

## CAMBRIDGE ANALYTICA: Escândalo, Legado e Possíveis Futuros para a Democracia

<http://dx.doi.org/10.21527/2176-6622.2020.53.182-195>

Recebido em: 29/12/2019

Modificações solicitadas em: 20/4/2020

Aceito em: 26/4/2020

### *Mateus de Oliveira Fornasier*

Doutorado em Direito pela Universidade do Vale do Rio dos Sinos (Unisinos, Brasil) (2013), com Pós-Doutorado pela University of Westminster (Reino Unido) (2018-2019). É professor/pesquisador da Universidade Regional do Noroeste do Estado do Rio Grande do Sul (Unijui) no Programa de Pós-Graduação Stricto Sensu (Mestrado e Doutorado) em Direito. Tem experiência na área de Direito, com ênfase em Sociologia Jurídica e Direito Constitucional, atuando principalmente nos seguintes temas: regulação da tecnologia, inteligência artificial e Direito, filosofia da tecnologia, democracia eletrônica e cidadania digital. <http://lattes.cnpq.br/3316861562386174>. <https://orcid.org/0000-0002-1617-4270>. [mateus.fornasier@unijui.edu.br](mailto:mateus.fornasier@unijui.edu.br)

### *Cesar Beck*

Graduação em Direito pela Fundação Getúlio Vargas (2010). Tem experiência na área de Direito, com Pós-Graduação (Lato Sensu) em Direito Constitucional pela Universidade Candido Mendes. Especialização em diversos cursos em Propriedade Intelectual, como o CopyrightX (Parceria ITS Rio-Harvard, 2014), Entendendo Bitcoin na Prática (ITS Rio, 2015) e Direito e Entretenimento (Uerj, 2015). <http://lattes.cnpq.br/6488052912983557>. <http://orcid.org/0000-0002-8625-6503>. [cesar.rutowsch@gmail.com](mailto:cesar.rutowsch@gmail.com)

### RESUMO

O texto traz um referencial acerca do caso da empresa Cambridge Analytica (CA). Foram demonstradas, ao longo do artigo, as causas que levaram ao escândalo ocorrido, o legado deixado a partir disso e as possibilidades de futuro para a referida empresa. São mencionados, ainda, os pontos que levaram a CA a cometer erros que custaram sua reputação. O artigo aborda também que o ocorrido com a empresa poderá acontecer com diversos outros setores, necessitando, portanto, de ações preventivas capazes de trabalhar e modificar pontos falhos. O texto é finalizado a partir da observação acerca da Fake News – tema amplamente mencionado no passado-recente e sobre a Deep Fake – tema do futuro-imediato. A importância do conhecimento acerca desses termos próximos das eleições a serem realizadas no ano de 2020, identifica que o eleitor brasileiro ainda precisa compreender melhor a questão da escolha consciente, a fim de promover a boa manutenção do Estado Democrático de Direito, sendo essas questões um aprendizado ensinado a partir da análise do exemplo do escândalo da CA. O estudo é feito por meio de uma pesquisa de natureza descritiva, com método hipotético-dedutivo, sendo um estudo de caso de abordagem qualitativa e transdisciplinar, com técnica bibliográfico-documental.

**Palavras-chave:** *Cambridge Analytica*. Escândalo. Reputação. Análise comportamental eleitoral.

### CAMBRIDGE ANALYTICA: SCANDAL, LEGACY AND POSSIBLE FUTURES FOR DEMOCRACY

### ABSTRACT

The text brings a reference about the case of Cambridge Analytica (CA). It was demonstrated throughout the article, the causes that led to the scandal occurred, the legacy left from that and the future possibilities for that company. Also mentioned are the points that led CA to make mistakes that cost her reputation. The article also discusses that what happened with the company could happen to several other sectors, thus requiring preventive actions capable of working and modifying failures. The text concludes from the remark about Fake News – a theme widely mentioned in the recent past and Deep Fake – an immediate future theme. The importance of knowledge about these terms near the elections to be held in 2020 identifies that the Brazilian voter still needs to better understand the issue of conscious choice in order to promote the proper maintenance of the Democratic Rule of Law from the analysis of the CA scandal example. The study is made through a descriptive research, with hypothetical-deductive procedure method, being a case study with a qualitative and transdisciplinary approach, with bibliographic-documentary technique.

**Keywords:** Cambridge Analytica. Scandal. Reputation. Electoral behavior analysis.

### SUMÁRIO

1 Introdução. 2 Da investigação jornalística ao escândalo da Cambridge Analytica. 3 Da obscuridade ao conhecimento da práxis da CA. 4 Do legado deixado pela Cambridge Analytica. 5 Identificação de novos problemas virais: nem todo problema possui um antídoto – algumas medidas paliativas já auxiliam na mitigação de eventuais danos. 6 Considerações finais. 7 Referências.

## 1 INTRODUÇÃO

O que o problema filosófico do *Mito da Caverna* tem em comum com o escândalo da *Cambridge Analytica* (CA)? De que forma a *Alegoria da Caverna* de Platão auxilia a entender a *práxis* de uma empresa focada em tecnologias de análise comportamental? Não existe necessidade para pânico acadêmico – para aqueles que ainda não leram a *Alegoria da Caverna*. É também conhecida como a *Alegoria dos Prisioneiros* – posto que aqui apenas será explorado o viés em que o conhecimento liberta os *prisioneiros de sombras* e obscuridades. Somente a transparência dos fatos, da forma que a empresa agia, o que e como isso influencia vidas (no cotidiano), permite blindar o direito à privacidade e criar novos mecanismos de resiliência na democracia. Para Sócrates, segundo Platão:

*SÓCRATES – Agora imagina a maneira como segue o estado da nossa natureza relativamente à instrução e à ignorância. Imagina homens numa morada subterrânea, em forma de caverna, com uma entrada aberta à luz; esses homens estão aí desde a infância, de pernas e pescoço acorrentados, de modo que não podem mexer-se nem ver senão o que está diante deles, pois as correntes os impedem de voltar à cabeça; a luz chega-lhes de uma fogueira acesa numa colina que se ergue por detrás deles; entre o fogo e os prisioneiros passa uma estrada ascendente. Imagina que ao longo dessa estrada está construído um pequeno muro, semelhante às divisórias que os apresentadores de títeres armam diante de si e por cima das quais exibem as suas maravilhas. [...] Sócrates – E se a parede do fundo da prisão provocasse eco, sempre que um dos transportadores falasse, não julgariam ouvir a sombra que passasse diante deles? Glauco – Sim, por Zeus! Sócrates – Dessa forma, tais homens não atribuirão realidade senão às sombras dos objetos fabricados. Glauco – Assim terá de ser. Sócrates – Considera agora o que lhes acontecerá, naturalmente, se forem libertados das suas cadeias e curadas da sua ignorância. Que se liberte um desses prisioneiros, que seja ele obrigado a endireitar-se imediatamente, a voltar o pescoço, a caminhar, a erguer os olhos para a luz: ao fazer todos estes movimentos sofrerá, e o deslumbramento impedi-lo-á de distinguir os objetos de que antes via as sombras. Que achas que responderá se alguém lhe vier dizer que não viu até então senão fantasmas, mas que agora, mais perto da realidade e voltado para objetos mais reais, vê com mais justeza? Se, enfim, mostrando-lhe cada uma das coisas que passam o obrigar, à força de perguntas, a dizer o que é?<sup>1</sup>*

Diante desse cenário de desinformação, tem-se que o problema de pesquisa deste artigo pode ser apresentado na forma do seguinte questionamento: Qual o legado da ocultação, da parte da CA, da coleta e do tratamento de dados pessoais e sensíveis que realizou em relação a milhões de eleitores no âmbito de importantes eventos democráticos – tais como o Referendum do Brexit de 2015 e as Eleições Presidenciais Americanas de 2016? Como hipótese, tem-se que, após entender seu *modus operandi*, pode-se observar o seu legado de corrupção de princípios fundamentais ao Estado Democrático de Direito: a privacidade/intimidade dos cidadãos (por meio da coleta de dados sensíveis sem permissão dos seus titulares, bem como pela difusão de Fake News) e a transparência em relação aos processos democráticos (mediante o Data Scrapping, principalmente). Ao observar a atuação de novos atores, o questionamento ao final do artigo encaminha-se em direção a quando uma empresa como a CA emergir: como a sociedade civil organizada e o Estado Democrático de Direito, ambos mais bem capacitados, responderão? Espera-se que de forma mais eficiente.

O artigo foi dividido em quatro seções. Na primeira delas buscou-se fazer um relato histórico acerca da descoberta do escândalo – que se revelou a partir de uma experiência importante de jornalismo investigativo. Já, na segunda, são detalhados os procedimentos ilícitos utilizados pela CA para a consecução de suas atividades. Na terceira parte são apontadas as principais lições que esse escândalo deixa para a existência do Estado Democrático de Direito. Por fim, a quarta seção se ocupa de mais algumas outras ameaças virtuais à democracia, análogas à ocorrida no âmbito da CA.

