nas instâncias internacionais pertinentes sobre estas questões de importância fundamental, sob a forma de uma parceria assente num entendimento comum e em definições comuns, com vista ao estabelecimento de normas e princípios internacionais; sublinha a importância de uma cooperação estreita com os EUA e outros Estados que partilham as mesmas ideias para a modernização das organizações multilaterais; congratula-se, neste contexto, com a Cimeira para a Democracia e espera que esta resulte em propostas e ações concretas para fazer face, através de ações coletivas, às maiores ameaças que as democracias enfrentam atualmente;

143. Defende que, com base num conhecimento comum da situação, os parceiros que partilham as mesmas ideias devem proceder ao intercâmbio de boas práticas e identificar respostas comuns a desafios à escala mundial, mas também a desafios a nível nacional que são comuns a todos eles, incluindo sanções coletivas e medidas de proteção dos direitos humanos e das normas democráticas; insta a UE a liderar o debate sobre as consequências penais da ingerência estrangeira, a promover definições e regras de imputação internacionais comuns e a desenvolver um quadro internacional para dar resposta às interferências nas eleições, de molde a estabelecer um código de conduta mundial para processos democráticos livres e resilientes;
144. Exorta a UE e os seus Estados-Membros a ponderarem sobre os formatos internacionais adequados para permitir uma tal parceria e cooperação entre parceiros que partilham as mesmas ideias; insta a UE e os seus Estados-Membros a iniciarem um processo a nível das Nações Unidas com vista à adoção de uma convenção global para promover e defender a democracia que estabeleça uma definição comum de «ingerência estrangeira»; insta a UE a propor um conjunto de instrumentos de defesa da democracia a nível mundial, a incluir na Convenção, que preveja ações conjuntas e sanções para combater a ingerência estrangeira;
145. Saúda a declaração da NATO de 14 de junho de 2021, que reconhece o crescente desafio colocado pelas ciberameaças, as ameaças híbridas e outras ameaças assimétricas, incluindo as campanhas de desinformação, e pela utilização mal-intencionada de tecnologias emergentes e disruptivas cada vez mais sofisticadas; regozija-se com os progressos realizados a nível da cooperação entre a UE e a NATO no domínio da ciberdefesa; congratula-se com a criação, pela Lituânia, do Centro Regional de Ciberdefesa, que conta com a participação dos EUA e dos países da Parceria Oriental; apoia uma cooperação mais estreita com os países parceiros no domínio da ciberdefesa, em termos de partilha de informações e de trabalho operacional; regozija-se com os debates entre os EUA e a UE sobre os controlos multilaterais das exportações de produtos de cibervigilância no contexto do Conselho de Comércio e Tecnologia;
146. Congratula-se com as iniciativas já tomadas, em particular a nível administrativo, para partilhar conhecimentos sobre o estado dos ataques híbridos, incluindo as operações de desinformação, em tempo real, como o Sistema de Alerta Rápido criado pelo SEAE, parcialmente aberto a países terceiros que partilham as mesmas ideias, o Mecanismo de Resposta Rápida criado pelo G7 e a Divisão Conjunta de Informações e Segurança da NATO;



147. Destaca que a cooperação mundial deve basear-se em valores comuns refletidos em projetos comuns, com a participação de organizações internacionais como a OSCE e a UNESCO, e no reforço da capacidade democrática e de uma paz e segurança sustentáveis em países confrontados com ameaças de ingerência estrangeira semelhantes; insta a UE a criar um fundo europeu para os meios de comunicação social democráticos para apoiar o jornalismo independente nos (potenciais) países do alargamento e nos países da vizinhança europeia, assim como nos países candidatos e potencialmente candidatos; destaca as necessidades práticas, como a obtenção de equipamento técnico de trabalho, que são regularmente expressas por jornalistas independentes de países vizinhos;
148. Saliencia a necessidade urgente de combater as informações erradas e a desinformação sobre o clima; saúda os esforços da COP 26 para adotar uma definição universal de «informações erradas e desinformação» sobre o clima, bem como para delinear ações para dar resposta a este problema; solicita que modelos como o Painel Intergovernamental sobre as Alterações Climáticas se baseiem na criação de um código de conduta mundial sobre desinformação, um processo que serviria de base para um Acordo de Paris sobre Desinformação;
149. Frisa a importância de proporcionar uma perspetiva clara aos países candidatos e potencialmente candidatos e de apoiar os países parceiros e os países vizinhos, como os países dos Balcãs Ocidentais e da vizinhança oriental e meridional da UE, uma vez que a Rússia, a Turquia e a China estão a tentar utilizar estes países como um laboratório de manipulação da informação e de guerra híbrida, com o objetivo de debilitar a UE; considera que os EUA são um parceiro importante na luta contra a ingerência estrangeira, as campanhas de desinformação e as ameaças híbridas nessas regiões; manifesta a sua preocupação, em particular, com o papel desempenhado pela Sérvia e pela Hungria na ampla propagação da desinformação nos países vizinhos; sublinha que a UE deve apoiar e colaborar com estes países, tal como previsto no Regulamento IVDCI<sup>30</sup>; considera que as suas ações podem assumir a forma de promoção do valor acrescentado e do impacto positivo da UE na região, de financiamento de projetos destinados a garantir a liberdade dos meios de comunicação social, de reforço da sociedade civil e do Estado de direito e de intensificação da cooperação em matéria de literacia mediática, digital e informacional, respeitando simultaneamente a soberania desses países; solicita, neste contexto, o aumento da capacidade do SEAE;
150. Incentiva a UE e os seus Estados-Membros a aprofundarem a cooperação com Taiwan no combate às operações de ingerência e às campanhas de desinformação levadas a cabo por países terceiros mal-intencionados, inclusive através da partilha de boas práticas, de abordagens conjuntas para promover a liberdade dos meios de comunicação social e o jornalismo, do aprofundamento da cooperação em matéria de cibersegurança e combate a ciberameaças, da sensibilização dos cidadãos e da melhoria global da literacia digital entre a população, de modo a reforçar a resiliência dos nossos sistemas democráticos; apoia a intensificação da cooperação entre agências governamentais,

