AUTORIDADE EUROPEIA PARA A PROTEÇÃO DE DADOS

Síntese do Parecer da AEPD sobre manipulação em linha e dados pessoais

(O texto integral do presente parecer encontra-se disponível em alemão, francês e inglês no sítio Web *da AEPD em www.edps.europa.eu)*

(2018/C 233/06)

A digitização da sociedade e da economia está a ter um impacto misto na participação cívica em processos de decisão e nos obstáculos ao envolvimento público em processos democráticos.

A análise dos grandes volumes de dados (*big data analytics*) e os sistemas de inteligência artificial tornaram possível reunir, combinar, analisar e armazenar, indefinidamente, grandes volumes de dados. Nas duas últimas décadas, emergiu o modelo de negócio dominante para a maioria dos serviços em linha que consiste em monitorizar as pessoas em linha e recolher dados sobre o seu caráter, saúde, relacionamentos, pensamentos e opiniões com o objetivo de gerar receita de publicidade digital. Estes mercados digitais têm vindo a concentrar-se à volta de umas poucas empresas que atuam como verdadeiros guardiães da Internet e dão origem a valores de capitalização de mercado ajustados pela inflação mais elevados do que qualquer outra empresa de que há registo histórico.

Este ecossistema digital ligou pessoas de todo o mundo, sendo que mais de 50 % da população tem acesso à Internet, ainda que de forma muito desigual no âmbito da geografia, riqueza e género. O otimismo inicial quanto ao potencial da Internet e das redes sociais para o envolvimento cívico deu lugar ao receio de que as pessoas sejam manipuladas: primeiro, através da constante recolha de informações, muitas vezes de natureza íntima; e, em seguida, através do controlo das informações que as pessoas veem na Internet de acordo com a categoria em que são classificadas. A indignação viral é para muitos serviços baseados em algoritmos um fator-chave de criação de valor, sendo que os produtos e as aplicações são concebidos para maximizar a atenção e a dependência. A interligação, pelo menos no modelo atual, levou à divisão.

O debate lançado tem girado em torno das informações enganosas, falsas ou caluniosas («conteúdos») que são oferecidas às pessoas com a intenção de influenciar o discurso político e as eleições, um fenómeno que veio a ser rotulado de «notícias falsas» ou «desinformação em linha». As soluções têm-se centrado em medidas de transparência que expõem a fonte da informação, mas descuram a responsabilização dos participantes do ecossistema que beneficiam com os comportamentos nocivos. Entretanto, a concentração do mercado e o aumento da hegemonia das plataformas representam uma nova ameaça ao pluralismo dos meios de comunicação. Para a AEPD, esta crise de confiança no ecossistema digital ilustra bem a dependência mútua entre a privacidade e a liberdade de expressão. A diminuição do espaço íntimo disponível para as pessoas, resultante da inevitável vigilância por empresas e governos, tem um efeito inibidor sobre a capacidade e a vontade das pessoas de se expressarem e de encetarem relações livremente, inclusive na esfera cívica tão essencial à saúde da democracia. Assim, o presente parecer refere-se ao modo como a informação pessoal é utilizada para segmentar indivíduos e grupos com conteúdos específicos, os direitos e valores fundamentais em jogo e a legislação relevante para mitigar as ameaças.

A AEPD apela há já vários anos a uma maior colaboração entre as autoridades de proteção de dados e outras entidades reguladoras para salvaguardar os direitos e os interesses dos indivíduos na sociedade digital, razão pela qual criou em 2017 a câmara de compensação digital (*Digital Clearinghouse*). Preocupados com o facto de as campanhas políticas poderem estar a explorar o espaço digital para contornar as leis em vigor, [1] acreditamos que é chegada a hora de alargar esta colaboração às autoridades reguladoras das eleições e do audiovisual.

