UMA VOTAÇÃO UM TANTO SECRETA

Lucy Purdon

• *Estudo de caso* •
sobre o processo eleitoral no Quênia

RESUMO

Este artigo aborda as eleições no Quênia e analisa o uso da tecnologia e a exploração de dados pessoais tanto no processo quanto na campanha eleitorais. Basta olhar para o histórico eleitoral do Quênia para entender por que essa análise é importante. A eleição de 2007/2008 resultou em uma onda de violência que matou mais de mil pessoas e deslocou mais de seiscentas mil. A eleição de 2013 foi relativamente pacífica, mas marcou a ascensão do "discurso de ódio" on-line que explorou as tensões étnicas. O resultado das eleições de 2017 foi anulado e uma nova eleição foi realizada em meio a uma enorme tensão e morte de pelo menos trinta e três pessoas, enquanto anúncios políticos on-line direcionados suscitavam temores nacionais de mais violência. O artigo conclui com um esboço das proteções e salvaguardas mínimas esperadas que podem ser aplicadas em âmbito global.

PALAVRAS-CHAVE

Quênia | Eleição | Votação | Política | Biométrico | Tecnologia | Dados | Perfilamento | Anúncios | Campanha | Direcionado | Hackear | Segurança | Bancos de dados | Desinformação | Propaganda | Proteção de dados | Análise de dados

2018 é um ano de eleições: Brasil, Colômbia, México, Paquistão, Zimbábue e, supostamente, a Tailândia terão eleições gerais ou presidenciais. A segurança e transparência dos processos eleitorais estão sob os olhares atentos de todo o mundo. Da implementação apressada do cadastro eleitoral biométrico, preocupações com a segurança dos registros de eleitores e dos próprios sistemas eleitorais, até o fenômeno da propaganda política direcionada e campanhas de desinformação nas mídias sociais, há diversas questões para distrair os eleitores da pergunta democrática mais importante: quem melhor representará você e seu país?

Este artigo aborda as eleições no Quênia e analisa o uso da tecnologia e exploração de dados pessoais tanto no processo como na campanha eleitorais.

Basta olhar para o histórico eleitoral do Quênia para entender por que a análise do tema é importante. A eleição de 2007/2008 resultou em uma onda de violência que matou mais de mil pessoas e deslocou mais de seiscentas mil. A eleição de 2013 foi relativamente pacífica, mas marcou a ascensão do "discurso de ódio" on-line que explorou as tensões étnicas. O resultado das eleições de 2017 foi anulado e uma nova eleição foi realizada em meio a uma enorme tensão e morte de pelo menos trinta e três pessoas, enquanto anúncios políticos on-line direcionados suscitavam temores nacionais de mais violência.

Este artigo se baseia em uma pesquisa da *Privacy International* realizada durante as eleições presidenciais de 2017 sobre as origens de duas campanhas on-line controversas e o envolvimento de empresas ocidentais de análise de dados.[1] Este artigo também se utiliza de pesquisas publicadas pelo *Centre for Intellectual Property and Information Technology* – CIPIT (na denominação original em inglês) da Universidade de Strathmore, no Quênia, em parceria com a Privacy International, que analisam a adoção e implementação do cadastro biométrico de eleitores.[2] Além disso, o artigo reflete sobre o trabalho de *advocacy* e incidência política empreendido pela *Privacy International* após o escândalo do Facebook/Cambridge Analytica que se tornou público em março de 2018 e que, mais uma vez, deu destaque às eleições de 2017 no Quênia.

1 • Cadastro eleitoral biométrico

Quando o governo queniano anunciou a adoção do cadastro biométrico e da autenticação eleitoral previstas na Lei Eleitoral de 2011, as motivações eram plausíveis. A recomendação de mudar para um novo sistema de cadastramento partiu da Comissão Kriegler, criada com o intuito de investigar o sistema eleitoral queniano após a onda de violência que sucedeu a eleição de 2007/2008.[3] O relatório da Comissão Kriegler também forneceu uma nota técnica sobre as características dos sistemas eleitorais biométricos.[4]