Metodologicamente, trata-se de pesquisa de natureza descritiva, com método de procedimento hipotético-dedutivo, um estudo de caso de abordagem qualitativa e transdisciplinar (tratado, principalmente, a partir de conceituações de Filosofia Política, Direito e Comunicação Social) e técnica de pesquisa bibliográfico-documental.

<sup>1</sup> PLATÃO. *A República*: Livro VII: 514a–541b. E-book (p. 296-298). Disponível em: [https://www.netmundi.org/home/wp-content/uploads/2017/07/Platao\\_A\\_Republica.pdf](https://www.netmundi.org/home/wp-content/uploads/2017/07/Platao_A_Republica.pdf). Acesso em: 28 nov. 2019.

## 2 DA INVESTIGAÇÃO JORNALÍSTICA AO ESCÂNDALO DA CAMBRIDGE ANALYTICA

O dia 17 de março de 2018 era para ser apenas mais um dia comum para os funcionários da CA, empresa fundada em 2013 como uma subsidiária do *SCL Group*<sup>2</sup> (uma empresa criada em 1990 com foco em mineração e tratamento de dados) e que em 1º de maio de 2018 solicitou em juízo a decretação de falência. As duas instituições já estavam acostumadas com alguns artigos que mostravam que a CA agia fora da lei, pois esta: (i) mantinha uma política contínua de coleta ilícita de dados pessoais; (ii) parte dos funcionários categorizam indivíduos, eleitores, usando seu próprio *software O.C.E.A.N.*; (iii) outros funcionários de grau sênior destinavam a maior parte dos recursos da CA para eleitores indecisos que poderiam, por exemplo, mudar de opinião entre votar a favor do Partido Republicano ou do Partido Democrata. A CA rotulou esses perfis de usuários como *the persuadables* (os persuadíveis). A empresa também fazia uso da rede social Facebook com a prática de *ataques-focais (microtargeting)*,<sup>3</sup> em inglês) de seus usuários, muitas vezes utilizando-se – de forma intencional – de notícias falsas (Fake News) para manipular tendências políticas de eleitores, resultando em uma *ruptura* da democracia e gerando, de forma deliberada, uma sociedade polarizada.

Essa prática – em sentido amplo – foi denunciada primeiramente pelo jornalista Harry Davies, em 11 de dezembro de 2015,<sup>4</sup> à época um jornalista de tempo integral para o jornal inglês *The Guardian*. Davies noticiou que a CA tinha coletado milhões de dados pessoais dos usuários da rede social Facebook de forma ilícita, isto é, sem o prévio consentimento (ou sequer a ciência) dos usuários. Essa prática havia sido encomendada para a então campanha presidencial estadunidense de 2016 do senador Ted Cruz.

Em dezembro de 2016, os jornalistas Hannes Grasseger e Mikael Krogerus, do periódico suíço *Das Magazin*, deram continuidade ao trabalho investigativo. Suas pesquisas foram traduzidas e republicadas pela Revista *Vice* em 30 de Janeiro de 2017.<sup>5</sup> O *The Guardian* continuou a investigação jornalística desde fevereiro de 2017, com a renomada jornalista Carole Cadwalladr, assim como o jornal independente *on-line The Intercept*, desde março do mesmo ano. No dia 7 de maio de 2017, Cadwalladr redigiu para o *The Observer*, em conjunto ao *The Guardian*, um artigo com título provocativo: *The great British Brexit robbery: how our democracy was hijacked*,<sup>6</sup> usando como principal meio de acesso às informações uma fonte, então, anônima. O artigo à época foi viral, alcançando mais de 63 mil compartilhamentos.

A CA, sentindo-se ameaçada na época, foi à ofensiva: ajuizou ações de responsabilidade civil e criminal por difamação ante os dois jornais e a jornalista, como tentativa de silenciar as investigações. Mesmo sob o temor de que todo o processo de investigação-jornalística fosse expurgado do mundo, Cadwalladr enfrentou a CA ao – de forma incansável – buscar o maior apoio na comunidade jornalística mundial possível ao seu alcance. Seu esforço logrou sucesso: tanto o canal britânico de TV aberta *Channel 4 News* quanto o jornal

<sup>2</sup> *SCL Group*. In: *Wikipédia*: a enciclopédia livre. Disponível em: [https://en.m.wikipedia.org/wiki/SCL\\_Group](https://en.m.wikipedia.org/wiki/SCL_Group). Acesso em: 28 nov. 2019.

<sup>3</sup> Para Jonathan Heawood (2018, p. 430-431), a prática de *microtargeting* (ataques focais) tornou-se possível por que foram os próprios usuários de mídias ou redes sociais que deram, de forma voluntária, a essas plataformas, uma quantidade colossal de informações pessoais. Essas empresas do novo ramo da economia de mídias ou redes sociais utilizam dados pessoais vendendo às empresas do ramo publicitário por meio de táticas de marketing eficientes, sem excluir publicitários políticos. Segundo o autor, empresas de novas mídias acompanham seus consumidores pela internet, não apenas mediante seus hábitos de compras, mas também pelas suas preferências políticas e prazeres sexuais. Assim, constroem perfis individuais altamente sofisticados a partir de centenas ou milhares de referências de dados. Plataformas de mídia social nunca poderiam ser desenhadas de forma mais maravilhosa do que para esse propósito. Tais empresas sequer necessitam pagar pela participação de cada consumidor em grupos focais, pois vasta quantidade de dados é a elas dada assim – quantidade esta que, então, é vendida a publicitários (inclusive políticos). A publicidade em mídias sociais pode atingir públicos em um nível granular: enquanto uma novela talvez possa atingir um público de cinco milhões, uma campanha publicitária na mídia social tem o potencial de atingir um público dez vezes maior. O *microtargeting* não é um efeito colateral da nova economia das mídias sociais, mas, sim, o piloto dessa economia. É por essa razão que dados pessoais são geralmente referidos como o “petróleo” da nova economia de mídias.

<sup>4</sup> DAVIES, Harry. *Ted Cruz using firm that harvested data on millions of unwitting Facebook users*. Londres: The Guardian, 2015. Disponível em: <https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data>. Acesso em: 28 nov. 2019.

<sup>5</sup> GRASSEGER, Hannes; KROGERUS, Mikael. *The Data That Turned the World Upside Down*. Nova Iorque: Vice, 2017. Disponível em: [https://www.vice.com/en\\_us/article/4x4x8n/the-data-that-turned-the-world-upside-down](https://www.vice.com/en_us/article/4x4x8n/the-data-that-turned-the-world-upside-down). Acesso em: 29 nov. 2019.

<sup>6</sup> CADWALLADR, Carole. *The great British Brexit robbery: how our democracy was hijacked*. Londres: The Guardian; The Observer, 2017. Disponível em: <https://www.theguardian.com/technology/2017/may/07/the-great-british-brexite-robbery-hijacked-democracy>. Acesso em: 30 nov. 2019.

americano renomado *The New York Times*, comprometeram-se com o *animus narrandi* inato à função de todo jornalista profissional e ao cumprimento do juramento de buscar a verdade dos fatos: continuaram a colaborar com Cadwalladr.

De volta à data, é 17 de março de 2018: o dia que selou o destino da CA para sempre. Nesse dia, três grandes organizações de periódicos e jornais do mundo – *The Observer*, *The Guardian* e *The New York Times* – publicaram em conjunto, simultaneamente, o artigo intitulado *How Trump Consultants Exploited the Facebook Data of Millions* (“Como os consultores de Trump exploraram os dados do Facebook de milhões”). O artigo somente foi viável após muito convencimento, por parte de Carole Cadwalladr, de demonstrar o caminho certo, ético e democrático – apesar de ter um enorme custo pessoal – de sua fonte anônima publicamente denunciar a CA de (i) suas práticas de mineração de dados (*Data Mining*) e tratamento de dados (interpreta-se aqui como a prática de *Data Scraping*)<sup>7</sup> e (ii) interferir de forma eficiente nos resultados de processos democráticos.<sup>8</sup>

Um ex-funcionário da CA (desligado em 2014 na época em que a CA ainda atuava sob o nome de *SCL Elections*), jovem de 28 anos, de origem canadense, de aparência *hipster*, acendeu a faísca da curiosidade da comunidade científica, jornalística e de usuários de redes sociais em escala mundial – seu nome é Christopher Wylie –, tornando-se o primeiro *whistleblower* (denunciante com fartas provas sobre as acusações feitas e evidências propositalmente divulgadas) do caso da CA.

Ocorre que, logo antes de sua demissão da SCL/CA, Wylie levou de forma discreta e cuidadosa cerca 84 milhões de dados pessoais e centenas de arquivos confidenciais da CA. Desde sua demissão, aparentemente a CA não tinha conhecimento que seu funcionário – ora autointitulado *Diretor de Dados* (da SCL/CA) ou *Cientista de Dados*, ora definido pela CA apenas como mais um *funcionário*<sup>9</sup> – tinha levado consigo uma volumosa quantidade de dados de seus servidores.