1. POR QUE RAZÃO ESTAMOS A PUBLICAR O PRESENTE PARECER?

i. Intenso debate público em curso

Atualmente existe um intenso debate público acerca do impacto que o vasto e complexo ecossistema de informação digital tem, não só na economia de mercado, mas também na economia política, e de como o ambiente político interage com a economia. As principais plataformas encontram-se no centro deste ecossistema, beneficiando de forma desproporcionada com o crescimento da publicidade digital, e estão a aumentar o seu poder relativo à medida que este ecossistema evolui. Os dados pessoais são necessários para segmentar e personalizar mensagens dirigidas às pessoas, mas a maioria dos anunciantes desconhece o modo como essas decisões são tomadas e a maioria das pessoas desconhece que está a ser utilizada. O sistema recompensa o conteúdo sensacional e viral e, em geral, não distingue entre

[1] V., por exemplo, http://www.independent.co.uk/news/uk/politics/election-2017-facebook-ads-marginal-seats-tories-labour-outdated-election-spending-rules-a7733131.html [acedido em 18.3.2018].

anunciantes, sejam eles de natureza comercial ou política. As revelações acerca do modo como a desinformação deliberada («notícias falsas») está a ser propagada através deste sistema leva-nos a pensar que a integridade das democracias pode estar comprometida. Os sistemas de Inteligência Artificial — cujo mercado se caracteriza também pela concentração — são eles próprios alimentados por dados e, se não forem controlados, aumentarão o distanciamento e a falta de rigor dos processos de decisão neste contexto.

ii. **Relevância da lei de proteção de dados e campanhas políticas**

Os direitos fundamentais à privacidade e à proteção de dados são claramente um fator importante na correção desta situação, o que torna este assunto uma prioridade estratégica para todas as autoridades de proteção de dados independentes. Na sua *Resolution on the Use of Personal Data for Political Communication* [Resolução de 2005 relativa ao Uso de Dados Pessoais para Comunicação Política], as entidades reguladoras de proteção de dados expuseram preocupações mundiais importantes em matéria proteção de dados relacionadas com o aumento do tratamento de dados pessoais por participantes não comerciais. Foi referido especificamente o tratamento de «dados sensíveis relacionados com condenações ou atividades morais e políticas reais ou supostas, ou com atividades de votação» e à «definição invasiva do perfil de pessoas atualmente classificadas — muitas vezes, indevidamente ou com base em contactos superficiais — como simpatizantes, apoiantes, filiados ou partido» ([1]). A resolução internacional apelava à adoção de regras de proteção de dados sobre minimização dos dados, tratamento lícito, consentimento, transparência, direitos dos titulares de dados, limitação dos objetivos e a aplicação mais rigorosa das normas em matéria de segurança dos dados. É chegada a hora de renovar o apelo.

A legislação da UE em matéria de proteção de dados e confidencialidade das comunicações eletrónicas aplica-se à recolha de dados, à definição de perfis e à microssegmentação. Se for cumprida corretamente, deverá ajudar a minimizar os danos causados pelas tentativas de manipulação de indivíduos e de grupos. Os partidos políticos que tratam os dados dos eleitores na UE encontram-se abrangidos pelo RGPD (Regulamento Geral sobre a Proteção de Dados, Regulamento (UE) 2016/79). O RGPD classifica os dados pessoais que revelem opiniões políticas como categorias especiais de dados. O tratamento de tais dados está sujeito a uma proibição geral, salvo quando se aplique uma das exceções enumeradas. No contexto das campanhas políticas, as duas exceções seguintes são particularmente relevantes e merecem citação completa:

«d) Se o tratamento for efetuado, no âmbito das suas atividades legítimas e mediante garantias adequadas, por uma fundação, associação ou qualquer outro organismo sem fins lucrativos e que prossiga fins políticos, filosóficos, religiosos ou sindicais, e desde que esse tratamento se refira exclusivamente aos membros ou antigos membros desse organismo ou a pessoas que com ele tenham mantido contactos regulares relacionados com os seus objetivos, e que os dados pessoais não sejam divulgados a terceiros sem o consentimento dos seus titulares;

e) Se o tratamento se referir a dados pessoais que tenham sido manifestamente tornados públicos pelo seu titular; […].

g) Se o tratamento for necessário por motivos de interesse público importante, com base no direito da União ou de um Estado-Membro, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular dos dados.»

O considerando 56 esclarece o artigo 9.º, n.º 2, alínea g): «[s]empre que, no âmbito do exercício de atividades eleitorais, o funcionamento do sistema democrático num Estado-Membro exigir que os partidos políticos recolham dados pessoais sobre a opinião política dos cidadãos, o tratamento desses dados pode ser autorizado por motivos de interesse público, desde que sejam estabelecidas garantias adequadas».