Acreditava-se que um sistema de cadastro biométrico, incluindo impressões digitais dos eleitores, além da verificação na seção eleitoral, asseguraria um voto por pessoa e evitaria denúncias de irregularidades nas urnas. Os resultados poderiam ser transmitidos

diretamente ao colégio eleitoral, evitando qualquer adulteração. Havia inquietações de que votos em nome de pessoas mortas que ainda constavam no registro eleitoral estivessem sendo computados. A Comissão Kriegler estimava que havia "provavelmente" 1,2 milhão de pessoas falecidas incluídas no registro em 2007,[5] mas não há dados disponíveis para embasar a alegação de que votos estavam sendo realizados em nome dessas pessoas, seja nessa eleição ou nas eleições subsequentes. George Morara, presidente da Comissão Nacional Queniana de Direitos Humanos (Kenyan National Commission on Human Rights - KNCHR, na denominação original em inglês), compartilhava essa preocupação e mencionou antes da eleição de 2017 que "dizem que no Quênia os mortos voltam para votar e depois retornam às suas sepulturas".[6] No entanto, havia uma solução alternativa, menos dispendiosa e invasiva que um sistema de cadastro biométrico eleitoral? Uma reorganização dos registros de nascimento e óbito teria resolvido o problema? Isso nunca foi discutido.

Antes de embarcar em iniciativas tão focadas na utilização de dados e potencialmente invasivas, os governos precisam se perguntar: por que fazer isso tudo? Qual problema um banco de dados biométrico, por exemplo, está tentando resolver? Como ser bem-sucedido? Quais são as consequências caso essa estratégia não dê certo?

Uma das principais preocupações é que os governos estão ávidos em implementar iniciativas que coletam muitos dados pessoais, mas não levam em consideração a proteção dos dados gerados por esses projetos. Sistemas biométricos são um exemplo de sistemas com uso intensivo de dados que potencialmente são muito invasivos. A preocupação dos defensores de direitos humanos na África do Sul, por exemplo, é que quando esses sistemas são adotados com a ausência de estruturas jurídicas fortes e salvaguardas rigorosas, as tecnologias biométricas representam ameaças graves à privacidade e segurança pessoal, pois sua aplicação pode ser ampliada para facilitar discriminação, perfilamento e vigilância em massa.[7] Outra preocupação é que a falta de precisão e as chances de falhas dessa tecnologia podem levar a erros de identificação, fraude e exclusão cívica, um fator central nos desafios atuais que estamos vendo na Suprema Corte da Índia em relação ao esquema biométrico de Aadhaar, atualmente em curso no país.[8]

No caso do Quênia, a tecnologia falhou de modo massivo durante as eleições de 2013, e as seções eleitorais tiveram que recorrer ao registro manual para identificar os eleitores. Em 2017, o sistema teve um desempenho relativamente bom em comparação ao desastre de 2013,[9] mas, conforme este artigo irá debater, ainda é possível contestar em que medida a tecnologia biométrica melhorou a credibilidade da democracia e das eleições quenianas, dada a variedade de outros fatores.

2 • Segurança dos bancos de dados de eleitores

Os bancos de dados de cadastro eleitoral frequentemente são mal protegidos e vulneráveis. As violações de dados ocorrem em todo o mundo e os números envolvidos são surpreendentes.

As informações pessoais de mais de 93 milhões de eleitores no México,[10] incluindo endereços residenciais, foram publicadas abertamente na internet após terem sido retiradas de um banco de dados governamental mal protegido. Esses dados podem ser uma informação altamente delicada, dado o contexto; no México, por exemplo, até cem mil pessoas são sequestradas por ano.[11] Da mesma forma, as informações pessoais de mais de cinquenta e cinco milhões de eleitores filipinos foram disponibilizadas publicamente on-line, a maior violação de dados na história das Filipinas.[12]

Uma pesquisa realizada no Quênia para descobrir se o banco de dados de eleitores de 2017 foi compartilhado com terceiros – e, em caso afirmativo, por quem - revelou que o registro estava disponível abertamente para venda, sem proteções ou salvaguardas. Consequentemente, os eleitores receberam mensagens de texto não solicitadas dos candidatos, identificando o destinatário pelo nome, pelo distrito eleitoral e até pela seção eleitoral local.[13] Sendo assim, já é possível notar que essas aplicações tecnológicas estão longe de restaurar a confiança tão necessária no processo eleitoral.