---

<sup>30</sup> Regulamento (UE) 2021/947 do Parlamento Europeu e do Conselho, de 9 de junho de 2021, que cria o Instrumento de Vizinhança, de Cooperação para o Desenvolvimento e de Cooperação Internacional – Europa Global, e que altera e revoga a Decisão n.º 466/2014/UE do Parlamento Europeu e do Conselho e revoga o Regulamento (UE) 2017/1601 do Parlamento Europeu e do Conselho e o Regulamento (CE, Euratom) n.º 480/2009 do Conselho (JO L 209 de 14.6.2021, p. 1).

ONG e grupos de reflexão europeus e taiwaneses neste domínio;

151. Solicita ao Parlamento que promova ativamente uma narrativa da UE, desempenhe um papel de proa na promoção do intercâmbio de informações e debata as boas práticas com os parlamentos parceiros de todo o mundo, utilizando a sua vasta rede de delegações interparlamentares, bem como as iniciativas em matéria de democracia e as atividades de apoio coordenadas pelo seu Grupo de Apoio à Democracia e de Coordenação Eleitoral; sublinha a importância de uma cooperação estreita com deputados de países terceiros, através de projetos específicos que apoiem uma perspetiva europeia para os países candidatos e potencialmente candidatos;
  152. Insta o SEAE a reforçar o papel das delegações da UE e das missões da PCSD da UE em países terceiros, a fim de consolidar a sua capacidade de detetar e desmistificar as campanhas de desinformação orquestradas por intervenientes estatais estrangeiros e de financiar projetos educativos que reforcem os valores democráticos e os direitos fundamentais; recomenda vivamente a criação de uma Plataforma de Comunicação Estratégica, iniciada pelo SEAE, para estabelecer uma cooperação estrutural em matéria de luta contra a desinformação e a ingerência estrangeira, que deverá estar sediada em Taipé; insta, além disso, as delegações da UE a contribuírem para a luta da UE contra a desinformação, traduzindo as decisões pertinentes da UE, como as resoluções urgentes do Parlamento, para a língua do país de estabelecimento;
  153. Solicita que a questão da ingerência mal-intencionada estrangeira seja abordada no âmbito das novas orientações estratégicas da UE;
  154. Apela à criação, no Parlamento Europeu, de um mecanismo institucional permanente dedicado ao acompanhamento destas recomendações, por forma a combater de forma sistemática a ingerência estrangeira e a desinformação na UE, para além do atual mandato da Comissão Especial INGE; apela a um melhor intercâmbio institucionalizado entre a Comissão, o SEAE e o Parlamento através deste organismo;
- o
- o   o
155. Encarrega a sua Presidente de transmitir a presente resolução ao Conselho, à Comissão, ao Vice-Presidente da Comissão/Alto Representante da União para os Negócios Estrangeiros e a Política de Segurança e aos governos e parlamentos dos Estados-Membros.

## EXPOSIÇÃO DE MOTIVOS

### *Contexto*

Quando, em 18 de junho de 2020, o Parlamento Europeu decidiu criar uma Comissão Especial sobre a Ingerência Estrangeira, incluindo a Desinformação, atribuiu-lhe o mandato de formular uma abordagem a longo prazo para analisar indícios de ingerência estrangeira nas instituições e nos processos democráticos da UE e dos seus Estados-Membros.

Um ano após a reunião constitutiva da comissão, em 23 de setembro de 2020, e com base numa longa série de testemunhos de vários peritos e profissionais, a relatora já pode expor a realidade, a escala e a extrema sofisticação das inúmeras formas utilizadas por operações de ingerência agressivas, decididas e financiadas por intervenientes estrangeiros contra a UE; a relatora também pode assinalar, com preocupação, a rapidez da adaptação, a volatilidade e a aceleração deste fenómeno, através de novos intervenientes, novas narrativas e novos instrumentos num período de apenas um ano.