Algumas autoridades de proteção de dados desenvolveram regras ou orientações relativas ao tratamento de dados para fins políticos:

— Em março de 2014, a autoridade de proteção de dados italiana, *Garante per la protezione dei dati personali*, adotou regras sobre o tratamento de dados pessoais pelos partidos políticos. As regras destacavam a proibição geral de utilizar dados pessoais divulgados na Internet, nomeadamente nas redes sociais ou em fóruns, para fins de comunicação política, caso esses dados tivessem sido recolhidos para outros fins ([2]).

— Em novembro de 2016, a comissão nacional de proteção de dados francesa (*Commission Nationale de l'Informatique et des Libertés*, CNIL) disponibilizou orientações adicionais às suas recomendações de 2012 sobre comunicação política que especificam as regras de tratamento dos dados pessoais nas redes sociais. Em especial, a CNIL sublinhou que a combinação de dados pessoais dos eleitores com o objetivo de definir os seus perfis e de monitorizá-los nas redes sociais só é lícita se baseada no consentimento enquanto fundamento para o tratamento dos dados ([3]).

([1]) Resolução disponível em língua inglesa aqui https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Use-of-Personal-Data-for-Polictical-Communication.pdf [accessed 18.3.2018].

([2]) http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3013267 «Provvedimento in materia di trattamento di dati presso i partiti politici e di esonero dall'informativa per fini di propaganda elettorale» publicado na Gazetta Ufficiale, número 71, em 26.3.2014 [docuje n.º 3013267].

([3]) https://www.cnil.fr/fr/communication-politique-quelles-sont-les-regles-pour-lutilisation-des-donnees-issues-des-reseaux «*Communication politique: quelles sont les règles pour l'utilisation des données issues des réseaux sociaux?*» publicado pela *Commission Nationale de l'informatique et des libertés* (Comissão Nacional Francesa de Informática e Liberdade) em 8.11.2016.

— Em abril de 2017, o organismo para a proteção dos dados do Reino Unido (*Information Commissioner's Office*, ICO) atualizou a *Guidance on political campaigning* [orientação em matéria de campanhas políticas], que também inclui orientações relativas ao uso da análise de dados nas campanhas políticas. O ICO explicou que quando uma organização política encomenda a um terceiro a análise de dados, este último é o subcontratante e a organização política, o responsável pelo tratamento. As disposições específicas da lei de proteção de dados que regem a relação entre o responsável pelo tratamento e o subcontratante devem ser cumpridas para que o tratamento de dados seja lícito ([1]).

As orientações das autoridades nacionais de proteção de dados podem proporcionar interpretações oficiais adicionais das disposições legais em matéria de proteção de dados e privacidade, o que explica as diferenças na organização dos sistemas políticos nacionais ([2]).

iii. **Objetivo do presente parecer da AEPD**

A AEPD tem como objetivo ajudar a UE a liderar pelo exemplo no diálogo global sobre a proteção de dados e a privacidade na era digital, identificando soluções políticas transdisciplinares para fazer face aos desafios dos grandes volumes de dados e desenvolvendo uma dimensão ética do tratamento de dados pessoais ([3]). Apelámos a que o titular dos dados seja tratado «como um indivíduo e não apenas como um consumidor ou utilizador» e assinalámos questões éticas relacionadas com os efeitos dos perfis preditivos e da personalização determinada por algoritmo ([4]). Apelámos ao desenvolvimento responsável e sustentável da sociedade digital baseada no controlo individual dos respetivos dados pessoais, numa engenharia e responsabilização conscientes da privacidade e na aplicação coerente das normas ([5]). O Grupo Consultivo de Ética da AEPD observou, no seu relatório de janeiro de 2018, que a «microssegmentação da campanha eleitoral altera as regras do discurso público, reduzindo o espaço de debate e o intercâmbio de ideias», o que «torna premente um debate democrático sobre a utilização e exploração de dados nas campanhas políticas e nos processos de decisão» ([6]).

A questão de usar informações e dados pessoais para manipular pessoas e políticas vai, naturalmente, muito além do direito à proteção de dados. Um ambiente em linha personalizado e microssegmentado cria «bolhas de filtro» em que as pessoas não só são expostas a informações «mais-do-mesmo», como também encontram menos opiniões, o que se traduz na maior polarização política e ideológica ([7]). O que intensifica o caráter difuso e persuasivo das histórias falsas e das conspirações ([8]). Estudos efetuados sugerem que a manipulação do *feed* de notícias ou dos resultados de pesquisa das pessoas pode influenciar o seu sentido de voto ([9]).

