



Brussels, 12.9.2018
COM(2018) 638 final

Free and Fair elections

GUIDANCE DOCUMENT

**Commission guidance on the application of Union data protection law in the electoral
context**

*The European Commission's contribution to the Leaders' meeting in
Salzburg, 20 September 2018*

ORIENTAÇÕES DA COMISSÃO SOBRE A APLICAÇÃO DO DIREITO DA UNIÃO EM MATÉRIA DE PROTEÇÃO DE DADOS NO CONTEXTO ELEITORAL

A comunicação com o eleitorado constitui a base do processo democrático. É uma prática corrente os partidos políticos adaptarem a comunicação eleitoral às audiências, tendo em consideração os seus interesses específicos. É, pois, natural que os intervenientes nas eleições explorem as possibilidades de utilização de dados para ganhar votos. O advento das ferramentas digitais e das plataformas em linha gerou muitas novas oportunidades de interação com os cidadãos no debate político.

No entanto, o desenvolvimento do micro-direcionamento da publicidade junto dos eleitores com base no tratamento ilícito de dados pessoais, como se verificou no caso das revelações da *Cambridge Analytica*, é de natureza diferente. Ilustra os desafios colocados pelas tecnologias modernas, mas também demonstra a especial importância da proteção de dados no contexto eleitoral. Tornou-se uma questão fundamental não só para as pessoas, como também para o funcionamento das nossas democracias, uma vez que constitui uma grave ameaça a um processo eleitoral democrático e justo e é suscetível de minar um debate aberto, a equidade e a transparência, que são elementos essenciais numa democracia. A Comissão considera que é da máxima importância tratar este problema a fim de restabelecer a confiança do público na equidade do processo eleitoral.

Os primeiros relatórios da autoridade de proteção dos dados do Reino Unido (*Information Commissioner's Office* — ICO) sobre a utilização da analítica de dados em campanhas políticas¹ e o parecer da Autoridade Europeia para a Proteção de Dados sobre a manipulação em linha e os dados pessoais² confirmaram o crescente impacto do micro-direcionamento, inicialmente desenvolvido para fins comerciais, no contexto eleitoral.

De modo mais geral, várias autoridades de proteção de dados têm-se debruçado sobre a questão da proteção de dados no contexto eleitoral³.

O Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho (Regulamento Geral sobre a Proteção de Dados)⁴, que passou a ser diretamente aplicável em toda a União em 25

¹ Relatórios das autoridades de proteção dos dados do Reino Unido (*Information Commissioner's Office* – ICO) de 10 de julho de 2018: «Investigation into the use of data analytics in political campaigns – Investigation update» e «Democracy Disrupted? Personal information and political influence».

² https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf.

³ <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 no Jornal Oficial da Autoridade para a Proteção de Dados italiana, n.º 71 em 26.3.2014 [doc. web n. 3013267]; <https://www.cnil.fr/fr/communication-politique-queles-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 Comissão Nacional de Informática e das Liberdades francesa (Commission Nationale de l'informatique et des libertés) de 8.11.2016; https://ico.org.uk/media/for-organisations/documents/1589/promotion_of_a_political_party.pdf Information Commissioner's Office «Guidance on political campaigning» [20170426].

⁴ Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (JO L 119 de 4.5.2016, p. 1).

de maio de 2018, dota a União dos instrumentos necessários para lidar com casos de utilização ilícita de dados pessoais no contexto eleitoral. No entanto, só uma aplicação firme e coerente das regras contribuirá para proteger a integridade de uma política democrática. Dado que é a primeira vez que estas regras serão aplicadas no contexto eleitoral europeu por ocasião das próximas eleições para o Parlamento Europeu, é importante proporcionar clareza aos intervenientes nos processos eleitorais — como autoridades eleitorais nacionais, partidos políticos, corretores e analistas de dados, plataformas de comunicação social e redes de publicidade em linha. Por conseguinte, o objetivo das presentes orientações é salientar as obrigações em matéria de proteção de dados relevantes para as eleições. As autoridades nacionais de proteção de dados, na sua qualidade de entidades responsáveis pela aplicação do Regulamento Geral sobre a Proteção de Dados, devem utilizar plenamente os seus poderes reforçados no tratamento de possíveis infrações, nomeadamente as ligadas ao micro-direcionamento da publicidade junto dos eleitores.

1. Quadro da União em matéria de proteção de dados

A proteção dos dados pessoais é um direito fundamental consagrado na Carta dos Direitos Fundamentais da União Europeia (artigo 8.º) e nos Tratados (artigo 16.º do TFUE). O Regulamento Geral sobre a Proteção de Dados reforça o quadro em matéria de proteção de dados, dotando a União de melhores meios para lidar com futuros casos de abuso de dados pessoais e responsabilizando mais fortemente todos os intervenientes quanto à forma como tratam os dados pessoais.