Desde as campanhas de desinformação de nova escala relacionadas com a COVID-19 até aos ciberataques contra autoridades públicas, nomeadamente infraestruturas de saúde pública, desde as estratégias de ingerência que incluem a captação de elites e de grupos de pressão industrial até ao financiamento encoberto de atividades políticas, passando pelo controlo de centros académicos e culturais e pela instrumentalização das diásporas nacionais, a nossa comissão tem vindo a analisar a dimensão multifacetada e dinâmica deste novo tipo de guerra, cujo objetivo é sabotar a coesão social e a confiança mútua das nossas sociedades democráticas europeias, a fim de as enfraquecer.

Felizmente, a comissão assistiu também à sensibilização para estas questões fundamentais, designadamente o entendimento comum de que a UE e os seus Estados-Membros devem estabelecer rapidamente políticas de resiliência e instrumentos de dissuasão plenamente consolidados, com base numa abordagem de toda a sociedade, que lhes permita enfrentar todos os tipos de ameaças e ataques híbridos e, deste modo, proteger o funcionamento sustentável da democracia.

### ***Reforçar a resiliência através do conhecimento situacional, da literacia mediática e informacional, do pluralismo dos meios de comunicação social, do jornalismo independente e da educação***

Afigura-se evidente que o primeiro passo para uma defesa sólida contra a ingerência estrangeira é o conhecimento situacional. Para tal, existem duas etapas importantes: em primeiro lugar, temos de supervisionar, identificar e analisar os diferentes tipos de ataques de ingerência, para que possamos compreender plenamente a ameaça; em segundo lugar, temos de garantir que todos aqueles que precisam de ter conhecimento estão a par desta análise.

Há vários investigadores, organizações da sociedade civil, jornalistas e funcionários de instituições nacionais ou europeias que fazem um excelente trabalho na investigação desta ameaça. Conhecemos muitos deles na Comissão INGE. A nível europeu, a relatora aprecia particularmente o trabalho levado a cabo pelos grupos de trabalho da Divisão StratCom do SEAE. Temos, contudo, de continuar a desenvolver este aspeto. É inaceitável que ainda não exista qualquer grupo de trabalho que supervise a ingerência chinesa.

Precisamos também de garantir que os conhecimentos sejam divulgados a um público mais vasto. É importante proceder à realização de ações de formação destinadas a pessoas cujas funções sejam sensíveis a ingerência estrangeira, bem como de campanhas gerais de sensibilização. Neste contexto, a educação para a literacia mediática e digital é essencial para dotar os cidadãos da capacidade de interpretar e avaliar melhor as informações com que se deparam.

Os jornalistas desempenham um papel fundamental na garantia de um ambiente de debate saudável. Infelizmente, têm sofrido financeiramente com a digitalização, sobretudo porque os sistemas publicitários parecem favorecer o conteúdo emocional, nomeadamente as opiniões e a desinformação, em detrimento do jornalismo de qualidade. Alguns jornalistas são também, frequentemente, vítimas de assédio e de ameaças organizadas quando investigam temas sensíveis. Embora seja importante defender a independência dos meios de comunicação social de qualidade, é igualmente imprescindível avaliar formas de apoiar os órgãos de informação e os jornalistas, tanto financeiramente como contra o assédio.

### ***Ingerência estrangeira através da utilização de plataformas em linha***

O atual sistema de divulgação de informações através de plataformas conduz, claramente, a um ambiente em linha distorcido, em que a desinformação e outros tipos de manipulação da informação prosperam. Os relatos sobre fugas e venda de dados sensíveis, os algoritmos que promovem conteúdos com vista à radicalização e as plataformas que ignoram violações claras da lei ou das suas próprias condições são tão comuns, que já quase nos habituámos à sua existência e deixamos de manifestar a nossa indignação. Temos de pôr termo a esta situação.

Após debater o assunto com diversos peritos, considero que o atual método de autorregulação não funciona e deve ser substituído por normas vinculativas. Não podemos aceitar que intervenientes estrangeiros possam manipular livremente os conteúdos que recebemos em linha através de plataformas ou utilizar abusivamente os sistemas publicitários para que os anunciantes acabem, inadvertidamente, por financiá-los. É, também, inaceitável que as plataformas não atuem sem sofrerem consequências.