A ironia está no fato de que, durante todo o período de três anos após a demissão de Wylie, a CA vangloriava seu êxito nas campanhas pelo *Brexit* no Reino Unido e pela vitória do candidato Donald Trump à presidência dos EUA,<sup>10</sup> na Campanha pelo Partido Republicano de 2016. Uma corporação de tecnologia que coleta e também faz tratamento de dados de forma profissional e séria, deveria ter adoto medidas e contingências de segurança que assegurariam possíveis vazamentos de informações. Esse, contudo, não foi um caso

<sup>7</sup> *Data scraping* é um processo que utiliza a transferência de dados entre programas e aplicativos com dados estruturados entre computadores e também para usuários no end-point (ponto de acesso terminal para o usuário), gerando diversos tipos de resultados correlacionados, podendo servir para diversas aplicações – sejam elas acadêmicas, sejam para o mundo prático. Utiliza-se uma ou a combinação de três variantes técnicas como: (i) *screen scrapping* (raspagem de dados visuais diretamente de um terminal), (ii) *Web Scraping* (ou raspagem de dados da web usando como fonte primária de informações dados em linguagem HTML e XHTML mas não exclusivamente), que objetivam servir como uma interface ou protocolo de comunicação entre programas de computador para simplificar a criar programas – ou ferramenta – para coletar dados de página da web; e (iii) *Report Mining* (mineração de relatórios), que tem como finalidade a coleta de dados de arquivos prontos para usuário-final, coletando dados desde HTML e XHTML, até textos e arquivos com extensão “.pdf”, com a ajuda de uma A.P.I. Um exemplo atual da combinação de técnicas de *Data Scraping* está no artigo de Kyle Vanhemert, *This Simple Data-Scraping Tool Could Change How Apps Are Made* (2014).

<sup>8</sup> BERGHEL, Hal. *Malice Domestic – the Cambridge Analytica Dystopia*. Nevada: University of Nevada, 2018. O autor aponta o escândalo de *Cambridge Analytica*, enquanto um ataque à de Democracia dos EUA, como um episódio já conhecido pelos americanos. Em seu artigo, o autor mostra que é normal que ocorram certas irregularidades no processo de eleição americana, e expõe a novidade na utilização de *microtargeting* pela CA por meio das redes sociais.

<sup>9</sup> Em entrevista para o documentário *The Great Hack* (“Privacidade Hackeada”, 2019) o ex-CFO e COO interino da CA, Julian Wheatland, relatou que Chris Wylie falou com grande autoridade sobre o que ocorreu dentro da Cambridge Analytica e SCL durante 2015 e 2016, em uma época em que ele nunca esteve lá. Ele trabalhou para a empresa por nove meses, saindo em 2014. Ele, então, direcionou-se e fez uma proposta à campanha de Trump e perdeu. Chris Wylie teve como objetivo matar a empresa.

<sup>10</sup> A Cambridge Analytica foi inicialmente contratada para auxiliar no êxito da Campanha Eleitoral à Presidência dos E.U.A. pelo candidato Ted Cruz. Acredita-se que a família Mercer, com 80% de controle da *Cambridge Analytica*, tenha convencido Ted Cruz a renunciar sua candidatura. Em seu lugar, a CA deveria fornecer toda ajuda possível ao candidato que ora estava a favor do Partido Republicano, e anunciava que ele iria nomear candidato independente: Donald Trump. A família Mercer fez grande doação à campanha de Donald Trump nos E.U.A. Logo, é possível inferir a *influência política* da família Mercer não apenas dentro da CA, mas no processo democrático americano, tendo como prova contundente o *Projeto Alamo*.

isolado com a CA. Essa não seria a única vez em que dados pessoais foram vazados<sup>11</sup> da empresa. Brittany Kaiser, analista de dados sênior da CA, também resolveu aderir à postura adotada por Wylie e se apresentou, de forma voluntária, para depor no Reino Unido contra a CA.

Vale notar, entretanto, que é perceptível que a perspectiva da CA era outra. A empresa, que já tinha logrado sucesso em campanhas na África do Sul (campanha presidencial) e no Reino Unido (referendo acerca do *Brexit*), continuava a demonstrar um comportamento segundo o qual parecia entender que, apesar de todos os vazamentos e depoimentos contra a ela, tudo seria contornável. Um exemplo de evidência sobre o clima da CA ocorreu quando a empresa de tecnologia prestou um comunicado oficial à imprensa, feito por Alexander James Ashburner Nix, ou Alexander Nix (C.E.O. da CA), na vitória da campanha eleitoral americana de Donald Trump, em 2016: “*We are thrilled that our revolutionary approach to data-driven communication has played such an integral part in President-elect Trump’s extraordinary win*”.<sup>12</sup>

Não se sabe ao certo se a CA realmente sabia que seu fim estava próximo ou se a empresa estava desiludida. Até as audiências públicas referentes ao vazamento de dados da CA começarem, o próprio ex-CFO Julian Wheatland alegava que não apenas ele acreditava, mas os demais diretores da CA também especulavam que a empresa, então avaliada em milhões, iria saltar para bilhões.

A família americana Mercer, conhecida por ter sido a maior doadora à campanha de Donald Trump, também possuía 80% do controle acionário sobre a CA. Muitos atores poderosos apostaram alto no sucesso ímpar da empresa. Com as audiências públicas, no entanto, realizadas tanto no Reino Unido quanto pelo Facebook perante o Senado dos EUA e os depoimentos de Christopher Wylie – com maior relevância – e de Brittany Kaiser, tornou-se claro o início do fim da CA.

### 3 DA OBSCURIDADE AO CONHECIMENTO DA PRÁXIS DA CA

Assim como no Mito da Caverna, é fundamental libertar-se e se forçar o olhar para o fogo do conhecimento. O conhecimento adquirido, mediante investigação jornalística previamente esclarecida apenas, dá uma perspectiva da nova realidade. Logo, também é necessário conhecer e entender o *modus operandi*, isto é, o modo em que a SCL/CA operava.

A carreira dos cientistas de dados não é fácil, pois: (i) analisam um enorme volume de informações pessoais (análise de *big data*), (ii) categorizados por indicadores (praticam *data mining* e *data scraping*) e (iii) tentam prever tendências das ações de indivíduos ou grupos (*microtargeting*). Logo, são tarefas a partir de medidas desumanas, pois o objeto de estudos sempre é feito com pesquisa comportamental de indivíduos, e valem muito mais que dados pessoais, metadados e outras métricas calculadas. Logo, também afirma-se que indivíduos reunidos em um banco de dados valem mais *naquele* banco de dados – por maior e mais complexo que seja – em que possam ser rotulados.

<sup>11</sup> Os dados dos usuários da rede social Facebook foram primeiramente obtidos pelo aplicativo *itsyourdigitallive*, desenvolvido sob a supervisão do doutor Aleksandr Kogan. Posteriormente, o software *O.C.E.A.N.* foi desenvolvido dentro da CA. Nenhum dado, *metadado* e/ou informação foi disponibilizado pela SCL/CA. Neste artigo, ao ler *vazamento de dados*, assim como nos demais artigos acadêmicos e jornalísticos, trata-se essencialmente da forma antiética e imoral de obtenção desses dados pela SCL/CA. Basta pensar que, caso alguém da SCL/CA publicasse na web todos os dados que conseguisse obter, não somente estaria cometendo crime em diversas jurisdições ao mesmo tempo no mundo, mas também estaria esvaziando o *fundo de comércio*, a *commodity* que a SCL/CA possuía. Em outras palavras, nunca esteve nos planos da SCL/CA divulgar as informações e de que modo foram coletadas, armazenadas e tratadas. Somente as comissões no Reino Unido tiveram acesso – de forma parcial – até que a SCL/CA decretasse falência e todos os arquivos fossem objeto protegido por sigilo de justiça no Reino Unido. Já nos E.U.A., o *Facebook* foi réu de ter colaborado de forma ativa com a SCL/CA durante a campanha presidencial americana de 2016. O fundador e CEO do *Facebook*, Mark Zuckerberg, teve de prestar depoimento ao Senado. Em 2018 novamente o *Facebook* não vazou ao público dados pessoais de nenhum usuário.

<sup>12</sup> Cambridge Analytica. *Cambridge Analytica Congratulates President-elect Donald Trump and Vice President-elect Mike Pence*. Nova Iorque: PR NewsWire, nov. 2016. Disponível em: <https://www.prnewswire.com/news-releases/cambridge-analytica-congratulates-president-elect-donald-trump-and-vice-president-elect-mike-pence-300359987.html>. Acesso em: 3 Dec. 2019. Tradução livre: “Nós estamos empolgados com a nossa abordagem revolucionária com a comunicação dirigida-por-dados em como esta tem atuado como elemento integral para a extraordinária vitória do Presidente-Eleito Trump”.