Confere às pessoas na União direitos adicionais e reforçados que são particularmente relevantes no contexto eleitoral. Um dos problemas do regime de proteção de dados em vigor na União nos últimos 20 anos tem sido, em especial, a aplicação fragmentada das regras entre os Estados-Membros, a ausência de quaisquer mecanismos formalizados de cooperação entre autoridades nacionais de proteção de dados e os poderes de execução limitados dessas autoridades. O Regulamento Geral sobre a Proteção de Dados aborda estas insuficiências: com base nos princípios comprovados de proteção de dados, harmoniza noções essenciais como o consentimento, reforça os direitos das pessoas a receberem informações sobre o tratamento dos seus dados, clarifica as condições em que os dados pessoais podem ser partilhados ulteriormente, introduz regras sobre violações de dados pessoais, estabelece um mecanismo de cooperação entre as autoridades de proteção de dados em casos transfronteiras e reforça os seus poderes de execução. Em caso de violação das regras da UE em matéria de proteção de dados, as autoridades de proteção de dados têm poderes para investigar (por exemplo, ordenando o fornecimento de informações, realizando inspeções nas instalações dos responsáveis pelo tratamento e subcontratantes) e corrigir comportamentos (por exemplo, emitindo avisos e reprimendas ou impondo uma suspensão temporária ou definitiva do tratamento de dados). Estão também habilitados a aplicar coimas até 20 milhões de EUR ou, no caso de uma empresa, até 4 % do seu volume de negócios a nível mundial⁵. Ao decidir

⁵ Orientações da Comissão relativas ao Regulamento Geral sobre a Proteção de Dados em: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_pt.

sobre a aplicação de coimas e respetivo nível, as autoridades de proteção de dados terão em conta as circunstâncias do caso concreto e fatores como a natureza, o âmbito ou o objetivo do tratamento de dados, o número de pessoas afetadas e o nível de danos por estas sofridos⁶. No contexto eleitoral, é provável que a gravidade da infração e o número de pessoas afetadas seja elevado. Tal poderá levar à imposição de coimas elevadas, nomeadamente tendo em conta a importância da questão da confiança dos cidadãos no processo democrático.

O recém-criado Comité Europeu para a Proteção de Dados, que reúne as autoridades nacionais de proteção de dados bem como a Autoridade Europeia para a Proteção de Dados, desempenha um papel fundamental na aplicação do Regulamento Geral sobre a Proteção de Dados mediante a formulação de orientações, recomendações e melhores práticas⁷. Enquanto garantes da execução do Regulamento Geral sobre a Proteção de Dados e de contactos diretos junto das partes interessadas, as autoridades nacionais de proteção de dados são as entidades mais bem colocadas para proporcionar segurança jurídica adicional no que diz respeito à interpretação do regulamento. A Comissão apoia ativamente esse trabalho.

A Diretiva Privacidade e Comunicações Eletrónicas (Diretiva 2002/58/CE do Parlamento Europeu e do Conselho⁸) completa o quadro da União em matéria de proteção de dados e é relevante no contexto eleitoral, dado que abrange regras sobre o envio eletrónico de comunicações não solicitadas, inclusivamente para fins de comercialização direta. A Diretiva Privacidade Eletrónica estabelece também regras sobre o armazenamento de informações e o acesso às informações já armazenadas, tais como testemunhos de conexão («cookies»), que podem ser utilizados para seguir o comportamento em linha de um utilizador, em equipamento terminal como um telefone inteligente ou um computador. A proposta da Comissão de um regulamento relativo à privacidade e às comunicações eletrónicas, («Regulamento Privacidade e Comunicações Eletrónicas»)⁹, atualmente em negociação, baseia-se nos mesmos princípios que a Diretiva Privacidade e Comunicações Eletrónicas. O novo regulamento não será apenas aplicável aos operadores de telecomunicações tradicionais, sendo o seu âmbito alargado a serviços de comunicações eletrónicas baseadas na Internet.

2. Principais obrigações dos vários intervenientes

O Regulamento Geral sobre a Proteção de Dados é aplicável a todos os que participam ativamente no contexto eleitoral, tais como partidos políticos europeus e nacionais (seguidamente designados: «partidos políticos») e fundações políticas nacionais (a seguir designadas: «fundações»), plataformas, empresas de análise de dados e autoridades públicas responsáveis pelo processo eleitoral. Estes devem proceder ao tratamento de dados pessoais (por exemplo, nomes e endereços) de uma forma lícita, leal e transparente, apenas para os fins

⁶ Artigo 83.º do Regulamento Geral sobre a Proteção de Dados.

⁷ A Autoridade Europeia para a Proteção de Dados também emite pareceres.