É certo que se verificaram muitas melhorias, tanto por iniciativa das próprias plataformas como através de medidas públicas como o Código de Conduta. No entanto, sem uma transparência significativa, é impossível calcular o impacto destas ações. É igualmente essencial que o Código de Conduta, que é por natureza voluntário, disponha de um mecanismo de execução eficaz e seja complementado por uma legislação sólida. Surpreende também o número de políticas anti-ingerência que são utilizadas apenas para conteúdos em língua inglesa ou conteúdos num número muito limitado de línguas. Não podemos tolerar uma situação em que os falantes de letão, búlgaro, grego ou mesmo francês e alemão tenham muito menos proteção contra a manipulação em linha do que os falantes nativos de inglês apenas porque as plataformas dão prioridade aos conteúdos nesta língua.

### ***Infraestruturas críticas e setores estratégicos***

As infraestruturas críticas são essenciais para o funcionamento da economia e da sociedade. Para proteger melhor os setores críticos, são necessários esforços coordenados e conjuntos em todos os setores e a diferentes níveis: nacional, regional, local e da UE. A nova diretiva da Comissão destinada a reforçar a resiliência das entidades críticas é um ponto de partida importante. A relatora considera, no entanto, que a lista de infraestruturas críticas deve ser

alargada de modo a incluir os meios de comunicação social, bem como as infraestruturas eleitorais, dada a sua respetiva importância essencial para garantir o funcionamento da UE e dos seus Estados-Membros, e que deve ser permitida flexibilidade relativamente ao aditamento de novos setores estratégicos no futuro. É da maior importância que a diretiva mantenha uma abordagem altamente adaptável que permita atualizações e modificações rápidas.

Para além disso, a dependência tanto dos investimentos estrangeiros como dos fornecedores estrangeiros de tecnologia em infraestruturas críticas dá origem a várias ameaças ao funcionamento autónomo dessas infraestruturas. A promoção da autonomia estratégica e da soberania digital empreendida pela UE é, pois, primordial para combater tais ameaças.

### ***Financiamento encoberto de atividades políticas por intervenientes e doadores estrangeiros***

Existem provas concretas de que intervenientes estrangeiros têm interferido ativamente em eleições democráticas e referendos dos países europeus, através de operações de financiamento encobertas durante as campanhas.

Estas operações maliciosas põem em risco a integridade das eleições organizadas na UE, uma vez que geram concorrência desleal entre partidos e candidatos, através da atribuição de recursos adicionais a alguns dos partidos, geralmente os partidos anti-UE, que não são declarados nas contas oficiais das campanhas eleitorais.

De acordo com o relatório de 2020 sobre financiamentos estrangeiros encobertos da Alliance for Securing Democracy (Aliança para assegurar a democracia)<sup>31</sup>, a Rússia, a China e outros regimes autoritários atribuíram mais de 300 milhões de dólares a 33 países na última década para interferir nos processos democráticos mais de 100 vezes, com a particularidade de metade destes casos dizerem respeito a ações da Rússia na Europa.

Algumas destas operações não são sequer ilegais: tiram partido das muitas lacunas existentes entre os Estados-Membros, cujas disposições nas legislações eleitorais nacionais relativas ao financiamento de atividades políticas não estão harmonizadas a nível da UE.

### ***Cibersegurança e resiliência contra ciberataques***

A digitalização crescente dos serviços conduziu a uma maior dependência das infraestruturas críticas em relação aos sistemas em linha, aumentando, por conseguinte, a sua vulnerabilidade aos ciberataques e à exposição de dados. O número de ciberataques aumentou nos últimos anos, visando setores estratégicos, nomeadamente a Agência Europeia de Medicamentos (EMA) e o Parlamento norueguês.

A fragmentação das capacidades e das competências, bem como o reduzido volume de recursos humanos e financeiros, demonstram a vulnerabilidade da UE aos ciberataques. Os ciberataques não respeitam fronteiras. É fundamental que a UE invista rapidamente nas suas capacidades e competências digitais estratégicas, afetando mais recursos humanos e financeiros à cibersegurança e garantindo, simultaneamente, um elevado nível comum de cibersegurança em todos os Estados-Membros. A Estratégia da UE para a Cibersegurança de 2020 e a Diretiva SRI 2 são propostas importantes para melhorar a cibersegurança da UE, que

---

<sup>31</sup> <https://securingdemocracy.gmfus.org/covert-foreign-money/>

serão reforçadas no futuro pela Diretiva Ciber-Resiliência e pela Política de Ciberdefesa.

Deve, além disso, ser dada uma resposta rápida à questão dos programas de espionagem, como o Pegasus, através do reforço do quadro legislativo para responsabilizar os distribuidores, os utilizadores e os infratores que a eles recorrem.

### ***Proteção dos Estados-Membros, instituições, agências, delegações e missões da UE***

A cibersegurança deve ser melhorada não só em todos os Estados-Membros, mas também nas instituições da UE. Os recentes ciberataques contra as instituições da UE evidenciaram a necessidade de uma forte cooperação interinstitucional em termos de deteção, monitorização e partilha de informações durante ciberataques ou para os evitar. As instituições europeias já adotaram medidas para reforçar a sua cibersegurança e dispõem de instrumentos para coordenar e detetar ciberataques, como a CERT-UE, a ENISA e, em breve, a ciberunidade conjunta.