Para esses analistas de dados, entretanto, é possível, a partir de um número grande de indicadores, saber, a título ilustrativo, do que alguém gosta de comprar *on-line*, como alguém se veste, em quem votou nas eleições passadas (dentre vários outros tópicos comportamentais) e, logo, concluir, em tendências precisas, em quem a pessoa votará nas próximas eleições de 2020 muito antes de os candidatos realizarem publicamente suas respectivas campanhas.

Isso acontece como o caso do *API*, chamado *thisisyourdigitallife*<sup>13</sup> pela *CA*, por meio de coleta de dados de forma imoral e dando um tratamento aos dados pessoais para fins privados. Eles, porém, não conseguiriam agir de forma eficiente, pois apenas o *API fora* previamente descrito, mas existiram também outros fatos.

Usuários de redes sociais muitas vezes clicam na opção “eu aceito os termos e condições”<sup>14</sup> deste aplicativo, quanto à Política de Privacidade, sem o conhecimento de que os termos e condições podem ser alterados, permitindo – em tese – que as empresas utilizem tais dados para quaisquer finalidades: inclusive a manipulação de processo democrático. Uma empresa – por cerca de 20 anos *sem fins lucrativos* – foi capaz, nas eleições americanas para a presidência, em 2016, de obter 1.500 pontos de referência por indivíduo para uma população um pouco maior – à época – de 300 milhões de cidadãos. Isto é, 450 bilhões de pontos de referência, em tese.

A Cambridge Analytica entrou em juízo no Reino Unido em primeiro de maio de 2018, decretando falência, e todos os arquivos da empresa permanecem até hoje sob investigação e sigilo judicial. Apesar de não ser possível o acesso aos arquivos da empresa, sua forma de atuação foi bem detalhada e descrita por Kaiser.

O *modus operandi* da *CA* era dividido em três frentes de ataque: o primeiro era responsável pela coleta, armazenamento e tratamento de dados pessoais no Facebook, incluindo, a título meramente exemplificativo, fotos pessoais, *posts insignificantes* do cotidiano, lista de amigos, lista de pessoas bloqueadas, grupos que as pessoas ingressaram e grupos que participam ativamente.

Essa tarefa de análise ou tratamento de um colossal banco de dados (*big data*) e sua categorização era realizada utilizando um software proprietário da *CA* chamado O.C.E.A.N.<sup>15</sup> Um indivíduo, por intermédio de uma pesquisa dentro do Facebook, não apenas respondia questões como “Eu estou sempre preparado” ou “Eu geralmente me sinto cabisbaixo”, em uma gradação que varia entre inexato, neutro e exato. O resultado final indicava que tipo de comportamento você possui diante de diferentes cenários e hipóteses.

<sup>13</sup> Em 2013, mesmo ano de criação da Cambridge Analytica, o professor de Psicologia da renomada Universidade de Cambridge, doutor Aleksandr Kogan (ora também conhecido como doutor Spectre), foi contatado à época por Christopher Wylie (a serviços da *SCL/CA*). O pedido de Wylie era que o professor trabalhasse em um aplicativo, posteriormente conhecido como *thisisyourdigitallife*. De acordo com o sociólogo e analista de privacidade Kozłowska: *This app, offered on Facebook, provided users with a personality quiz. After a Facebook user downloads the app, it would start collecting that person's personal information such as profile information and Facebook activity (e.g., what content was "liked"). Around 300,000 people downloaded the app. But the data collection didn't stop there. Because the app also collected information about those users' friends, who had their privacy settings set to allow it, the app collected data from about 87 million people. (Este app oferecido dentro do Facebook dá aos usuários um teste de personalidade. Depois que um usuário do Facebook faça o download do app, [o aplicativo] começa a coletar informações pessoais daquele indivíduo como informações de seu perfil assim como sua atividade no Facebook (por exemplo, quais conteúdos eram "admirados" [liked, em inglês]). Cerca de 300 mil pessoas fizeram o download do aplicativo. A coleta de dados, contudo, não terminou aí. O aplicativo também coletou informações sobre os amigos desses usuários, aqueles que tinham os ajustes de privacidade para permitir essa prática; o app coletou dados de cerca de 87 milhões de pessoas).* KOZŁOWSKA, Iga. *Facebook and Data Privacy in the Age of Cambridge Analytica*. Seattle: Henry M. Jackson School of International Studies, College of Arts and Sciences, University of Washington, 2019 (2 p., tradução livre).

<sup>14</sup> Em 2010, a empresa desenvolvedora de jogos para computador e videogames *Blizzard* (por meio da *GameStation* no Reino Unido) adicionou ao EULA (*End User License Agreement* ou *Licença de Uso para o Usuário Final*) uma forma de *Termos e Condições* para jogar um jogo: usuários que clicavam sem ler as cláusulas do contrato não sabiam que, ao aceitar os termos e condições, estariam vendendo a alma deles para a empresa. Sete mil e quinhentas almas foram comercializadas naquela época. A empresa fez isso como uma provocação ao fato de que praticamente ninguém lê os termos e condições de aplicativos e programas, inclusive jogos. Para maiores informações: BROWNLEE, John. *GameStation EULA collects 7,500 souls from unsuspecting customers*. San Francisco: Geek.com, 2010. Disponível em: <https://www.geek.com/games/gamestation-eula-collects-7500-souls-from-unsuspecting-customers-1194091/>. Acesso em: 5 dez. 2019.

<sup>15</sup> O.C.E.A.N. é um software na forma de *A.P.I.* que serviu como um teste de personalidade ou teste comportamental, e significa *Openness* (ou *Abertura*: o quão aberto um indivíduo está para novas ideias e experiências), *Conscientiousness* (ou *Consciência*: o quão objetivo, possuidor de metas, persistente e organizado um indivíduo é), *Extraversion* (ou *Extrovertimento*: o quão um indivíduo é enérgico e extrovertido com o mundo ao seu redor), *Agreeableness* (Ou *Concordância*: o quão um indivíduo coloca os interesses e necessidades de outros à frente dos seus) e *Neuroticism* (ou *Neuroticismo*: o quão sensível um indivíduo é ante a *gatilhos* emocionalmente negativos, assim como perante o *stress*). Além do O.C.E.A.N., outros dois testes comportamentais muito similares foram inseridos com interesses privados à *CA*, também conhecidos como *The Big Five Assessment Test* e o *The Five Factor Survey*.

Ao clicar em fazer o teste pelo Facebook, contudo, quase a totalidade dos usuários (aqueles que não leram os termos e condições da pesquisa e a política de privacidade do aplicativo) dava acesso à CA para coletar os seus dados pessoais – a título exemplificativo: idade, cor, religião, altura, região onde o indivíduo reside e trabalha, sua geolocalização, por onde você costuma caminhar, seu passo de caminhada, acesso a todas as suas postagens, fotos e arquivos que foram colocados nessa rede social.

A violação ao Direito de Privacidade não parava aqui: vale ressaltar que – sem o consentimento e conhecimento – todos os amigos daquele indivíduo que fez o teste de personalidade *O.C.E.A.N.* também tinham todos os seus dados coletados. Por meio dessa *falha* de design na rede social *Facebook*, milhões de seus usuários ficaram às margens da proteção de sua privacidade. Foi dessa forma que a CA *hackeou* o *Facebook* ao coletar não apenas todos os dados pessoais supradescritos, mas de seus amigos e conhecidos também. Ademais, a CA não somente obteve um *retrato* do perfil coletado de cada usuário do *Facebook*, mas obteve um *filme em tempo real* – uma vez que a coleta de dados era contínua, e, isto posto, apenas bastava fazer o teste de personalidade uma vez –, desenvolvendo, de modo prospectivo, diversas tendências de todos os usuários.

De forma *orgulhosa*, a CA alegava, em um determinado momento – após o senador Ted Cruz renunciar à campanha presidencial americana de 2016 e o *Projeto Alamo*<sup>16</sup> estar em pleno funcionamento –, ter acesso à quase totalidade dos eleitores americanos. Essas equipes de analistas de dados possuíam uma tarefa menos difícil dentro da empresa: apenas gerar relatórios úteis e em tempo real ao seu principal cliente – a família Mercer – interessada em que Donald Trump ganhasse as eleições americanas de 2016. A empresa utilizou roteiros de programação (*scripts*) como *filtros* de pesquisa demográfica, realizando *ataques-focais (microtargeting)*<sup>17</sup> com muita precisão e eficiência. Também fizeram uso de tecnologia de Inteligência Artificial – mesmo que ainda em estágios rudimentares de *aprendizado artificial-mecânico (machine learning)* –, com a tarefa de segregar e polarizar artificialmente determinados grupos da sociedade americana em um processo muito mais célere.