A AEPD pretende ajudar a garantir que o tratamento de dados pessoais na aceção do RGPD está ao serviço da humanidade e não o contrário ([10]). O progresso tecnológico não deve ser travado, mas direcionado de acordo com os nossos

([1]) https://ico.org.uk/media/for-organisations/documents/1589/promotion_of_a_political_party.pdf *Information Commissioner's Office* «*Guidance on political campaigning*» [20170426].

([2]) De acordo com o artigo 57.º, n.º 1, alínea d), do RGPD, «cada autoridade de controlo, no território respetivo […] promove a sensibilização dos responsáveis pelo tratamento e dos subcontratantes para as suas obrigações nos termos [deste] regulamento».

([3]) V. Liderar pelo exemplo: a Estratégia da AEPD para 2015-2019, p. 17. Em nosso entender, «o termo "Megadados" (*Big data*) refere-se à prática de combinar volumes colossais de informações provenientes de várias fontes e analisá-los, utilizando amiúde algoritmos inteligentes para esclarecer as decisões. Um dos principais valores dos megadados para empresas e governos provém da monitorização do comportamento humano, a nível coletivo e individual, e reside no seu potencial preditivo» (Parecer 4/2015 da AEPD sobre «Rumo a uma nova ética digital: dados, dignidade e tecnologia», 11.9.2015, p. 6).

([4]) A utilização de perfis para prever o comportamento das pessoas acarreta o risco de estigmatização, reforçando os estereótipos existentes, a segregação social e cultural e a exclusão, com essa «inteligência coletiva» a subverter a escolha individual e a igualdade de oportunidades. Essas «bolhas de filtro» ou «câmaras de eco pessoais» podem acabar por sufocar a criatividade, inovação e liberdades de expressão e associação que permitiram a expansão das tecnologias digitais (Parecer da AEPD 4/2015, p. 13, referências omitidas).

([5]) Parecer 7/2015 da AEPD sobre «Corresponder aos desafios dos grandes volumes de dados», p. 9.

([6]) Relatório do Grupo Consultivo de Ética da AEPD de janeiro de 2018 (disponível em língua inglesa), p. 28.

([7]) Ver, por exemplo, «The Economist, How the World Was Trolled» (4-10 de novembro de 2017), vol. 425, n.º 9065, p. 21-24.

([8]) Allcott H. and Gentzkow M., «Social Media and Fake News in the 2016 Election» (primavera de 2017). Stanford University, Journal of Economic Perspectives, Vol. 31, No. 2, págs. 211-236. https://web.stanford.edu/~gentzkow/research/fakenews.pdf, p. 219.

([9]) Numa das experiências, os utilizadores da plataforma social foram informados sobre o sentido de voto dos seus amigos, o que provocou um aumento estatisticamente significativo de um segmento da população (0,14 % da população em idade de votar ou cerca de 340 mil eleitores) a votar nas eleições intercalares para o Congresso, em 2010; Allcott H. e Gentzkow M., «Social Media and Fake News in the 2016 Election» (primavera de 2017), Universidade de Stanford, Journal of Economic Perspectives, vol. 31, n.º 2, p. 211-236., p. 219). Num outro estudo, os investigadores afirmaram que diferenças nos resultados de busca do Google podiam mudar o sentido de voto dos eleitores indecisos em 20 % dos casos: Zuiderveen Borgesius, F. & Trilling, D. e Möller, J. & Bodó, B. e de Vreese, C. & Helberger, N. (2016). «Should we worry about filter bubbles?», Internet Policy Review, 5(1). DOI: 10.14763/2016.1.401, p. 9.

([10]) Considerando 4 do 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 (a seguir «Regulamento Geral sobre a Proteção de Dados»).

valores. O respeito pelos direitos fundamentais, incluindo o direito à proteção de dados, é crucial para garantir a equidade das eleições, sobretudo quando nos aproximamos das eleições para o Parlamento Europeu de 2019 ([1]). O presente parecer é o mais recente de uma série de iniciativas importantes da AEPD relativas ao modo como deve ser aplicada a proteção de dados para responder às preocupações mais prementes em matéria de política pública. Baseia-se no trabalho anterior da AEPD sobre grandes volumes de dados e ética digital e na necessidade de coordenar a regulamentação de mercados competitivos e leais ([2]). O parecer resume, em primeiro lugar, o processo através do qual os dados pessoais alimentam e determinam o ciclo dominante da monitorização digital, microssegmentação e manipulação. Em seguida, considera os papéis dos vários intervenientes no ecossistema de informações digitais. Considera os direitos fundamentais em jogo, os princípios relevantes de proteção de dados e outras obrigações legais relevantes. Conclui referindo que o problema da manipulação em linha só poderá agravar-se; que nenhuma abordagem de regulação única será suficiente por si só e que os reguladores precisam, por isso, de colaborar urgentemente a fim de combater não apenas os abusos localizados, mas também as distorções estruturais causadas pela concentração excessiva do mercado.