Há, no entanto, mais por fazer. Em primeiro lugar, deve haver um aumento dos recursos humanos e financeiros para responder aos desafios de um cenário de ameaças em constante evolução. Em segundo lugar, as instituições da UE devem proceder a uma revisão exaustiva dos seus serviços e redes, a fim de atenuar os riscos de segurança e garantir que a segurança das instituições não dependa de tecnologias estrangeiras. Por último, devem ser asseguradas a sensibilização, formação e orientação adequadas de todo o pessoal para atenuar e fazer face aos riscos à segurança cibernética e não cibernética.

### ***Ingerência por parte de intervenientes mundiais através da captação de elites, diásporas nacionais, universidades e eventos culturais***

Outro dos instrumentos utilizados por países estrangeiros com o intuito de interferir no funcionamento da UE é a ingerência através das pessoas.

A «captação de elites», ou cooptação é, infelizmente, um fenómeno generalizado. O seu modo de atuação mais habitual consiste na contratação de antigos políticos e funcionários públicos europeus de alto nível por parte de empresas controladas por Estados estrangeiros em troca dos conhecimentos que estes adquiriram durante o desempenho das suas funções ou mandatos públicos. Os seus conhecimentos, frequentemente baseados em informações e contactos confidenciais, são posteriormente utilizados em detrimento dos interesses estratégicos da UE e dos seus Estados-Membros. Estas operações são muitas vezes associadas a estratégias de tráfico de influências a nível industrial, em que os objetivos económicos e políticos se fundem.

Outra forma de ingerência através das pessoas é a crescente influência e, em última instância, o controlo de universidades, escolas e centros culturais e religiosos por agentes de Estados estrangeiros, no que concerne a temas pertinentes para o país estrangeiro em causa. A forma como os Institutos Confúcio, recentemente designados «Centros para a Educação e a Cooperação Linguísticas», procuram controlar todos os tipos de investigação, ensino ou mesmo exposições culturais relacionadas com a China em muitas universidades e museus europeus é um exemplo flagrante desta prática. Existem outros países também muito ativos neste domínio, designadamente a Rússia, através das igrejas ortodoxas.

Esta forma de ingerência beneficia, em grande medida, dos esforços para controlar a diáspora

nacional que vive na UE, o que representa uma potencial influência de grande alcance em vários níveis das sociedades europeias. Estes esforços visam igualmente silenciar os opositores políticos que vivem no estrangeiro.

### ***Dissuasão, imputação e contramedidas coletivas, incluindo sanções***

A UE e os seus Estados-Membros devem criar instrumentos de dissuasão credíveis. Com efeito, a UE e os seus Estados-Membros não dispõem, atualmente, de qualquer regime específico de sanções relacionado com a ingerência estrangeira e as campanhas de desinformação orquestradas por intervenientes estatais estrangeiros.

A relatora está ciente dos desafios jurídicos que podem surgir no estabelecimento de tal regime de sanções, designadamente a necessidade de definir com precisão os elementos dos crimes e os seus possíveis efeitos cumulativos, em conformidade com o direito da UE e o direito internacional.

A relatora considera, todavia, que a UE pode inspirar-se de forma útil no que foi feito por outros parceiros a este respeito, nomeadamente a Austrália, em especial ao definir o que constitui a «ingerência estrangeira intencional» e ao criminalizar atividades encobertas e desonestas de intervenientes estrangeiros.

A relatora considera igualmente que podemos tirar partido do que já existe a nível da UE, nomeadamente o regime de medidas restritivas contra os ciberataques que ameaçam a União e os seus Estados-Membros, que foram utilizados duas vezes no ano passado.

Por último, mas não menos importante, frisamos a necessidade de cooperar estreitamente com os nossos parceiros internacionais que partilhem as mesmas ideias no atinente a qualquer regime de sanções, com o objetivo de impor sanções em conjunto, a fim de reforçar a eficácia e o efeito dissuasor.

As entidades estrangeiras responsáveis por operações agressivas de ingerência contra as democracias não devem partir do princípio de que as suas campanhas de desestabilização estarão isentas de consequências.

### ***Cooperação mundial e multilateralismo***

A UE está longe de ser a única zona democrática do mundo confrontada com um número cada vez maior de ações agressivas de ingerência estrangeira. Muitos outros países, sejam eles desenvolvidos ou em desenvolvimento, são também visados por tais operações, por parte da China ou da Rússia e de outros regimes autoritários, cujo intuito é sempre o mesmo: prejudicar o funcionamento democrático para ganhar influência.

Precisamos de reunir parceiros que partilhem as mesmas ideias e dar resposta a estas questões de forma coordenada, com base numa parceria democrática.

Em primeiro lugar, temos de estar em sintonia no respeitante a definições comuns e partilhar os mesmos pontos de vista sobre o que está atualmente em jogo, a fim de chegar a acordo sobre normas e padrões internacionais.