Um segundo grupo era responsável – no curso das eleições americanas de 2016 – por uma tarefa mais complexa. Funcionários *Sênior* da empresa – como é o caso de Brittany Kaiser – tinham de minerar as informações (*data mining*) desse enorme banco de dados e, por este processo, buscar em Estados da Confederação Americana os *votos indecisos* (votos que poderiam ir tanto para o lado Conservador quanto para o lado Democrata).

Alguns Estados do EUA – mais precisamente Califórnia, Florida e Nova Iorque – são notoriamente conhecidos, em época de eleição, como Estados *coringa*. Em outras palavras, são Estados que possuem quase a mesma quantidade de eleitores dispostos a votar tanto para a direita Conservadora quanto para a esquerda<sup>18</sup> democrata, e uma quantidade significativa de eleitores definidos por funcionárias sênior, como Kaiser, de *the persuadables* ou *os persuasíveis*. Kaiser tinha como uma de suas principais funções a criação de *ataques-fo-*

<sup>16</sup> O *Projeto Alamo* foi designado pela CA em parceria com a Campanha Presidencial do Partido Republicano de 2016 de Donald Trump e possuía como objetivo atender à campanha eleitoral apontando à equipe oficial de Donald Trump – porém sem indicar ou demonstrar o Modus Operandi da CA (uma empresa do Reino Unido que detinha muito conhecimento sobre a vida cotidiana dos americanos) – como realizar ataques-focais (microtargeting) de perfis on-line, no Facebook, em diversas regiões dos E.U.A. ao mesmo tempo.

<sup>17</sup> Para Campos, a fala de Wylie para o *The Guardian* resume bem o pensamento motriz por trás de NIX e da *Cambridge Analytica*: Christopher Wylie, ao descrever a caracterização das operações da [Cambridge] Analytica, está bem em sintonia, afirmando que a firma estava: “[brincando] com a psicologia de todo um país sem sua anuência ou ciência [...] no contexto do processo democrático.” Como exemplificação, Campos aponta o fato de que durante a campanha de Trump foram usadas práticas de *grupos-focais (microtargeting)*: For example, Trump’s Campaign used “dark posts” which could only be seen by targeted groups in the Little Haiti district of Miami. These posts contained messages about the Clinton Foundation’s failure to respond to the earthquake in Haiti, aiming to sway potential Clinton voters away from the ballot box (GRASSEGGER; KROGERUS, 2017) (“...foram utilizados ‘posts’ às escuras”, com certo grau de anonimato, somente para *grupos-focais* no distrito de *Little Haiti* em *Miami*. As mensagens continham um conteúdo sobre a Fundação de Clinton em fracassar a responder o terremoto no Haiti, tentando convencer eleitores que votariam na Hillary a não votarem nela – tradução livre). (CAMPOS, Matt. Cambridge Analytica, Microtargeting, and Power – “A Full-Service Propaganda Machine” in the Information Age. *Trail Six, Undergraduate Journal of Geography*, British Columbia, v. 13, p. 26-27, 2018-2019).

<sup>18</sup> Nos E.U.A. o Partido Democrata não é reconhecido necessariamente como um partido de esquerda. É um Partido Político contrário ao Partido Republicano. Apesar, contudo, de o Partido Democrata ter diversas ideias de política pública consideradas em certa medida, era relacionado ao Socialismo ou a uma ideia de Estado do Bem-Estar Social; eles não são um partido publicamente assumido como de esquerda. São progressistas em muitos aspectos, porém em diversas questões seus membros divergem muito sobre assunto polêmico como o Direito da Mulher ao Aborto ou sobre a Comercialização de maconha.

cais aos *the persuadables* ou os *persuadíveis*. Dessa forma, tornou-se possível moldar como tais Estados votariam, mesmo que isso significasse manipular uma cultura regional e decidir a política de maneira antiética e antidemocrática.

Por fim, o último grupo de funcionários da Cambridge Analítica funcionava de forma quase clandestina a tudo que é ético, democrático e contrário ao espírito dos *Founding Fathers* (fundadores do Estados Unidos da América). Trata-se, em síntese, de traição a todo um processo democrático que deve sempre ser vigiado e tutelado. Este último grupo, em que muitos funcionários da empresa até hoje alegam que desconheciam as práticas descritas a seguir, tornou-se uma ferramenta maliciosa extremamente eficiente.

A CA obteve sucesso ao polarizar grupos em Estados Americanos assim como havia obtido êxito, com mesmo estilo perverso, no Reino Unido com o *Brexit*. Para auxiliar a polarização artificial, não foram poupados esforços para criação de notícias falsas (Fake News, em inglês) e de maneira dolosa realizar *ataques-focais* (*microtargeting*<sup>19</sup>) em diversos usuários dessa rede social.

Como exemplo real, porém ilustrativo, da polarização artificial criada pela CA está: i) um Estado americano como a Geórgia (tendo como capital: Atlanta), localizada no Leste Americano, que possui uma predominância de negros. Em subúrbios e bairros de Atlanta, a hegemonia é de negros e, infelizmente, assim também é a pobreza. Município como Atlanta, apesar de ter um dos aeroportos mais eficientes do mundo, também é um dos que possuem uma das maiores desigualdades sociais nos E.U.A. Logo, a CA usou ferramentas de publicidade em mídias sociais no *Facebook* e publicou, diretamente na *timeline* (na linha de informações novas de cada usuário desta mídia social) de usuários, campanhas publicitárias com a *hashtag* #BlackLivesMatter (Vidas Negras Importam) para a população de Atlanta. Não haveria problema ético se não fosse o fato que (ii) a mesma empresa operasse da mesma forma em municípios como *Kansas City*, em Estados Centrais (nos E.U.A. existem três distintos fuso-horários entre Leste, Centro e Oeste), de predominância de cor de pele hegemonicamente branca, mas igualmente atingindo indicadores de desigualdade social.

A CA buscava disseminar um sentimento de ódio e polarização entre brancos e negros, pois nesses estados centrais – ao mesmo tempo – postava propagandas com imagens e *hashtags* de #WhiteLivesMatter (Vidas Brancas Importam) ou #AllLivesMatter (Todas as Vidas Importam).

Sem relativizar o mérito da questão filosófica, o que a empresa claramente tentou e conseguiu obter foram resultados eficientes, visíveis em tempo real (lembrem-se: eles tinham acesso aos seus *posts* antes, durante e após a vitória de Donald Trump à presidência americana) de rixas de natureza racial. Dessa forma, retirou-se da pauta e do escopo democrático da eleições questões e matérias relevantes às campanhas dos presidenciais.

#### 4 DO LEGADO DEIXADO PELA CAMBRIDGE ANALYTICA

Um dos maiores exemplos dos possíveis *ensinamentos* que o *escândalo da CA* nos apresenta é que infelizmente se está fadado a apenas um único e fatídico episódio de (i) usurpação de dados pessoais, (ii) de coleta de informações em grande quantidade e de forma continuada e (iii) que podem tecer toda uma *narrativa comportamental* de quem é cada indivíduo. Mesmo que essas *narrativas* sejam verossímeis, indivíduos serão sempre mais do que apenas métricas; conjuntos de indicadores transformados em estatística e logo permitindo que algumas conclusões sejam inferidas.

Apesar de a Cambridge Analytica não existir mais formalmente, desde um pouco antes de seu fim, já existiam e ainda persistem indícios de novas empresas de *análise comportamental eleitoral* no mundo, inclusive no Brasil. Durante o primeiro semestre de 2018, a Cambridge Analytica fez uma parceria com a empresa brasileira (Ponte Estratégia) do Publicitário André Torretta (também dono da McMann & Tate Pesquisas e

<sup>19</sup> Há duas importantes observações sobre os ataques-focais (*microtargeting*): i) não são eficazes em relação a determinados grupos (ou indivíduos) que verificam a fonte das informações (*fact-checking*) antes de reproduzi-los nas redes sociais – mas, como a maioria da população, não apenas dos EUA, encontra-se à margem de uma educação de qualidade, universal e gratuita, a penetração quase cirúrgica desses ataques em redes sociais é alta; ii) as consequências e danos causados por *microtargeting* são gravíssimos, pois esses ataques: buscam explorar dados pessoais; escondem a sua verdadeira função e meta; alegações realizadas em privado não podem ser corrigidas em um ambiente mercantilizável de ideias; muitas vezes são relacionados à disseminação de informações falsas; permitem que partidos políticos façam promessas incompatíveis com diferentes segmentos de seu eleitorado; e permitem que atores políticos estrangeiros realizem ataques com informações falsas e desinformações (HEAWOOD, 2018).