7. **CONCLUSÃO**

A manipulação em linha representa uma ameaça para a sociedade porque as bolhas de filtro e as comunidades muradas dificultam o entendimento e a troca de experiências entre as pessoas. O enfraquecimento desta «cola social» pode comprometer a democracia, bem como vários outros direitos e liberdades fundamentais. A manipulação em linha também é um sintoma da opacidade e falta de responsabilidade no ecossistema digital. O problema é real e urgente, e é provável que se agrave à medida que mais pessoas e coisas se ligam à Internet, e o papel dos sistemas de Inteligência Artificial aumentam. Na raiz do problema, está, em parte, o uso irresponsável, ilegal ou antiético de informações pessoais. A transparência é necessária, mas não basta. A gestão de conteúdos pode ser necessária, mas não pode comprometer os direitos fundamentais. Parte da solução consiste, portanto, em aplicar as regras existentes, especialmente o RGPD, com rigor e em simultâneo com outras normas em matéria de eleições e de pluralismo dos meios de comunicação social.

Como contributo para aprofundar o debate, a AEPD organizará na primavera de 2019 um *workshop* em que os reguladores nacionais da área da proteção de dados e do direito eleitoral e audiovisual poderão explorar melhor estas interações, partilhar os desafios que enfrentam e delinear oportunidades para ações conjuntas tendo em consideração as próximas eleições para o Parlamento Europeu.

O presente Parecer demonstra que a tecnologia e o comportamento no mercado estão a causar danos, devido a distorções e desequilíbrios estruturais. Apelamos a ajustes nos incentivos à inovação. Os gigantes da tecnologia e os pioneiros têm beneficiado, até ao momento, do facto de operarem num ambiente relativamente desregulado. As indústrias tradicionais e os conceitos básicos de jurisdição territorial, soberania e também de normas sociais, incluindo a democracia, estão a ser afetadas. Estes valores dependem de uma pluralidade de vozes e do equilíbrio entre as partes. Nenhum interveniente ou setor individual pode enfrentar esta situação sozinho. A proteção de dados é parte da solução e talvez uma parte maior do que se poderia esperar. Não basta confiar na boa vontade dos participantes comerciais que não podem ser responsabilizados. Precisamos de agir com o objetivo de expandir, de forma mais justa, os benefícios da digitalização.

Feito em Bruxelas, em 19 de março de 2018.

Giovanni BUTTARELLI

Supervisor Europeu para a Proteção de Dados

([1]) Conforme declarado pelo Tribunal Europeu dos Direitos Humanos no caso Orlovskaya Iskra c. Rússia, «as eleições livres e a liberdade de expressão, especialmente a liberdade de debate político formam, em conjunto, a base de qualquer sistema democrático. Os dois direitos estão inter-relacionados e funcionam de modo a reforçarem-se um ao outro: por exemplo, a liberdade de expressão é uma das "condições" necessárias para "assegurar a livre expressão da opinião do povo na escolha da legislatura". Por essa razão, é particularmente importante, no período que antecede uma eleição, que as opiniões e informações de todos os tipos possam circular livremente. No contexto dos debates eleitorais, o exercício desimpedido da liberdade de expressão pelos candidatos tem particular significado» (referências omitidas do texto), n.º 110. http://hudoc.echr.coe.int/eng?i=001-171525.

([2]) 2014 — Parecer preliminar sobre «Privacidade e Competitividade na Era dos grandes volumes de dados»; 2015 — Parecer 4/2015 sobre «Rumo a uma nova ética digital. Dados, dignidade e tecnologia»; 2015 — Parecer 7/2015 sobre «Corresponder aos desafios dos grandes volumes de dados. Um apelo à transparência, controlo do utilizador, proteção de dados desde a conceção e responsabilidade»; 2016 — Parecer 8/2016 Parecer da AEPD sobre «A aplicação coerente dos direitos fundamentais na era dos grandes volumes de dados».