As perguntas que se seguem devem ser abordadas e respondidas de forma precisa e coletiva: o

que é uma ingerência estrangeira agressiva? Como qualificar juridicamente as operações de desinformação e manipulação orquestradas por um país estrangeiro? Como podemos definir estas ameaças e ataques como crimes? Que regime de sanções coletivas poderia ser instituído?

A cooperação global deveria, posteriormente, assentar num intercâmbio de boas práticas e na gestão de projetos concretos. O Parlamento Europeu, através da sua vasta rede de fóruns interparlamentares, desempenharia, neste caso, um papel de liderança, tal como as delegações da UE em países terceiros.

### ***Métodos de trabalho***

Independentemente da nossa visão política sobre os diferentes atos legislativos e as nossas cores no espectro político, enquanto membros da Comissão INGE partilhamos da opinião de que a nossa democracia deve manter-se sólida face a tentativas de ingerência estrangeira. Por este motivo, desenvolvemos o nosso trabalho na comissão com base numa cooperação aprofundada entre os grupos políticos. Os coordenadores decidiram, juntamente com a presidência, quais os peritos a convidar e os estudos a encomendar. Enquanto relatora, consultei regularmente os relatores-sombra durante o meu trabalho de redação.

Do ponto de vista temático, podemos distinguir a fase de diagnóstico da fase centrada nas soluções. Durante a primeira fase, convidámos peritos que nos pudessem ajudar a compreender as ameaças e os métodos em todas as suas variedades. No âmbito do nosso mandato, levámos a cabo uma série de audições sobre ingerências na esfera pública e privada e investigámos os métodos utilizados por diferentes intervenientes estrangeiros. Na fase de concentração nas soluções, a Comissão INGE centrou-se na identificação de possíveis instrumentos e estratégias para prevenir e combater os problemas identificados.

A Comissão INGE encomendou igualmente seis estudos e convidou os autores a apresentarem as suas conclusões. A situação sanitária associada à pandemia de COVID-19 impediu-nos de organizar quaisquer deslocações em serviço durante os dois primeiros semestres da existência da Comissão INGE. No entanto, enquanto este documento era redigido, os membros da Comissão INGE regressavam de uma primeira deslocação em serviço com êxito à Agência da União Europeia para a Cibersegurança (ENISA), em Atenas, na Grécia. Estão previstas mais três deslocações: a Taipé, Paris e Washington.

A fim de continuar a preparar as nossas recomendações, formulámos duas perguntas com pedidos de respostas orais. Em julho de 2021, perguntámos ao Vice-Presidente e Alto Representante Josep Borrell como pretendia suprir a falta de recursos e a inexistência de um mandato para os grupos de trabalho da Divisão StratCom do SEAE e a ausência de sanções adequadas contra intervenientes estrangeiros envolvidos em atividades de ingerência. Em outubro de 2021, perguntámos à Vice-Presidente da Comissão, Věra Jourová, como tencionava assegurar que a falta de coordenação entre setores e níveis políticos não aumente a exposição a ingerências estrangeiras, como melhorar a transparência dos algoritmos e apoiar a literacia mediática.

Uma das nossas principais conclusões foi a importância da cooperação e da partilha de informações, tanto a nível mundial como entre os níveis de governação e os diferentes setores na UE. Foi precisamente por esse motivo que, desde o início, convidámos outras comissões e delegações com competências relacionadas com a ingerência estrangeira a participarem nas nossas reuniões. Os conhecimentos especializados destes órgãos homólogos enriqueceram os



debates que tivemos com os convidados e garantiram que os resultados das nossas audições fossem transmitidos às comissões ordinárias que trabalham com propostas legislativas correspondentes.

Um dos principais eventos será a reunião interparlamentar que realizaremos em novembro de 2021. Esta reunião entre deputados de países da UE e um grupo selecionado de parceiros mundiais que partilham as mesmas ideias constituirá uma oportunidade crucial para aprendermos uns com os outros e debater desafios e soluções comuns.

Para elaborar o presente relatório, a relatora elaborou quatro documentos de trabalho: um deles debruça-se sobre o estado da ingerência estrangeira na União Europeia, designadamente a desinformação, outro sobre o financiamento encoberto de atividades políticas por doadores estrangeiros, outro sobre a ingerência estrangeira através de plataformas em linha e outro sobre o reforço da resiliência da UE contra as ameaças híbridas.

Para além de todas as reuniões formais mencionadas, a relatora recolheu conhecimentos em reuniões, através da participação em conferências e da leitura de vários estudos e artigos jornalísticos.