⁸ 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 (Diretiva relativa à privacidade e às comunicações eletrónicas) (JO L 201 de 31.7.2002, p. 37).

⁹ Proposta de Regulamento do Parlamento Europeu e do Conselho relativo ao respeito pela vida privada e à proteção dos dados pessoais nas comunicações eletrónicas e que revoga a Diretiva 2002/58/CE (Regulamento relativo à privacidade e às comunicações eletrónicas), COM(2017) 10 final.

especificados. Não podem utilizá-los posteriormente de uma forma incompatível com as finalidades para as quais os dados foram inicialmente recolhidos. O tratamento para fins jornalísticos também está abrangido pelo Regulamento Geral sobre a Proteção de Dados, em princípio, mas pode beneficiar de isenções e derrogações conforme previsto na legislação nacional, tendo em conta a importância do direito à liberdade de expressão e informação numa sociedade democrática¹⁰.

A noção de dados pessoais é vasta. Entende-se por «dados pessoais» a informação relativa a uma pessoa singular identificada ou identificável. Os dados tratados no contexto eleitoral incluirão frequentemente categorias especiais de dados pessoais («dados sensíveis») como, por exemplo, opiniões políticas, filiação sindical, origem étnica, vida sexual, etc., que beneficiam de um regime mais protetor¹¹. Além disso, a análise de dados pode inferir «dados sensíveis» (tais como opiniões políticas, mas também crenças religiosas ou orientação sexual) a partir de séries de dados não sensíveis. O tratamento desses dados inferidos também está abrangido pelo Regulamento Geral sobre a Proteção de Dados e deve, por conseguinte, respeitar todas as normas em matéria de proteção de dados.

Em conclusão, praticamente todas as operações de tratamento de dados no contexto eleitoral estão abrangidas pelo Regulamento Geral sobre a Proteção de Dados.

Tendo em conta a necessidade de proporcionar maior clareza a todos os intervenientes implicados no processo eleitoral e as primeiras conclusões no caso da *Cambridge Analytica*, as secções que se seguem salientam as obrigações em matéria de proteção de dados que se afiguram de particular relevância no contexto eleitoral. No anexo é apresentada uma síntese dessas obrigações.

2.1 Responsáveis pelo tratamento de dados e subcontratantes

A noção de obrigação de prestação de contas a que estão sujeitos os responsáveis pelo tratamento de dados e os responsáveis conjuntos pelo tratamento de dados constitui um elemento essencial do Regulamento Geral sobre a Proteção de Dados. O responsável pelo tratamento de dados é a organização que decide, por si mesma ou em colaboração com outras, a razão e o modo como os dados pessoais são tratados; o subcontratante de dados procede ao tratamento dos pessoais exclusivamente em nome, e sob as instruções, do responsável pelo tratamento de dados (sendo a sua relação determinada num contrato ou noutro ato jurídico vinculativo). Os responsáveis pelo tratamento de dados devem estabelecer medidas adequadas aos riscos, implementar a proteção de dados desde a conceção e estar em condições de demonstrar a conformidade do tratamento com o Regulamento Geral sobre a Proteção de Dados (princípio da responsabilidade).

O papel do responsável pelo tratamento de dados ou do subcontratante deve ser avaliado em cada caso concreto. No contexto eleitoral, os responsáveis pelo tratamento de dados podem ser vários intervenientes: os partidos políticos, os candidatos a título individual e as fundações

¹⁰ Artigo 85.º, n.º 2, do Regulamento Geral sobre a Proteção de Dados.

¹¹ Artigo 9.º, n.º 1, do Regulamento Geral sobre a Proteção de Dados.

são, na maioria dos casos, os responsáveis pelo tratamento de dados; as plataformas e empresas de analítica de dados podem ser responsáveis (conjuntos) pelo tratamento ou subcontratantes em relação a um determinado tratamento em função do grau do seu controlo sobre o tratamento em causa¹²; as autoridades eleitorais nacionais são responsáveis pelo tratamento de dados no que diz respeito aos cadernos eleitorais.

Quando as suas atividades de tratamento de dados estão relacionadas com a oferta de bens e serviços a pessoas na União ou com o controlo do seu comportamento na União, as empresas com sede fora da União têm também de cumprir o Regulamento Geral sobre a Proteção de Dados. É este o caso de uma série de plataformas e empresas de analítica de dados.