3 • O problema da falta de proteção de dados

O Quênia não possui uma legislação abrangente de proteção de dados que obrigue qualquer entidade – pública ou privada – a respeitar os critérios básicos em matéria de proteção de dados. Isso incluiria o detalhamento do que é coletado, o objetivo da coleta, como esses dados serão armazenados e com quem serão compartilhados. Sob as novas leis de proteção de dados na Europa, por exemplo, as entidades também devem fornecer a base jurídica para coletar e obter o consentimento informado do indivíduo, em particular para o processamento de dados pessoais confidenciais, como dados biométricos. Sem leis apropriadas de proteção de dados, os indivíduos ficam vulneráveis à coleta excessiva de dados sobre eles, obtidos sem o seu consentimento e tendo seus dados utilizados de maneiras desconhecidas. Quando as empresas coletam dados em países com legislação insuficiente e os compartilham com terceiros, não está claro quais normas elas e esses terceiros estão adotando, isso caso tenham seguido alguma norma. Uma vez que os dados são gerados, os indivíduos deveriam ser capazes de saber que tipos de dados organizações e empresas mantêm sobre eles e com qual finalidade esses dados são utilizados. Ter uma lei descrita nos códigos jurídicos é uma coisa, mas ela também deve ser efetivamente implementada. Uma parte essencial é a existência de uma autoridade independente que disponha de recursos adequados e seja capaz de investigar denúncias.

A proteção de dados teria ajudado as ocorrências descritas neste artigo? Ela poderia ter feito o governo queniano pensar duas vezes antes de implementar o sistema da maneira como o fez. Ela tornaria mais fácil para os quenianos exercerem seus direitos e obterem respostas, como descobrir quais dados foram coletados, como foram utilizados, por quanto tempo foram armazenados e com quem foram compartilhados.

As próximas duas seções exploram essa questão em um contexto diferente.

4 • Desinformação e propaganda

Em países de todo o mundo, a disseminação de desinformação e propaganda durante o período eleitoral tem sido um problema há décadas, mas recebeu pouca atenção ou preocupação internacional. De modo frustrante, quando recentemente se tornou um problema nos Estados Unidos da América (EUA) durante a eleição presidencial de 2016 e também na Europa em torno do Brexit, de repente ganhou um título: "notícias falsas" (*fake news*).[14]

Na segunda década do século XXI vimos as mídias sociais serem aclamadas como a faísca inicial das revoluções e das mudanças democráticas.[15] Mas menos atenção foi dada às tensões políticas e sociais amplificadas pelos mesmos espaços. O Vale do Silício não conseguiu prever, compreender ou mesmo tentar entender o que estava acontecendo ao redor do mundo, nem prestar atenção aos repetidos alertas de que o conteúdo destinado a instigar tensões étnicas postado em suas plataformas teve um efeito real no mundo. No Quênia, por exemplo, já se sabia que mensagens de texto, blogs e rádios desempenharam um papel na onda de violência após as eleições de 2007/2008.[16] A eleição de 2013 no Quênia também foi repleta de conteúdo divisionista e inflamatório nas mídias sociais, espaço encontrado como saída após a implementação de controles mais rígidos na mídia impressa e telecomunicações.[17]

O espaço on-line é um ímã que atrai todos em época de eleição. Campanhas políticas sempre foram um assunto complexo e, embora as campanhas políticas baseadas em dados não sejam novidade, o nível de desagregação dos dados disponíveis e o poder potencial de influenciar ou inibir os eleitores por meio desses dados ocorre, particularmente, por meio de publicidade política direcionada on-line.

5 • Publicidade política direcionada com base em análise de dados

As campanhas políticas em todo o mundo rapidamente se transformaram em sofisticadas operações de dados. A forma como os dados são utilizados em eleições e campanhas políticas é potencialmente muito invasiva à privacidade, levanta importantes questões referentes à segurança e tem o potencial de abalar a confiança no processo democrático.

As plataformas de mídia social ganham dinheiro com publicidade segmentada, com base nas informações que coletam do usuário, incluindo dados demográficos, localização e interesses detalhados.[18] Da mesma forma que a publicidade on-line direciona seu conteúdo para pessoas com base em seus interesses, personalidade e humor com o objetivo de vender produtos, os partidos políticos as convencem a comprar o que estão vendendo em época de eleição.