### ***Cooperação com outros órgãos do Parlamento Europeu e órgãos da UE***

Devido à natureza intersetorial do nosso mandato, a Comissão INGE convidou e debateu diferentes aspetos da ingerência estrangeira com cinco comissários:

- Věra Jourová, Vice-Presidente dos Valores e Transparência,
- Margaritis Schinas, Vice-Presidente da Promoção do Modo de Vida Europeu,
- Josep Borrell, Vice-Presidente da Comissão Europeia e Alto Representante da União para os Negócios Estrangeiros e a Política de Segurança,
- Thierry Breton, Comissário do Mercado Interno, e
- Margrethe Vestager, Vice-Presidente Executiva responsável por Uma Europa Preparada para a Era Digital e pela Concorrência.

Realizámos igualmente vários debates com funcionários da Comissão e dos Serviços para a Ação Externa, bem como uma reunião extraordinária, juntamente com a Comissão CONT, com o Tribunal de Contas Europeu, sobre o seu Relatório Especial n.º 09/2021 - Desinformação na UE: fenómeno combatido, mas não controlado.

A Comissão Especial INGE estabeleceu igualmente um plano de cooperação com várias comissões do PE com as quais partilha algumas competências. Até à data, a referida comissão conta com onze comissões e onze delegações.

### ***Peritos externos***

A Comissão Especial sobre a Ingerência Estrangeira em Todos os Processos Democráticos na União Europeia, incluindo a Desinformação, solicitou conhecimentos especializados externos sobre os seguintes temas, pertinentes para os trabalhos em curso da comissão:

- Desinformação - levantamento e soluções, nomeadamente a regulamentação de plataformas;
- Financiamento - levantamento e soluções;
- Infraestruturas;
- Boas práticas na abordagem global da sociedade à luta contra as ameaças híbridas;
- O impacto das campanhas de desinformação sobre os migrantes, as pessoas LGBTI e os grupos minoritários;
- Ensinos retirados dos abusos cometidos por regimes autoritários.

### *Resumo das audições com peritos externos*

#### Audições temáticas

- **Ameaças híbridas, desinformação e polarização – perspetiva institucional**, 24 de setembro de 2020
- **Ingerência eleitoral, financiamento dos partidos políticos e plataformas de redes sociais – visão geral**, 2 de outubro de 2020
- **Como a interferência estrangeira prejudica a soberania: o exemplo dos nossos vizinhos do Leste**, 21 de outubro de 2020
- **Ingerência estrangeira na esfera pública: verificação de factos, plataformas de redes sociais e a sua utilização na desinformação, na ingerência estrangeira e no reforço da resiliência**, 26 de outubro e 9 de novembro de 2020
- **Ingerência estrangeira na esfera política: ingerência estrangeira durante os processos eleitorais, nomeadamente através de ciberataques, fugas de dados e comunicação maliciosa**, 12 de novembro de 2020
- **Ingerência estrangeira na esfera política: financiamento político através de canais legais ou ilegais e de doadores que agem enquanto testas de ferro usando fontes de países terceiros**, 2 de dezembro de 2020
- **Jornalismo versus propaganda**, 11 de dezembro de 2020
- **Possíveis ameaças de ingerência por parte de países terceiros num contexto geopolítico**, 25 de janeiro e 1 de fevereiro de 2021
- **Comunicação estratégica na luta contra a ingerência estrangeira**, 22 de fevereiro de 2021
- **Como tornar mais transparente o financiamento dos partidos e das campanhas políticas: quais são as regras de que precisamos na UE?**, 23 de fevereiro de 2021
- **Democracia em linha: quais são os riscos? Como podemos proteger-nos?**, 17 de

março de 2021

- **Ingerência estrangeira no financiamento de organizações antiescolha na UE**, 25 de março de 2021
- **A evolução tecnológica e as abordagens regulamentares à desinformação: ingerência através da publicidade**, 13 de abril de 2021
- **A evolução tecnológica e as abordagens regulamentares no que respeita à desinformação**, 15 de abril de 2021
- **Troca de pontos de vista com Mikhail Khodorkovsky, fundador do Dossier Center**, 10 de maio de 2021
- **Audição com o Facebook, o Twitter e o YouTube sobre o papel das plataformas de redes sociais na propagação e criação de desinformação, bem como na sua deteção e combate**, 10 de maio de 2021
- **Como a história, a cultura e a educação podem ajudar a combater a desinformação**, 15 de junho de 2021
- **Desinformação e discriminação**, 12 de julho de 2021
- **O Plano de Ação para a Democracia Europeia, o Ato Legislativo sobre os Serviços Digitais e outros instrumentos da UE: como poderão estas propostas proteger os processos democráticos na UE da ingerência estrangeira e o rumo a seguir**, 2 de setembro de 2021
- **Sanções e contramedidas coletivas**, 2 de setembro de 2021

Troca de pontos de vista sobre:

- **O papel da educação, dos meios de comunicação social e da cultura na luta contra a desinformação e a ingerência estrangeira**, 9 de setembro de 2021
- **Ingerência estrangeira e espionagem de personalidades políticas e instituições europeias**, 9 de setembro de 2021
- **A segurança das Instituições da UE: resposta à escalada de ciberataques**, 9 de setembro de 2021
- **Danos económicos causados pela ingerência estrangeira/desinformação, incluindo o mercado de dados**, 14 de outubro de 2021.