2.2 Princípios, licitude do tratamento e condições especiais aplicáveis a «dados sensíveis»

Os intervenientes nas eleições só podem proceder ao tratamento de dados pessoais, incluindo os dados obtidos a partir de fontes públicas, em conformidade com os princípios relativos ao tratamento de dados pessoais e com base num número limitado de motivos claramente definidos no Regulamento Geral sobre a Proteção de Dados¹³. Os motivos mais relevantes para tratamento lícito no contexto eleitoral parecem ser o consentimento de uma pessoa, o cumprimento de uma obrigação legal ao abrigo do direito da União ou da legislação nacional, o desempenho de uma missão levada a cabo no interesse público e o interesse legítimo de um dos intervenientes. No entanto, os intervenientes no contexto eleitoral só podem invocar o motivo de interesse legítimo se aos seus interesses não se sobrepuserem os interesses ou os direitos e liberdades fundamentais das pessoas em causa.

Além disso, o armazenamento de informações, ou o acesso a informações já armazenadas no equipamento terminal (computador, telemóvel inteligente, etc.) deve obedecer aos requisitos da Diretiva Privacidade e Comunicações Eletrónicas relativos à proteção dos equipamentos terminais, o que significa que a pessoa em causa teria de dar o seu consentimento.

Quando o consentimento é utilizado como fundamento jurídico, o Regulamento Geral sobre a Proteção de Dados estabelece que este seja dado por um ato positivo inequívoco e que seja livre e informado¹⁴.

As autoridades públicas envolvidas no contexto eleitoral procedem ao tratamento de dados pessoais a fim de dar cumprimento a uma obrigação legal ou exercer uma missão pública. Outros intervenientes no contexto eleitoral podem proceder ao tratamento de dados por motivos de consentimento ou de interesse legítimo¹⁵. Os partidos políticos e as fundações

¹² A jurisprudência recente do Tribunal de Justiça da União Europeia (processo C-25/17, Testemunhas de Jeová, acórdão de 10 de julho de 2018) clarificou que uma organização que «exerce influência» numa atividade de recolha e tratamento de dados pessoais pode, em determinadas circunstâncias, ser considerada um responsável pelo tratamento de dados.

¹³ Artigos 5.º e 6.º do Regulamento Geral sobre a Proteção de Dados.

¹⁴ Artigo 7.º e artigo 4.º, n.º 11, do Regulamento Geral sobre a Proteção de Dados.

¹⁵ Sob reserva de os direitos e as liberdades das pessoas em causa não serem gravemente afetados.

políticas podem também proceder ao tratamento de dados por motivos de interesse público quando previsto no direito nacional¹⁶.

As autoridades públicas só podem divulgar aos partidos políticos determinadas informações sobre pessoas que figuram nas listas eleitorais ou em registos de residentes quando expressamente autorizados pelo direito do Estado-Membro e apenas para fins de publicidade no contexto eleitoral e na medida do necessário para o efeito, como o nome e o endereço.

O tratamento de dados no contexto eleitoral implicará frequentemente «dados sensíveis». O tratamento desses dados, incluindo «dados sensíveis» inferidos, é em geral proibido, exceto quando é aplicável uma das justificações específicas previstas no Regulamento Geral sobre a Proteção de Dados¹⁷. O tratamento de «dados sensíveis» exige o cumprimento de condições específicas e mais rigorosas: a pessoa deve ter dado o seu consentimento explícito¹⁸ ou ter tornado públicos os dados em causa¹⁹. Os partidos políticos e as fundações políticas podem também proceder ao tratamento de «dados sensíveis» em caso de interesse público substancial ao abrigo do direito da União ou do Estado-Membro e se estiverem estabelecidas as garantias necessárias²⁰. O Regulamento Geral sobre a Proteção de Dados estabelece que estes podem também tratar «dados sensíveis» na medida em que dizem respeito apenas aos seus membros ou antigos membros ou a pessoas que tenham contactos regulares com os mesmos — mas apenas para comunicação dentro do seu partido político ou fundação política²¹. Todavia, esta disposição específica não pode ser utilizada por um partido político para tratamento de dados de potenciais membros ou eleitores.

A finalidade do tratamento de dados deve ser especificada no momento da recolha (princípio de «limitação das finalidades»)²². Os dados recolhidos para uma finalidade só podem ser objeto de tratamento posterior para uma finalidade compatível; caso contrário, tem de ser estabelecido um novo fundamento jurídico, previsto no Regulamento Geral sobre a Proteção de Dados, como o consentimento, a fim de permitir o tratamento para a nova finalidade. Em especial, quando os corretores ou plataformas recolhem dados sobre estilos de vida, esses dados não podem ser sujeitos a tratamento posterior no contexto eleitoral.

A menos que exerçam a devida diligência e verifiquem que os dados foram obtidos legalmente, os partidos políticos e as fundações políticas não podem utilizar os dados assim recebidos de um terceiro.

¹⁶ Ver o considerando 56 do Regulamento Geral sobre a Proteção de Dados em que «sempre 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.»

¹⁷ Artigo 9.º do Regulamento Geral sobre a Proteção de Dados.