Em suma, isso significa que as empresas, muitas das quais você provavelmente nunca ouviu falar, são capazes de aprender sobre seus hábitos, personalidade, interesses sexuais, crenças políticas e muito mais para fazer previsões sobre sua personalidade e comportamento. Isso é

conhecido como "perfilamento" ou categorização de perfis.[19] O perfilamento gera inferências e previsões altamente significativas sobre a personalidade, o comportamento e as crenças das pessoas. Em última análise, os eleitores estão sendo segmentados com base em informações que não necessariamente sabem que forneceram. Isso é especialmente preocupante quando informações confidenciais, como crenças políticas ou traços de personalidade, são inferidas a partir de dados sem nenhuma relação entre si, usando o perfilamento.

Os partidos políticos que disputam as eleições empregam diretamente analistas de dados e empresas de mídia digital, especialistas na categorização de perfis, para realizar suas campanhas on-line. Essas empresas, por sua vez, podem trabalhar diretamente com plataformas on-line, como o Facebook, para criar mensagens políticas minuciosamente direcionadas que são projetadas para influenciar a maneira como você vota, com base em informações coletadas e inferidas sobre você. Elas frequentemente contam com dados comercialmente disponíveis de corretores de dados, ou registros disponíveis publicamente e dados acessíveis on-line para criar perfis extremamente detalhados, incluindo conclusões sobre sua personalidade, medos e estado emocional. Anúncios e mensagens de campanha direcionadas podem, então, inundar os resultados de pesquisa on-line e *feeds* de mídia social. A campanha presidencial de Trump em 2016, por exemplo, utilizou entre quarenta e cinquenta mil variantes das mesmas mensagens on-line todos os dias para segmentar diferentes grupos de pessoas.[20] Mas os detalhes por trás desse processo costumam não ser claros – para quem exatamente essas empresas trabalham, o que fazem, como fazem, que dados coletam e o quanto são bem-sucedidas são todos segredos bem guardados.

No início de 2017, a *Privacy International* averiguou uma denúncia segundo a qual a Cambridge Analytica, empresa de análise de dados com sede no Reino Unido, trabalhava de forma sigilosa para o Partido Jubileu no período que antecedeu as eleições quenianas. Escrevemos para a empresa em maio de 2017 para pedir esclarecimentos sobre seu papel e como ela, já que se trata de uma empresa britânica, estava aderindo às leis de proteção de dados enquanto o Quênia não tinha nenhuma.[21] Preocupava-nos que a potencial coleta de dados pudesse ser extremamente invasiva, incluindo dados pessoais confidenciais, como a etnia de uma pessoa. Em países onde há histórico de tensões étnicas que resultam em violência política, como no Quênia, fazer campanhas com base em dados analíticos e categorização de perfis é um terreno desconhecido, repleto de grande risco. Não recebemos nenhuma resposta.

Nossas fontes confirmaram que a Cambridge Analytica estava de fato trabalhando para o Partido Jubileu, reunindo dados de pesquisas para ajudar na campanha e administrar a imagem do Presidente. Na mesma época, duas campanhas on-line incendiárias, "O Verdadeiro Raila" (*The Real Raila*) e "Uhuru Para Nós" (*Uhuru For Us*), que visavam à oposição queniana, começaram a circular on-line no Quênia. Sua criação foi reivindicada por "um grupo diverso e preocupado de jovens quenianos", e teve enorme influência nas violentas eleições passadas do Quênia e nos temores de qualquer violência futura. A

campanha do Verdadeiro Raila afirmou que o governo do candidato da oposição, Raila Odinga, "removeria tribos inteiras".[22] Como esses vídeos dominaram as pesquisas do Google e inundaram as contas do Twitter, Facebook e YouTube em todo o país em 2017, a Privacy International realizou uma investigação aprofundada[23] sobre a origem dos vídeos.

Como já se sabia que a Cambridge Analytica estava trabalhando para o Partido Jubileu, esperávamos algum envolvimento por parte da empresa na criação dos vídeos. No entanto, a investigação da *Privacy International* revelou que os vídeos foram criados pela Harris Media LLC, uma agência do Texas que usa a análise de dados para criar campanhas políticas. Nessa ocasião, a segmentação foi feita por meio do uso criterioso do Google AdWords, no qual anúncios pagos para as campanhas foram exibidos acima dos resultados de pesquisa orgânica do Google a partir de diversos termos de pesquisa relacionados a eleições quenianas, como "data de eleição do Quênia".