## **POSIÇÃO MINORITÁRIA DE CLARE DALY, EM NOME DO GRUPO THE LEFT**

A ingerência estrangeira provoca graves danos sociais e merece particular atenção, mas não é algo de novo nem afeta exclusivamente a Europa. De entre os exemplos de ingerência nos processos democráticos na União Europeia, o mais relevante e sistémico é o das grandes concentrações de capital, tanto estrangeiro como europeu, que influenciam a elaboração da legislação e a definição de políticas.

No entanto, este facto dificilmente é reconhecido pela maioria na Comissão Especial INGE, que preferiu prosseguir uma narrativa falaz de vitimização europeia às mãos de adversários geopolíticos perversos. A investigação foi utilizada para empolar as ameaças de ingerência russa e chinesa, ignorar as causas concretas da crise de legitimidade política na Europa, estigmatizar as posições divergentes em relação à política externa oficial da UE e utilizar motivos de segurança para impor restrições à liberdade de expressão e a outros direitos fundamentais.

O relatório daí resultante é de tal forma desprovido de bom senso e objetividade, que ele próprio constitui desinformação. O predomínio, no relatório, da referência a «conhecimentos especializados» de grupos de reflexão atlanticistas e da NATO, que exercem pressão a favor de interesses que beneficiam com o conflito, deve, ele próprio, ser considerado uma forma de ingerência estrangeira. A orientação política a que este relatório vincula a União é gravemente lesiva para o carácter democrático das sociedades europeias a longo prazo. As gerações futuras lamentarão a existência deste documento.

**INFORMAÇÕES SOBRE A APROVAÇÃO  
NA COMISSÃO COMPETENTE QUANTO À MATÉRIA DE FUNDO**

|  |   |
|--|---|
| <b>Data de aprovação</b>                               | 25.1.2022   |
| <b>Resultado da votação final</b>                      | +: 25<br>-: 8<br>0: 1   |
| <b>Deputados presentes no momento da votação final</b> | Vladimír Bilčík, Andrea Bocskor, Ioan-Rareș Bogdan, Jorge Buxadé Villalba, Włodzimierz Cimoszewicz, Gwendoline Delbos-Corfield, Anna Júlia Donáth, Marco Dreosto, Nicolaus Fest, Sunčana Glavak, Raphaël Glucksmann, Markéta Gregorová, Bart Groothuis, Balázs Hidvéghi, Sandra Kalniete, Andrey Kovatchev, Jeroen Lenaers, Nathalie Loiseau, Juan Fernando López Aguilar, Morten Løkkegaard, Pierfrancesco Majorino, Lukas Mandl, Thierry Mariani, Dace Melbārde, Maite Pagazaurtundúa, Tonino Picula, Manu Pineda, Robert Roos, Andreas Schieder, Sabine Verheyen, Viola Von Cramon-Taubadel, Javier Zarzalejos |
| <b>Suplentes presentes no momento da votação final</b> | Clare Daly, Petra Kammerevert   |

## VOTAÇÃO NOMINAL

|   |                    |
|---|--------------------|
| <b>Votação final – Projeto alterado (Votação nominal)</b> | <b>+</b><br>25/8/1 |
|---|--------------------|

### RESULTADOS DA VOTAÇÃO NOMINAL

#### Votação nominal: Votação final

| <b>25</b> | <b>+</b>   |
|-----------|--|
| ECR       | Dace Melbārde  |
| PPE       | Vladimír Bilčík, Ioan-Rareş Bogdan, Sunčana Glavak, Sandra Kalniete, Andrey Kovatchev, Jeroen Lenaers, Lukas Mandl, Sabine Verheyen, Javier Zarzalejos |
| Renew     | Anna Júlia Donáth, Bart Groothuis, Nathalie Loiseau, Morten Løkkegaard, Maite Pagazaurtundúa   |
| S&D       | Włodzimierz Cimoszewicz, Raphaël Glucksmann, Petra Kammerevert, Juan Fernando López Aguilar, Pierfrancesco Majorino, Tonino Picula, Andreas Schieder   |
| Verts/ALE | Gwendoline Delbos-Corfield, Markéta Gregorová, Viola Von Cramon-Taubadel   |

| <b>8</b> | <b>-</b>                           |
|----------|------------------------------------|
| ECR      | Jorge Buxadé Villalba, Robert Roos |
| ID       | Nicolaus Fest, Thierry Mariani     |
| NI       | Andrea Bocskor, Balázs Hidvéghi    |
| The Left | Clare Daly, Manu Pineda            |

| <b>1</b> | <b>0</b>      |
|----------|---------------|
| ID       | Marco Dreosto |