¹⁸ Artigo 9.º, n.º 2, alínea a), do Regulamento Geral sobre a Proteção de Dados.

¹⁹ Artigo 9.º, n.º 2, alínea e), do Regulamento Geral sobre a Proteção de Dados.

²⁰ Artigo 9.º, n.º 2, alínea g), do Regulamento Geral sobre a Proteção de Dados.

²¹ Artigo 9.º, n.º 2, alínea d), do Regulamento Geral sobre a Proteção de Dados. Um partido político ou a fundação política não pode partilhar com terceiros os dados relativos aos seus membros ou antigos membros, ou a pessoas que tenham contactos regulares com estes, sem o consentimento da pessoa em causa.

²² Artigo 5.º, n.º 1, alínea b), do Regulamento Geral sobre a Proteção de Dados.

2.3 Requisitos em matéria de transparência

O caso da *Cambridge Analytica* demonstrou a importância de combater a opacidade e de informar devidamente as pessoas em causa. Frequentemente, as pessoas não sabem quem trata os seus dados pessoais e para que finalidades. Os princípios do tratamento equitativo e transparente exigem que as pessoas sejam informadas da operação de tratamento de dados e das suas finalidades²³. O Regulamento Geral sobre a Proteção de Dados clarifica as obrigações dos responsáveis pelo tratamento de dados sobre esta matéria. Devem informar as pessoas sobre os aspetos-chave relacionados com o tratamento dos seus dados pessoais, tais como:

- a identidade do responsável pelo tratamento de dados;
- as finalidades do tratamento;
- os destinatários dos dados pessoais;
- a fonte dos dados, quando não recolhidos diretamente do próprio;
- a existência de decisões automatizadas e
- quaisquer outras informações necessárias para assegurar um tratamento equitativo e transparente²⁴.

Além disso, o Regulamento Geral sobre a Proteção de Dados estabelece que as informações devem ser dadas de uma forma concisa, transparente, inteligível e facilmente acessível, utilizando uma linguagem clara e simples²⁵. Por exemplo, um aviso opaco e sucinto sobre proteção de dados impresso apenas em caracteres pequenos no material eleitoral não satisfaria os requisitos de transparência.

De acordo com as conclusões preliminares, o facto de as informações sobre a finalidade da recolha de dados estarem incompletos foi uma das principais lacunas no caso *Cambridge Analytica*, o qual pôs também em causa a validade do consentimento das pessoas em causa. Todas as organizações que tratam dados pessoais no contexto eleitoral têm de garantir que as pessoas compreendem plenamente como e para que finalidades serão utilizados os seus dados pessoais, antes de darem o seu consentimento ou antes do início do tratamento pelo responsável pelo tratamento de dados por qualquer outro motivo para o tratamento.

Devem ser fornecidas informações às pessoas em cada fase do tratamento, não apenas no momento da recolha dos dados.

Em especial, quando procedem ao tratamento dos dados obtidos de fontes de países terceiros (como a partir de registos eleitorais, corretores de dados, analistas de dados e outras fontes), os partidos políticos devem normalmente informar e explicar às pessoas em causa o modo

²³ Artigo 5.º, n.º 1, alínea a), do Regulamento Geral sobre a Proteção de Dados.

²⁴ Artigos 13.º e 14.º do Regulamento Geral sobre a Proteção de Dados.

²⁵ Orientações do Comité Europeu para a Proteção de Dados em matéria de transparência.

como combinam e utilizam esses dados a fim de assegurar o tratamento equitativo dos dados²⁶.

2.4 Definição de perfis, decisões automatizadas e micro-direcionamento

A definição de perfis é a forma de tratamento automatizado dos dados utilizada para analisar ou prever aspetos relacionados, por exemplo, com preferências pessoais, interesses, situação económica, etc.²⁷. A definição de perfis pode ser utilizada no micro-direcionamento para pessoas específicas, nomeadamente para analisar dados pessoais (tais como um historial de pesquisas na Internet) a fim de identificar os interesses particulares de uma pessoa ou público específico com vista a influenciar as suas ações. O micro-direcionamento pode ser utilizado para enviar uma mensagem personalizada a uma pessoa ou a um público através de um serviço em linha, por exemplo, redes sociais.

O caso da *Cambridge Analytica* revelou os desafios específicos suscitados pelos métodos de micro-direcionamento nas redes sociais. As organizações podem proceder à extração dos dados recolhidos dos utilizadores das redes sociais para gerar os perfis dos votantes. Tal poderia permitir a essas organizações identificar eleitores que podem ser mais facilmente influenciados e, por conseguinte, permitir a essas organizações exercerem uma influência no resultado das eleições.