Eventos atuante Projeto #Colabora). A joint-venture no Brasil durou poucos meses e chamava-se CA-Ponte. Em entrevista para o jornal El País, Torretta, de forma franca, chegou ao ponto de questionar se não existe arrogância em suas respostas: “Estou te enganando? Não, estou apenas entregando o que você quer ver” – disse Torretta ao ser questionado sobre sua estratégia com a parceria. Vale dar a atenção devida à sua fala – mesmo com o fim da CA-Ponte – por que ele já prestou serviços desde Sarney a FHC, incluindo para a LIDE (Organização de propriedade de João Doria), bem conhecidos por marqueteiros no Brasil. O El País divulgou em 15 de outubro de 2017 que, segundo, Torretta: “O problema é que a Cambridge talvez seja muito sofisticada para o mercado brasileiro regional, porque a gente não faz nenhuma campanha digital bem feita”. “Agora está abrindo uma brecha para que os políticos façam impulsionamento (pagar para que as publicações alcancem mais pessoas no Facebook).” Assim ele acredita que “a Cambridge ficará sexy” para o mercado brasileiro. Também outra passagem salta os olhos quando ele afirma nos Estados Unidos: o “ovo” fica “em pé” graças as cerca de 7.000 informações que a Cambridge, segundo Torretta, consegue levantar sobre cada indivíduo. No Brasil, Torretta calcula que este número de informações pontuais sobre cada um chegue a 750, e é aí que começa a “tropicalização” que ele diz ter feito no método. “Os bancos de dados do Brasil estão sendo construídos agora. Temos bons e munidos bancos de dados públicos. O governo deve ter, no mínimo, de 500 a 700 pontos de informação da gente, e o IBGE deve ter uns 250 pontos, não pessoal, mas da microrregião onde você mora”, explica. “Já temos então 700 pontos de informação de cada brasileiro. O Serasa deve ter mais uns 40 pontos de informação”, se empolga. Ele se diz convicto de que, mesmo que a situação de dados brasileira não se compara com a dos EUA, sua nova empresa já vai trabalhar com muitíssimo mais informação em qualquer concorrente seu. Nem sequer a iniciativa privada usa o potencial dos dados já disponíveis no Brasil, afirma o marqueteiro (ROSSI; MARREIRO, 2017).

Em uma entrevista posterior (20 mar. 2018) ao BBC Brasil, no entanto, Torretta já adotava outro tom, pós a circulação simultânea em três jornais renomados naquele mesmo mês, isto é, pós o escândalo da CA ter viralizado: “Ainda bem que isso saiu agora. Se tivesse saído daqui a seis meses eu estava morto. Foi uma surpresa. Eu não sabia de nada”, diz Torretta, para quem as denúncias parecem “coisa de filme de 007”. Ele nega repetidas vezes que tivesse conhecimento do modo como a empresa obteve informações sobre eleitores americanos. [...] Segundo Torretta, as negociações com possíveis clientes estavam começando e nenhum contrato havia sido firmado até o escândalo vir à tona. Ele não quis revelar os nomes dos interessados no serviço da Cambridge Analytica, em cumprimento com o que chamou de “ética do marketing político”. Torretta apenas negou que tenha procurado o governador de São Paulo, Geraldo Alckmin, porque o tucano já teria um marqueteiro, e ressaltou que nunca trabalharia para Jair Bolsonaro. “Minha regra era não trabalhar com extremos, tanto de esquerda quanto direita” (PASSARINHO, 2019).

Por fim, no curso deste artigo foram levantadas diversas empresas que foram criadas, fechadas e recriadas. Por recriadas, interpreta-se fundadas pelos mesmos proeminentes indivíduos sob outras pessoas jurídicas: indivíduos como Nix, que atuou como presidente da CA, e também fez parte da Emerdata, o que seria uma espécie sucessora da SCL/CA. A empresa foi fundada em agosto de 2017 e tinha como sede o mesmo endereço da SCL/CA em Londres. Em 23 de janeiro de 2018, Nix foi nomeado diretor da Emerdata Ltda. Em 16 de março do mesmo ano, as duas filhas do Bilionário Robert Mercer, Rebekah Mercer e Jennifer Mercer, também foram nomeadas diretoras. Um outro diretor da Emerdata foi o lobista e presidente da Frontier Service Group (uma empresa de segurança privada com forte atuação na África), Johnson Chun Shun Ko. A última diretora do Emerdata foi Jacquelyn James-Varga (ela previamente trabalhou diretamente para a Fundação Mercer Family). Em janeiro de 2018, a Emerdata anunciou que tinha mais de 19 milhões de dólares americanos de investidores estrangeiros. A Emerdata também não existe mais, porém ela foi comprada pelo Grupo Firecrest Technologies em 7 de março de 2018 e terminada em 19 de fevereiro de 2019.<sup>20</sup> Também vale citar que durante o mês de maio de 2018, logo antes da CA decretar falência no Reino Unido, Nix aparentemente sacou 6 milhões de libras esterlinas ou 8 milhões de dólares americanos.<sup>21</sup> Outro exemplo é a *AggregateIQ*, empresa de

<sup>20</sup> FIRECREST TECHNOLOGIES LIMITED, Company number: 11238956. Londres: Companies House of The United Kingdom Disponível em: <https://beta.companieshouse.gov.uk/company/11238956/filing-history>. Acesso em: 8 dez. 2019.

<sup>21</sup> KANTER, Jake. *Cambridge Analytica's CEO allegedly took \$8 million from the firm before its closure*. Nova Iorque: Business Insider. 2018. Disponível em: <https://www.businessinsider.com/alexander-nix-allegedly-took-8-million-cambridge-analytica-2018-6?r=UK>. Acesso em: 8 dez. 2019.

consultoria no ramo de Tecnologia da Informação, fundada em 2013 no Canadá. A empresa prestou serviços à CA ao desenvolver uma plataforma de software chamada *Ripon*. O conhecimento dessa plataforma tornou-se pública depois de um *GitLab* (um repositório na internet de diferentes espécies de arquivos para um API funcionar e ser testado na internet) desprotegido ser descoberto por meio de reportagem por Dell Cameron.<sup>22</sup> Ademais, em fevereiro de 2018, a *Data Propria* foi criada como uma empresa subsidiária da *CloudCommerce Inc.*, tendo como presidente o C.T.O. ou *diretor tecnológico operacional* da ex-CA, Matt Oczkowski, tendo participação societária de Brad Parscale (*CloudCommerce Inc.*), que é o *gerente de campanha* para a reeleição presidencial de Donald Trump em 2020. A empresa<sup>23</sup> está contratando cientistas de dados (verificado até a submissão deste artigo em 14 de dezembro de 2019) e já existem algumas alegações indicando a sua atuação para a campanha de reeleição de Donald Trump em 2020.<sup>24 25</sup> Por fim, vale também informar a existência da *Civis Analytics*,<sup>26</sup> empresa fundada por Dan Wagner (que foi o *diretor de Análise de Dados* ou CAO, *Chief Analytics Officer*, para a campanha de reeleição de Barack Obama em 2012) e financiada por Eric Schmidt (ex-CEO/Presidente da Google entre 2001-2011), focada em consultoria e *software* de ciências de dados. A empresa ajuda outras empresas a entenderem seus bancos de dados, dar um tratamento eficiente a eles e prever determinados comportamentos.

## 5 IDENTIFICAÇÃO DE NOVOS PROBLEMAS *VIRAIS*: NEM TODO PROBLEMA POSSUI UM ANTÍDOTO – ALGUMAS MEDIDAS PALIATIVAS JÁ AUXILIAM NA MITIGAÇÃO DE EVENTUAIS DANOS

De forma inconclusiva e preocupante, parte deste artigo é finalizada. Ao investigar-se as práticas da CA buscou-se, ao mesmo tempo, ver seus oponentes neste *mercado azul*.<sup>27</sup> Apesar de ser possível, em dezembro de 2019, observar a participação ativa de novas empresas e *players* (pessoas físicas e jurídicas com interesse privado por trás pelo financiamento e participação societária nessas empresas), é difícil saber se a CA foi o *catalisador* para que novas empresas fossem criadas após seu escândalo, aprendendo que o mundo inteiro obteve conhecimento e aperfeiçoando, em especial, a segurança do banco de dados *proprietário* das novas empresas.

Ao mesmo tempo, não é possível ter certeza de que algumas dessas empresas já existiam antes do escândalo da CA. O vazamento de informações e a investigação jornalística apenas lançaram luz sobre empresas que já atuavam no mercado, porém com um perfil mais discreto e que também aumentaram suas respectivas medidas de proteção e salvaguarda de seus bancos de dados.

<sup>22</sup> CAMERON, Dell. *AggregateIQ Created Cambridge Analytica's Election Software, and Here's the Proof*. Nova Iorque: Gizmodo Media Group, 2018. Disponível em: <https://gizmodo.com/aggregateiq-created-cambridge-analyticas-election-softw-1824026565>. Acesso em: 9 dez. 2019.

<sup>23</sup> Disponível em: <https://datapropria.com>. Acesso em: 9 dez. 2019.