No entanto, foi somente em março de 2018, após as investigações do jornal *The Guardian* e do *Channel 4 News* no Reino Unido, que a Cambridge Analytica passou a ocupar um lugar de destaque na agenda de notícias. Um informante se apresentou descrevendo a "colheita" de perfis no Facebook para atingir os eleitores durante a eleição presidencial dos EUA em 2016.[24] Uma investigação sigilosa do *Channel 4 News* gravou secretamente funcionários da Cambridge Analytica se gabando de seu envolvimento em eleições, inclusive no Quênia. Mark Turnbull, diretor-administrativo da Cambridge Analytica Political, uma subsidiária da Cambridge Analytica, confirmou isso e muito mais no vídeo secreto,

> *Nós reformulamos a imagem de todo o partido duas vezes, escrevemos seu manifesto, fizemos duas rodadas de cinquenta mil questionários, uma quantidade enorme de pesquisas, análises, mensagens e depois escrevemos todos os discursos e organizamos tudo, então basicamente todos os elementos da campanha dele.*[25]

Outra reportagem do *Channel 4 News* que se concentrou no Quênia também destacou a disseminação dos vídeos on-line[26] detalhada em nossa investigação anterior. O que ficou sem resposta, no entanto, foi exatamente o tipo de dados coletados sobre os cidadãos quenianos, de quais fontes e o envolvimento específico da Cambridge Analytica. Não se sabe, por exemplo, quais dados podem ter sido coletados ou compartilhados pelo Facebook, outras plataformas ou outras empresas de análise de dados que trabalharam no Quênia durante as eleições.[27]

No entanto, o escândalo gerou uma onda bem-vinda de análises e debates sobre o comportamento das corporações e a falta de garantias de proteção dos dados pessoais em toda a África.[28] Essa história que está se desenrolando atualmente aponta para um ecossistema corporativo poderoso e sombrio por trás da propaganda política on-line direcionada que prospera a partir dos nossos dados pessoais, seja para nos vender sabão ou para nos convencer em quem votar.

6 • Transparência nas campanhas políticas

Em países com histórico de violência política, isso não deveria ser considerado banal. A questão étnica no Quênia, por exemplo, ainda é delicada e as eleições são um período de crescente tensão. Portanto, no mínimo, as empresas desse ecossistema devem ser transparentes sobre seu papel nas campanhas políticas on-line. As leis eleitorais quenianas não exigem de modo claro que os candidatos declarem as campanhas ou os anúncios que financiaram. As empresas envolvidas não são solícitas em prestar contas sobre o seu papel. É fundamental que as campanhas políticas sejam realizadas de forma transparente e responsável, especialmente quando os riscos são tão altos em um país como o Quênia. Atualmente, a publicidade política on-line direcionada não faz nenhuma das duas coisas. Exigir que os partidos políticos sejam transparentes sobre as campanhas de marketing que financiaram, como desenvolveram mensagens direcionadas ou com quais empresas trabalharam não é algo polêmico. Quando não fica claro quem financiou ou criou anúncios de campanha, não há prestação de contas.

Democracias saudáveis não são definidas somente pelas eleições. O Quênia é somente um dos países onde existem desafios referentes ao cadastro biométrico de eleitores e autenticação, e levará tempo para desvendar a rede de empresas que exploram dados pessoais para campanhas pagas por partidos políticos. A dificuldade, claro, é que aqueles que se beneficiam são os próprios partidos políticos. Por que eles mudariam um sistema que os ajuda a chegar ao poder?

Os quenianos devem esperar alguns anos até a próxima eleição. Para todos aqueles com eleições neste ano, protejam as mesmas exigindo transparência e proteções adequadas, desde o cadastro até o exercício do seu voto de fato. Na atualidade, isso é mais importante do que nunca.

NOTAS

1 • "Texas Media Company Hired By Trump Created Kenyan President's Viral 'Anonymous' Attack Campaign Against Rival, New Investigation Reveals," Privacy International, 15 de dezembro de 2017, acesso em 6 de junho de 2018, https://privacyinternational.org/feature/954/texas-media-company-hired-trump-created-kenyan-presidents-viral-anonymous-attack.

2 • "Biometric Technology, Elections, and Privacy. Investigating Privacy Implications of Biometric Voter Registration in Kenya's 2017 Election Process," CIPIT at Strathmore University, Nairobi, maio de 2018, acesso em 6 de junho de 2018, https://blog.cipit.org/wp-content/uploads/2018/05/Biometrics-Privacy-Report-by-CIPIT.pdf.