Todos os princípios e regras gerais do Regulamento Geral sobre a Proteção de Dados são aplicáveis a esse tratamento de dados, como os princípios da licitude, equidade, transparência e limitação das finalidades. As pessoas não estão frequentemente conscientes que são objeto de definição de perfis: não compreendem por que razão recebem publicidade tão claramente relacionada com as suas últimas pesquisas ou mensagens personalizadas de diferentes organizações. O Regulamento Geral sobre a Proteção de Dados estabelece que todos os responsáveis pelo tratamento dos dados, por exemplo partidos políticos ou analistas de dados, têm a obrigação de informar as pessoas quando utilizam essas técnicas e sobre as suas consequências²⁸.

O Regulamento Geral sobre a Proteção de Dados reconhece que as decisões automatizadas, incluindo a definição de perfis, podem ter consequências graves. O Regulamento Geral sobre a Proteção de Dados estabelece que uma pessoa tem o direito de não ficar sujeita a qualquer decisão tomada exclusivamente com base no tratamento automatizado e que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar, a menos que esse tratamento seja efetuado em condições rigorosas, nomeadamente quando a pessoa dá o seu consentimento explícito ou quando tal é permitido pelo direito da União ou do Estado-Membro que estabelece garantias adequadas²⁹.

As práticas de micro-direcionamento no contexto eleitoral inserem-se nesta categoria quando produzem efeitos suficientemente significativos nas pessoas. O Comité Europeu para a

²⁶ Artigo 14.º do Regulamento Geral sobre a Proteção de Dados.

²⁷ Conforme definido no artigo 4.º, n.º 4, do Regulamento Geral sobre a Proteção de Dados.

²⁸ Artigo 13.º, n.º 2, do Regulamento Geral sobre a Proteção de Dados.

²⁹ Artigo 22.º do Regulamento Geral sobre a Proteção de Dados.

Proteção de Dados declarou que este é o caso quando a decisão é suscetível de afetar significativamente as circunstâncias, o comportamento ou as escolhas das pessoas ou de ter um impacto prolongado ou permanente na pessoa³⁰. O Comité considerou que a publicidade direcionada em linha seria suscetível, em determinadas circunstâncias, de afetar significativamente as pessoas quando, por exemplo, é intrusiva ou explora as vulnerabilidades conhecidas das pessoas. Dada a importância do exercício do direito democrático de voto, mensagens personalizadas que possam, por exemplo, fazer com que as pessoas não votem ou fazê-las votar de uma forma específica, são suscetíveis de preencher o critério de efeito significativo.

Por conseguinte, no contexto eleitoral, os responsáveis pelo tratamento de dados devem assegurar que qualquer tratamento que utilize essas técnicas seja lícito nos termos dos princípios e condições rigorosas supramencionados do Regulamento Geral sobre a Proteção de Dados.

2.5 Segurança e exatidão dos dados pessoais

A segurança reveste-se de especial importância no contexto eleitoral, dada a dimensão dos conjuntos de dados envolvidos e o facto de esses conjuntos conterem frequentemente «dados sensíveis». O Regulamento Geral sobre a Proteção de Dados estabelece que os operadores que tratam dados pessoais (tanto os responsáveis pelo tratamento como os subcontratantes) devem aplicar medidas técnicas e organizativas adequadas para assegurar um nível de segurança apropriado aos riscos colocados pelo tratamento no que diz respeito aos direitos e liberdades das pessoas³¹.

O Regulamento Geral sobre a Proteção de Dados estabelece que os responsáveis pelo tratamento de dados devem notificar violações de dados pessoais à autoridade de controlo competente sem demora injustificada e, o mais tardar, no prazo de 72 horas. Quando a violação dos dados pessoais for suscetível de implicar um elevado risco para os direitos e as liberdades das pessoas, o responsável pelo tratamento deve informar as pessoas afetadas pela violação de dados sem demora injustificada³².

Os partidos políticos e outros intervenientes no processo eleitoral devem ter especial cuidado em assegurar a exatidão dos dados pessoais quando estão em causa grandes conjuntos de dados e quando os dados são compilados a partir de fontes diferentes e heterogéneas. Os dados inexatos devem ser imediatamente apagados ou retificados e, se necessário, atualizados.

2.6 Avaliação de impacto sobre a proteção de dados

O Regulamento Geral sobre a Proteção de Dados introduz um novo instrumento para a avaliação dos riscos antes do início do tratamento de dados: a avaliação de impacto sobre a

³⁰ Orientações do Comité Europeu para a Proteção de Dados em matéria de decisões automatizadas, WP251rev.01 com a última redação revista e adotada em 6.2.2018.

³¹ Artigo 32.º do Regulamento Geral sobre a Proteção de Dados.