<sup>24</sup> FARIVAR, Cyrus. *Data Propria, run by Cambridge Analytica alumni, working on Trump 2020 campaign*. São Francisco: Arstechnica, 2018. Disponível em: <https://arstechnica.com/tech-policy/2018/06/data-propria-run-by-cambridge-analytica-alumni-working-on-trump-2020-campaign/>. Acesso em: 9 dez. 2019.

<sup>25</sup> Ver também: HORWITZ, Jeff. *AP: Trump 2020 working with ex-Cambridge Analytica staffers*. Nova Iorque: The Associated Press, 2018. Disponível em: <https://apnews.com/96928216bdc341ada659447973a688e4>. Acesso em: 9 dez. 2019.

<sup>26</sup> Disponível em: <https://www.civisanalytics.com>. Acesso em: 9 dez. 2019.

<sup>27</sup> Por *Mercado Azul* atribui-se a interpretação da terminologia aplicada à *Gestão de Negócios*, em especial muito aplicada a *Novos Modelos de Negócios* e *Startups*. Trata-se, em síntese, de *Mercados Nunca Explorados*, logo a cor azul turquesa, de tom claro e quando é perceptível até onde se *pisa na areia* (uma analogia de o quão profundo é o potencial deste mercado). A criação deste novo Mercado existe há cerca de uma década: alguns indicam as campanhas presidenciais de Barack Obama, visto como o pioneiro na aplicabilidade de métricas ao seu mote “*Yes, we can!*” (*Sim, nós podemos!* – em tradução livre). Outros afirmam que foi a S.C.L., sob sua subsidiária *Cambridge Analytica*, a primeira empresa a vender serviços usando *psicométricas* combinadas, como *estudos comportamentais* e outras práticas mais invasivas já descritas neste artigo, e como a pioneira no ramo do que atualmente se busca rotular o termo *electioneering* (ou *engenharia eleitoral*).

Por ser um tema recente, a única conclusão plausível é de que é possível inferir neste ponto que um próximo vazamento há de ocorrer mais cedo ou mais tarde (em relação a uma eleição). Isso<sup>28</sup> deve-se, acima de tudo, por que empresas sempre serão feitas, mantidas e administradas por seres humanos, como Wylie e Kaiser.

Agências de Inteligência também estão vulneráveis a vazamentos. Apenas a título de anedota: Edward Snowden era analista de dados para uma das maiores agências de inteligência do mundo: a NSA (*National Security Agency*). Uma agência de inteligência americana centenas de vezes maior que o FBI (*Federal Bureau of Investigation*) e a CIA (*Central Intelligence Agency*) juntas. Snowden foi o *whistleblower* no caso supracitado. Assim como Wylie, tinha uma jornalista séria e comprometida com sua carreira, agindo com lisura: Cadwalldr. Snowden, da mesma forma, confiou no trabalho jornalístico sério e competente, como Glenn Greenswald.

Pode-se notar, em dezembro de 2019, que perceptivelmente surge uma nova preocupação que evita holofotes do jornalismo investigativo e da sociedade civil e organizada. Emerge como expressão do escândalo da CA: trata-se de um novo mercado chamado de *electioneering a favor* de grupos políticos, empresariais, bélicos ou quem pague mais, além de diversos *Predictable Analytic Toolkits* (conjunto de ferramentas digitais que servem para coletar dados, classificar determinados grupos de eleitores e inferir conclusões, tendências e probabilidades de previsões) estarem à venda na *deep web* (a internet não indexada por website – indexadores de conteúdo – como o Google e parte do Facebook).<sup>29</sup>

Por fim, resta uma inferência sob uma perspectiva *humanista*. Percebe-se que, enquanto o componente humano estiver por trás de empresas com interesses privados e *por ventura* perversos, sempre haverá a possibilidade para alguém *vazar*, delatar e resistir às pressões de grandes corporações. Sempre haverá o potencial para o *civismo*, isto é, atitudes e ideias que fazem com que o indivíduo queira compartilhar certas noções e práticas como se fossem deveres fundamentais para a vida compartilhada da sociedade, para o bem da *coisa pública* e manutenção das instituições democráticas.

## 6 CONSIDERAÇÕES FINAIS

Em dezembro de 2019, menos de 360 dias dos resultados das eleições municipais no Brasil, percebe-se uma nova forma de acesso entre candidatos com reais chances ao Poder Público e seus respectivos eleitores: o (*ab*)uso em mídias e redes sociais e aplicativos, no ocidente (no Brasil), como o *WhatsApp*, de forma extremamente frequente com o único intuito: aproximar os possíveis eleitores da versão dos fatos, sejam eles *Fake News*, *Deep Fake*<sup>30</sup> ou não, sejam perfis falsos criados por *bots* (contas falsas criadas em massa) com o intuito de, em poucas horas, reproduzirem, como se fossem *cabos eleitorais virtuais*, uma espécie, ao contrário de a *vida imitar à arte*, de forma perversa e inconsequente.

Na primeira seção do texto buscou-se estudar, sob um forte viés cronológico dos fatos, o arco de ascensão e o fim da CA. Mediante depoimentos detalhados de Christopher Wylie e de Brittany Kaiser, ambos ex-funcionários da CA, concluiu-se que não era possível para o CEO da empresa, Alexander Nix, desconhecer as práticas invasivas que a empresa fazia. Tudo leva a crer que Nix sabia de todo o *modus operandi* da empresa; tanto é que, mesmo sabendo de sua única saída sem ter de enfrentar tempo encarcerado, Nix decretou a falência da empresa, fechando todos os arquivos pessoais da CA sem antes sacar a enorme quantia de 8 milhões de libras esterlinas dias antes da falência ter sido decretada.

Já na segunda seção do artigo buscou-se entender a forma como a CA atuava: tanto pelo emprego de disseminação de Fake News quanto pelas práticas de data mining, data scraping e big data analytics. A empresa conseguiu obter – sem o consentimento dos usuários da rede social Facebook – um volume de informações

<sup>28</sup> Por mais que empresas tomem diversas medidas e protocolos de segurança, inclusive com a incorporação de Inteligência Artificial para medir o comportamento de seus funcionários.

<sup>29</sup> Na internet não indexada, ou seja, na *deep web*, existe um porta de acesso à plataforma da rede social Facebook. Seja o Facebook verdadeiro ou apenas uma forma de indivíduos de índole extremamente duvidosa capturarem os nomes de usuários e suas senhas (uma prática imoral chamada de *phishing*), redirecionando-os em seguida ao Facebook verdadeiro, uma porta para o <Facebook.onion> realmente existe. É necessário o navegador Tor para acessar a página, porém aqui fica o alerta de acessar de um computador não seguro tal página.

<sup>30</sup> AFONSO, Nathália. #Verificamos: menina atirando em vídeo não é ativista sueca Greta Thunberg. Disponível em: <https://piaui.folha.uol.com.br/lupa/2019/12/11/verificamos-atirando-greta/>. Acesso em: 13 dez. 2019.

personais nunca antes obtido. Ademais, a empresa fez uso de propagandas no Facebook com a intenção artificial de polarizar questões raciais, como foi o caso da propaganda #BlackLivesMatter versus #AllLivesMatter. A CA atacava perfis de usuários mais vulneráveis, mais facilmente manipuláveis, com práticas de *microtargeting*, endereçando especificamente a eles notícias absurdamente falsas: Fake News.

A terceira seção do texto aborda o futuro pós-falência da CA. Apesar de formalmente não mais existir no mercado, é certo que a empresa impulsionou que uma série de outras empresas entrassem no ramo de *electioneering*, inclusive à título meramente exemplificativo a *Data Propria*. Também foi abordado que a CA já estava em negociações com a empresa Ponte Estratégia, no Brasil, para captar novos potenciais clientes. Bolsonaro não foi bem-visto pela CA naquela época, porém a utilização massificada de Fake News em aplicativos de mensagem com criptografia ponta a ponta, como o WhatsApp, foi algo surpreendente para a empresa com sede em Londres. André Torretta, responsável pela joint-venture CA-Ponte no Brasil, detalhou que partiu dele a ideia de utilizarem o WhatsApp como ferramenta eficiente para eleger o próximo candidato à presidência da República.

A quarta e última seção do texto aborda o dever cívico das pessoas que trabalhavam tanto em empresas privadas quanto em agências de inteligência no mundo. Em outras palavras, às vezes é necessário tomar medidas antipatriotas e nocivas aos ganhos de determinada empresa em privilégio da segurança dos dados pessoais das pessoas, assim como a proteção da manutenção da democracia em Estados soberanos. Nenhuma agência de inteligência, nem empresa privada, deve ter tanto poder para conseguir manipular os resultados de um determinado processo democrático, sob o risco de romper com a própria essência da Democracia.