3 • "Report of the Independent Review Commission on the General Elections held in Kenya on 27th December, 2007" (conhecida como Kriegler Commission), Recommendations Concerning Registration of Voters, p. 157, Kenya Law, 2008, acesso em 6 de junho de 2018, http://kenyalaw.org/kl/fileadmin/CommissionReports/Report-of-the-Independent-Review-Commission-on-the-General-Elections-held-in-Kenya-on-27th-December-2007.pdf.

4 • *Ibid.*, Annex 3.A, pp. 260-295.

5 • *Ibid.*, p. 8.

6 • Agence France-Presse, "Dead Voters and Other Ways to Steal a Kenyan Election." The Daily Nation, 1 de agosto de 2017, acesso em 6 de junho de 2018, https://www.nation.co.ke/news/Kenya-General-Election-2017-and-rigging/1056-4040292-5toedlz/index.html.

7 • Dale T. McKinley e Campanha Right To Know, "New Terrains of Privacy in South Africa." Right2Know, 15 de dezembro de 2016, acesso em 6 de junho de 2018, http://www.r2k.org.za/2016/12/15/research-new-terrains-of-privacy-in-south-africa/.

8 • Dhananjay Mahapatra, "Supreme Court Reserves Verdict on Aadhaar Validity." The Times of India, 11 de maio de 2018, acesso em 6 de junho de 2018, https://timesofindia.indiatimes.com/india/supreme-court-reserves-verdict-on-aadhaar-validity/articleshow/64116972.cms.

9 • "Biometrics in Kenya's Election," CIPIT blog, 2017, acesso em 27 de março de 2018, http://blog.cipit.org/wp-content/uploads/2017/12/Biometrics_history.png.

10 • Dell Cameron, "Private Records of 93.4 Million Mexican Voters Exposed In Data Breach." The Daily Dot, 22 de abril de 2016, acesso em 6 de junho de 2018, http://www.dailydot.com/layer8/amazon-mexican-voting-records/.

11 • Vladimir Hernandez, "Our World: Kidnapped in Mexico." Huffington Post, 15 de março de 2017, acesso em 6 de junho de 2018, http://www.huffingtonpost.com/vladimir-hernandez/our-world-kidnapped-in-mexico_b_9462258.html.

12 • "State of Privacy Report for The Philippines," Privacy International, janeiro de 2018, acesso em 6 de junho de 2018, https://www.privacyinternational.org/state-privacy/1009/state-privacy-philippines.

13 • "Biometric technology, elections, and privacy," CIPIT, maio de 2018.

14 • Mike Wendling, "The (Almost) Complete History of 'Fake News." BBC, 22 de janeiro de 2018, acesso em 6 de junho de 2018, http://www.bbc.co.uk/news/blogs-trending-42724320.

15 • Ethan Zuckerman, "The First Twitter Revolution?" Foreign Policy, 24 de março de 2011, acesso em 6 de junho de 2018, http://foreignpolicy.com/2011/01/15/the-first-twitter-revolution-2/; Essam Mansour, "The Role of Social Networking Sites (SNSs) in the January 25th Revolution in Egypt," *Library Review* 61, no. 2 (2012): 128-159.

16 • "On the Brink of the Precipice: A Human Rights Account of Kenya's Post-2007 Election Violence," The Kenyan National Commission on Human Rights, 2003, acesso em 6 de junho de 2018, www.knchr.org/Portals/0/Reports/KNCHR_REPORT_ON_THE_BRINK_OF_THE_PRECIPE.pdf.

17 • "Corporate Responses to Hate Speech in the 2013 Kenya Presidential Elections. Case Study: Safaricom," The Institute for Human Rights and Business, p. 23, novembro de 2013, acesso em 6 de junho de 2018, https://www.ihrb.org/pdf/DD-Safaricom-Case-Study.pdf.

18 • Por exemplo, Facebook Business, Homepage, 2018, acesso em 6 de junho de 2018, https://en-gb.facebook.com/business/products/ads/ad-targeting.