³² Artigos 33.º e 34.º do Regulamento Geral sobre a Proteção de Dados e Orientações do Comité Europeu para a Proteção de Dados em matéria de notificação da violação de dados pessoais.

proteção de dados. Esta avaliação é necessária quando o tratamento é suscetível de implicar um elevado risco para os direitos e as liberdades das pessoas³³. É este o caso no contexto eleitoral quando um responsável pelo tratamento de dados avalia, de forma sistemática e extensiva, aspetos pessoais de uma pessoa (incluindo a definição de perfis) que afetam significativamente a pessoa e quando o responsável pelo tratamento procede ao tratamento de «dados sensíveis» em larga escala. As autoridades eleitorais nacionais atuando no exercício das suas missões públicas poderiam não ter de efetuar uma avaliação de impacto sobre a proteção de dados se uma tal avaliação já tiver sido efetuada no contexto da adoção de legislação.

As avaliações de impacto a realizar pelos diferentes intervenientes no contexto eleitoral devem incluir os elementos necessários para enfrentar os riscos associados a esse tratamento, nomeadamente a licitude do tratamento também em relação a conjuntos de dados obtidos de terceiros e os requisitos de transparência.

3. Direitos das pessoas

O Regulamento Geral sobre a Proteção de Dados confere às pessoas direitos adicionais e reforçados, que são particularmente relevantes no contexto eleitoral:

- o direito de acesso aos seus dados pessoais;
- o direito de solicitar a supressão dos seus dados pessoais se o tratamento tiver por base o consentimento e esse for retirado, se os dados já não forem necessários ou se o tratamento for ilícito e
- o direito à correção dos dados pessoais incorretos, inexatos ou incompletos.

As pessoas têm também o direito de se opor ao tratamento (por exemplo dos dados incluídos nas listas eleitorais transmitidas aos partidos políticos) se o tratamento dos seus dados pessoais tiver por motivo o «interesse legítimo» ou o «interesse público».

As pessoas têm o direito de não serem objeto de decisões baseadas unicamente no tratamento automatizado dos seus dados pessoais. Em tais casos, a pessoa pode solicitar a intervenção de uma pessoa singular e tem o direito de exprimir o seu ponto de vista e de contestar a decisão.

Para que as pessoas possam exercer esses direitos, todos os intervenientes têm de fornecer as ferramentas e parâmetros necessários. O Regulamento Geral sobre a Proteção de Dados prevê a possibilidade de elaboração de um código de conduta aprovado por uma autoridade de proteção de dados que especifique a aplicação do regulamento em domínios específicos, nomeadamente no contexto eleitoral.

O Regulamento Geral sobre a Proteção de Dados concede às pessoas o direito de apresentar uma reclamação a uma autoridade de controlo e o direito a recurso judicial. Também confere às pessoas o direito de mandar uma organização não governamental a apresentar uma

³³ Artigos 35.º e 36.º do Regulamento Geral sobre a Proteção de Dados e Orientações do Comité Europeu para a Proteção de Dados em matéria de avaliação de impacto sobre a proteção de dados.

reclamação em seu nome³⁴. Em determinados Estados-Membros, a legislação nacional permite a uma organização não governamental apresentar uma reclamação sem ser mandatada por uma pessoa. Este aspeto é particularmente relevante no contexto eleitoral, dado o grande número de pessoas potencialmente afetadas.

³⁴ Artigo 80.º, n.º 1, do Regulamento Geral sobre a Proteção de Dados.

Principais questões em matéria de proteção de dados relevantes no processo eleitoral³⁵

<p>Partidos políticos e fundações políticas</p>	<p>Os partidos políticos e as fundações políticas são responsáveis pelo tratamento dos dados</p> <ul style="list-style-type: none"> • Cumprem o princípio de limitação das finalidades, procedendo a tratamento posterior apenas para finalidades compatíveis (por exemplo, quando da partilha de dados com plataformas) • Escolhem a base jurídica adequada para o tratamento (também de dados inferidos): consentimento, interesse legítimo, missão de interesse público (se prevista na lei), condições específicas de «dados sensíveis» (por exemplo: opinião política) • Realizam uma avaliação de impacto sobre a proteção de dados • Informam as pessoas sobre cada finalidade do tratamento (requisitos de transparência), quer quando da recolha de dados diretamente ou quando da sua obtenção junto de terceiros • Asseguram a exatidão dos dados, em particular no que diz respeito aos dados provenientes de diferentes fontes e aos dados inferidos • Verificam se os dados recebidos de terceiros foram obtidos legalmente e para que finalidades (por exemplo: se as pessoas em causa deram o seu consentimento informado para uma determinada finalidade) • Têm em conta os riscos específicos da definição de perfis e estabelecem garantias adequadas • Respeitam condições específicas quando da utilização de decisões automatizadas (por exemplo, obtêm o consentimento explícito e aplicam garantias adequadas) • Identificam claramente quem tem acesso aos dados • Garantem a segurança do tratamento através de medidas técnicas e organizativas • Comunicam violações de dados • Clarificam obrigações em contratos ou noutros atos juridicamente vinculativos celebrados com os responsáveis pelo tratamento de dados, tais como empresas de análise de dados • Apagam os dados quando já não são necessários para a finalidade inicial para a qual foram recolhidos
<p>Corretores de dados e empresas de</p>	<p>Os corretores de dados e as empresas de análise de dados são responsáveis (conjuntos) ou subcontratantes em função do grau de controlo que têm sobre o tratamento</p>