Posto os presentes pontos, é inegável que a hipótese do presente artigo se confirma: a Cambridge Analytica, com sua *práxis*, deixou o mundo sem antes desestabilizar os processos democráticos em algumas das maiores potências mundiais; milhões de cidadãos tiveram a sua intimidade e privacidade coletada via mídia social a troco de elegerem o candidato que masi bem pagou a empresa. Basta recordar que, antes de Donald Trump contratar a CA, a empresa prestava consultoria nos EUA para Ted Cruz, seu adversário dentro do Partido Republicano. A operação continuada de Fake News, somada à práticas de *microtargeting* e coleta de dados via *data mining & scraping*, demonstrou a terrível essência do setor privado em querer minerar e gerar lucro de processos democráticos.

Dito isso, é necessário perceber que seria temerário afirmar que todos os problemas relacionados com as práticas da CA foram-se quando a empresa faliu. Hoje existem novas empresas, como a Data Propria, que operam de maneira similar para não dizer de forma mais sofisticada que antes. É necessário ter modéstia ao observar uma nova e crescente onda de empresas que veem em *electioneering* uma forma de lucrarem às custas de rupturas e danos irreparáveis aos processos democráticos. Foi a função deste artigo alertar, porém sem esgotar o tema, pois, na medida em que se entra na década de 2020 a 2030, novas práticas de coleta de dados, assim como de Fake News, irão se popularizar. É necessário ter olhar crítico para essas novas empresas que prometem, porventura por pseudociências, como *psychometrics*, que é possível alcançar-se a eleição de um candidato por um preço *x*. Práticas como *Deepfakes* estão apenas no início de serem desenvolvidas para esse fim e certamente até o final dessa década teremos novos casos sofisticados de Fake News capazes de enganar milhões de eleitores em potencial.

Infelizmente, para 2020 a combinação de i) uma escolha de Estado nas últimas décadas (para não se dedicar um capítulo historiográfico remontando às práticas em que a norma social proibia o *acesso à educação* desde antes do Brasil Império) pela falta de educação formal e cívica para a enorme parcela da população brasileira, somada a uma ii) sociedade atualmente polarizada entre uma extrema direita com indícios de fascismo e uma extrema esquerda reativa a ela, e, por fim, iii) a falta de diálogo, do debate de ideias e propostas para

um país melhor, com a tolerância com a pluralidade de opiniões e de cidadãos de diversos *brasis*: prevê-se não apenas o contínuo e eficaz *uso ilegal* de propagação em massa de notícias falsas, mas também a propagação de vídeos que possam até parecer realistas, porém são falsos: trata-se de vídeos *Deepfakes*.<sup>31</sup>

Cidadãos e Estado, contudo, são atores de seus próprios processos, e têm não apenas um direito de opinar e de expressar o desgosto com práticas nocivas à Democracia, porém se pode, em conjunto, mediante atuação simbiótica de troca de informações, estabelecer conexões com outros atores que mostrem a mesma indignação diante de mentiras perpetradas por determinadas campanhas eleitorais, com fantoches de interesses corporativos grandes. Somente dessa forma é possível evoluir em direção a um futuro democraticamente promissor, não apenas levando consigo todo o Legado do escândalo da *Cambridge Analytica*, mas estando prontos para o próximo escândalo.

## 7 REFERÊNCIAS

- AFONSO, N. *#Verificamos: menina atirando em vídeo não é ativista sueca Greta Thunberg*. Disponível em: <https://piaui.folha.uol.com.br/lupa/2019/12/11/verificamos-atirando-greta/>. Acesso em: 13 dez. 2019.
- BERGHEL, H. *Malice Domestic: The Cambridge Analytica Dystopia*. Nevada: University of Nevada, 2018.
- BROWNLEE, J. *GameStation EULA collects 7,500 souls from unsuspecting customers*. San Francisco: Geek.com, 2010. Disponível em: <https://www.geek.com/games/gamestation-eula-collects-7500-souls-from-unsuspecting-customers-1194091/>. Acesso em: 5 dez. 2019.
- CADWALLADR, C. *The great British Brexit robbery: how our democracy was hijacked*. Londres: The Guardian; The Observer, 2017. Disponível em: <https://www.theguardian.com/technology/2017/may/07/the-great-british-brexite-robbery-hijacked-democracy>. Acesso em: 30 nov. 2019.
- CAMERON, D. *AggregateIQ Created Cambridge Analytica's Election Software, and Here's the Proof*. Nova Iorque: Gizmodo Media Group, 2018. Disponível em: <https://gizmodo.com/aggregateiq-created-cambridge-analyticas-election-softw-1824026565>. Acesso em: 9 dez. 2019.
- CAMPOS, M. Cambridge Analytica, Microtargeting, and Power: "A Full-Service Propaganda Machine" in the Information Age. *Trail Six: Undergraduate Journal of Geography*, British Columbia, v. 13, 2018-2019.
- DAVIES, H. *Ted Cruz using firm that harvested data on millions of unwitting Facebook users*. Londres: The Guardian, 2015. Disponível em: <https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data>. Acesso em: 28 nov. 2019.
- EDWARDS, L. *Cambridge Analytica and the deeper malaise in the persuasion industry*. Londres: LSE Business Review, 2018.
- FARIVAR, C. *Data Propria, run by Cambridge Analytica alumni, working on Trump 2020 campaign*. São Francisco: Arstechnica, 2018. Disponível em: <https://arstechnica.com/tech-policy/2018/06/data-propria-run-by-cambridge-analytica-alumni-working-on-trump-2020-campaign/>. Acesso em: 9 dez. 2019.
- HEAWOOD, J. *Pseudo-public political speech: Democratic implications of the Cambridge Analytica scandal*. Londres: Impress, 2018.
- HORWITZ, J. *AP: Trump 2020 working with ex-Cambridge Analytica staffers*. Nova Iorque: The Associated Press, 2018. Disponível em: <https://apnews.com/96928216bdc341ada659447973a688e4>. Acesso em: 9 dez. 2019.
- GRASSEGGGER, H.; KROGERUS, M. *The Data That Turned the World Upside Down*. Nova Iorque: Vice, 2017. Disponível em: [https://www.vice.com/en\\_us/article/4x4x8n/the-data-that-turned-the-world-upside-down](https://www.vice.com/en_us/article/4x4x8n/the-data-that-turned-the-world-upside-down). Acesso em: 29 nov. 2019.
- KANTER, J. *Cambridge Analytica's CEO allegedly took \$8 million from the firm before its closure*. Nova Iorque: Business Insider, 2018. Disponível em: <https://www.businessinsider.com/alexander-nix-allegedly-took-8-million-cambridge-analytica-2018-6?r=UK>. Acesso em: 8 dez. 2019.
- KOZLOWSKA, I. *Facebook and Data Privacy in the Age of Cambridge Analytica*. Seattle: Henry M. Jackson School of International Studies; College of Arts and Sciences; University of Washington, 2019.
- PASSARINHO, N. *Ex-sócio da Cambridge Analytica no Brasil diz que empresa não tinha banco de dados de brasileiros*. Londres:

<sup>31</sup> Vídeos de *Deepfakes* podem ser considerados uma evolução tecnológica do *Fake News*. O objetivo é o mesmo: a disseminação de informações inverídicas com a intenção de prejudicar os demais candidatos em uma eleição democrática. De forma *simplista*, porém, pode-se afirmar que, enquanto o *Fake News* é estático, basta uma foto com letras garrafais e um *meme* agressivo; o vídeo de *deep fake* é dinâmico; trata-se de um vídeo que utiliza técnicas avançadas de edição de imagem e de geração de computação gráfica – às vezes com o auxílio de uma Inteligência Artificial para editar (juntar todos os *frames* ou quadros e sincronizar as camadas de áudio com os quadros do vídeo) – com o intuito de *emular, copiar e simular* não apenas o rosto de um adversário político à uma situação constrangedora, mas utilizar a fala dele de outros vídeos verídicos e descontextualizar o áudio, inserindo na edição final – em camadas de áudio secundárias – o vídeo de *deep fake* vídeo.

BBC Brasil. Disponível em: <https://www.bbc.com/portuguese/brasil-43481279>. Acesso em: 9 dez. 2019.

PLATÃO. *A República*: Livro VII: 514a–541b. *E-book* (296-298 p.) Disponível em: [https://www.netmundi.org/home/wp-content/uploads/2017/07/Platao\\_A\\_Republica.pdf](https://www.netmundi.org/home/wp-content/uploads/2017/07/Platao_A_Republica.pdf). Acesso em: 28 nov. 2019.

ROSSI, M.; MARREIRO, F. *O marqueteiro brasileiro que importou o método da campanha de Trump para usar em 2018*.

Madrid: El País – Brasil (parte do Grupo PRISA), 2017. Disponível em: [https://brasil.elpais.com/brasil/2017/10/11/politica/1507723607\\_646140.html](https://brasil.elpais.com/brasil/2017/10/11/politica/1507723607_646140.html). Acesso em: 9 dez. 2019.

VANHEMERT, K. *This Simple Data-Scraping Tool Could Change How Apps Are Made*. San Francisco: Wired, 2014. Disponível em: <https://www.wired.com/2014/03/kimono/>. Acesso em: 28 nov. 2019.