19 • Perfilamento é um termo definido no Regulamento Geral Europeu sobre Proteção de Dados (RGPDP), a ser publicado, como "qualquer forma de processamento automatizado de dados pessoais que consista no uso de dados pessoais para avaliar certos aspectos pessoais relativos a uma pessoa física, em particular para analisar ou prever aspectos relativos ao desempenho dessa pessoa no trabalho, situação econômica, saúde, preferências pessoais, interesses, confiabilidade, comportamento, localização ou movimentos". "Article 4 EU GDPR 'Definitions'," Privacy Plan, 2018, acesso em 6 de junho de 2018, http://www.privacy-regulation.eu/en/article-4-definitions-GDPR.htm.

20 • Sean Illing, "Cambridge Analytica, The Shady Data Firm that Might be a Key Trump-Russia Link, Explained." Vox, 17 de março de 2018, acesso em 6 de junho de 2018, https://www.vox.com/policy-and-politics/2017/10/16/15657512/cambridge-analytica-christopher-wylie-facebook-trump-russia.

21 • "Letter to Cambridge Analytica on 2017 Kenya Election," Privacy International, 30 de maio de 2017, acesso em 6 de junho de 2018, https://privacyinternational.org/advocacy-briefing/1683/letter-cambridge-analytica-2017-kenya-election.

22 • "Kenya in 2020 if Raila Odinga is elected President," vídeo do YouTube, 1:28, postado por The Real Raila, 10 de julho de 2017, acesso em 6 de junho de 2018, https://www.youtube.com/watch?v=o45NlqZXDXw.

23 • "Texas Media Company Hired By Trump...," Privacy International, 2017.

24 • "The Cambridge Analytica Files," The Guardian, março de 2018, acesso em 6 de junho de 2018, https://www.theguardian.com/news/series/cambridge-analytica-files.

25 • "Revealed: Trump's Election Consultants Filmed Saying They Use Bribes and Sex Workers to Entrap Politicians," Channel 4 News, at 9", 19 de março de 2018, acesso em 6 de junho de 2018, https://www.channel4.com/news/cambridge-analytica-revealed-trumps-election-consultants-filmed-saying-they-use-bribes-and-sex-workers-to-entrap-politicians-investigation.

26 • "Kenyans Bombarded With Fake News in Presidential Election," Channel 4 News, 25 de março de 2018, acesso em 6 de junho de 2018, https://www.channel4.com/news/kenyans-bombarded-with-fake-news-in-presidential-election.

27 • "Further Questions on Cambridge Analytica's Involvement in the 2017 Kenyan Elections and Privacy International's Investigations," Privacy International, 27 de março de 2018, acesso em 6 de junho de 2018, https://medium.com/@privacyint/further-questions-on-cambridge-analyticas-involvement-in-the-2017-kenyan-elections-and-privacy-15e54d0e4d7b.

28 • Maggie Fick and Alexis Akwagyiram, "In Africa, Scant Data Protection Leaves Internet Users Exposed." Reuters, 4 de abril de 2018, acesso em 6 de junho de 2018, https://www.reuters.com/article/us-facebook-africa/in-africa-scant-data-protection-leaves-internet-users-exposed-idUSKCN1HB1SZ; Nick Miriello, David Gilbert and Julia Steers, "Kenyans Face a Fake News Epidemic." Vice, 22 de março de 2018, acesso em 6 de junho de 2018, https://news.vice.com/en_us/article/43bdpm/kenyans-face-a-fake-news-epidemic-they-want-to-know-just-how-much-cambridge-analytica-and-facebook-are-to-blame?utm_campaign=sharebutton; "Kenyans Want to Know What Role Cambridge Analytica Played in their 2017 Presidential Election," Vice News, 22 de março de 2018, acesso em 6 de junho de 2018, https://www.youtube.com/watch?v=0xw-DhxNv2Q.

LUCY PURDON – *Reino Unido*
Lucy é coordenadora de políticas da Privacy International e é responsável pelo desenvolvimento de estratégias políticas da organização, onde coordena o trabalho de política global sobre segurança cibernética e identidade. Ela trabalha de maneira transversal na organização e com parceiros internacionais para desenvolver recomendações de políticas e posicionamentos baseados em descobertas encontradas em projetos de pesquisa.

contato: *lucyp@privacyinternational.org*

Recebido em março de 2018.
Original em inglês. Traduzido por Fernando Sciré.

"Este artigo é publicado sob a licença de Creative Commons Noncommercial Attribution-NoDerivatives 4.0 International License"