³⁵ As informações supra não são de modo algum exaustivas. O seu objetivo é destacar uma série de obrigações importantes relacionadas com dados abrangidos pelo Regulamento Geral sobre a Proteção de Dados que sejam relevantes no processo eleitoral. Correspondem a um cenário em que os partidos políticos estão eles próprios a recolher dados (a partir de fontes públicas, da sua presença em redes sociais, diretamente dos eleitores, etc.) e utilizam o serviço de corretores de dados ou de empresas de análise de dados com o objetivo de visar eleitores através de plataformas de redes sociais. As plataformas podem também ser uma fonte de dados para os intervenientes supramencionados. Outras disposições legislativas podem também ser relevantes, tais como as regras relativas ao envio de comunicações não solicitadas e à proteção dos equipamentos terminais na Diretiva Privacidade e Comunicações Eletrónicas.

analítica de dados	Como responsável pelo tratamento de dados	Como subcontratante de tratamento de dados
	<ul style="list-style-type: none"> • Cumprem o princípio de limitação das finalidades, procedendo a tratamento posterior apenas para finalidades compatíveis (por exemplo, quando da partilha de dados com terceiros) • Escolhem a base jurídica adequada para o tratamento: consentimento, interesse legítimo. Em caso de «dados sensíveis», o tratamento só é possível se o consentimento for explícito ou os dados tiverem sido manifestamente tornados públicos • Realizam uma avaliação de impacto sobre a proteção de dados • Informam as pessoas sobre cada finalidade do tratamento (requisitos de transparência) — em especial quando é solicitado o consentimento, dado que geralmente os dados serão vendidos a um terceiro • Respeitam condições específicas quando da utilização de decisões automatizadas (por exemplo, obtêm o consentimento explícito e aplicam garantias adequadas) • Prestam especial atenção à licitude do tratamento e à exatidão quando da combinação de diferentes conjuntos de dados • Garantem a segurança do tratamento através de medidas técnicas e organizativas • Comunicam violações de dados 	<ul style="list-style-type: none"> • Cumprem as obrigações decorrentes do contrato ou de outro ato jurídico vinculativo celebrado com o responsável pelo tratamento dos dados • Garantem a segurança do tratamento através de medidas técnicas e organizativas • Apoiam o responsável pelo tratamento na avaliação de impacto sobre a proteção de dados, no exercício dos direitos dos titulares dos dados ou na comunicação ao responsável pelo tratamento de uma violação de dados, sem demora, se tiverem disso conhecimento
	<p>Geralmente, as plataformas funcionam como responsáveis pelo tratamento de dados relativamente ao tratamento realizado nas suas plataformas e, possivelmente, como corresponsáveis com outras organizações</p>	
Plataformas de redes sociais/redes de publicidade em linha	<ul style="list-style-type: none"> • Escolhem a base jurídica adequada para o tratamento: contrato com pessoas singulares, consentimento, interesse legítimo. Em caso de «dados sensíveis», o tratamento só é possível se o consentimento for explícito ou os dados tiverem sido manifestamente tornados públicos • Utilizam apenas os dados necessários para a finalidade definida • Realizam uma avaliação de impacto sobre a proteção de dados • Garantem a legalidade em caso de partilha de dados dos membros com terceiros • Cumprem os requisitos de transparência, em especial no que diz respeito aos termos e condições, se os dados forem posteriormente partilhados com 	

	<p>um terceiro, etc.</p> <ul style="list-style-type: none"> • Respeitam condições específicas quando da utilização de decisões automatizadas (por exemplo, obtêm o consentimento explícito e aplicam garantias adequadas) • Garantem a segurança do tratamento através de medidas técnicas e organizativas • Comunicam violações de dados • Providenciam controlos e parâmetros para as pessoas exercerem efetivamente os seus direitos, incluindo o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis
	<p>As autoridades eleitorais nacionais são responsáveis pelo tratamento dos dados</p>
<p>Autoridades eleitorais nacionais</p>	<ul style="list-style-type: none"> • Base jurídica para o tratamento de dados: obrigação legal ou missão de interesse público fundamentada na lei • Realizam uma avaliação de impacto sobre a proteção de dados se o impacto não tiver já sido avaliado na legislação