APOIO AO PROFESSOR

O QUE FOI FEITO DA MINHA PRIVACIDADE?

Inúmeras inovações tecnológicas surgem diariamente e passam a fazer parte da rotina dos indivíduos. Muitas delas possuem um grande potencial de coleta de informação individual sobre seus hábitos, os quais não são explicitamente evidenciados aos seus usuários

Por João Antonio de Moraes*

* João Antonio de Moraes é doutor em Filosofia pela Unicamp e professor do Departamento de Filosofia da Faculdade João Paulo II.

Já não é mais surpreendente a ligação entre as informações que uma pessoa insere em seu buscador com aquelas que aparecem em forma de propaganda em sua rede social, instantaneamente. A procura por um tênis de corrida faz com que surjam janelas indicando lojas que vendem determinado modelo, além de academias e lojas de suplementação esportiva próximas a sua localidade. Apenas uma informação inserida na rede e um perfil é atribuído àquele usuário.

Por um lado, ingenuamente, pode-se considerar que a realização dessa troca de informação pessoal promove uma otimização dos interesses do usuário (nesse caso, uma rapidez no acesso a locais de compra e promoções do objeto desejado). Por outro, destaca-se um dos objetivos principais de tal troca pelas instituições provedoras de internet, qual seja: o potencial econômico que esse tipo de dado pode gerar. Como diz Ronaldo Lemos (2018): "Dados são o novo petróleo, [...] funcionam como a engrenagem que move a economia digital". Na maioria dos casos os indivíduos não estão conscientes da realização de tal operação por parte das instituições, ocorrendo a invasão da privacidade dos mesmos.

INGENUAMENTE, PODE-SE CONSIDERAR QUE A TROCA DE INFORMAÇÃO PESSOAL PROMOVE UMA OTIMIZAÇÃO DOS INTERESSES DO USUÁRIO, COMO A RAPIDEZ NO ACESSO A PROMOÇÕES DO OBJETO DESEJADO. POR OUTRO, DESTACA-SE QUE HÁ UM INTERESSE PURAMENTE ECONÔMICO DAS GRANDES EMPRESAS

IMAGENS: SHUTTERSTOCK

O termo privacidade é entendido, pela literatura acadêmica, como a informação de conteúdo pessoal acessível apenas ao indivíduo sobre a qual ela diz respeito ou a quem ele/ela considere confiável[1]. Logo, para que a privacidade não incorra em um problema ético faz-se necessária a autorização do indivíduo para acesso àquele conteúdo específico; caso contrário, há invasão da privacidade. Tal invasão também se caracteriza como um problema pela privacidade ser um valor relacionado a duas expressões da vida humana: felicidade e liberdade. Conforme o ditado popular: "Você é quem realmente é quando ninguém está olhando". Quando o indivíduo desconfia que sua privacidade esteja em risco, ele deixa de agir espontaneamente, uma vez que pode estar sendo observado. Em outras palavras, em uma sociedade na qual se apresenta uma sensação de vigilância a ação livre e autônoma é colocada em xeque. Tecnologias de *Big Data* se destacam entre as que possuem um grande potencial de invasão da privacidade e têm colocado em risco os dados pessoais dos indivíduos.

BIG DATA

Tecnologias de *Big Data* possibilitam a análise de grandes quantidades de dados, de modo a identificar padrões e correlações informacionais a partir das quais se inferem possibilidades de ações futuras. Seu caráter de novidade está na reunião e processamento de informação acerca

[1] MORAES, 2018.

AS TECNOLOGIAS DE *BIG DATA* POSSIBILITAM A ANÁLISE DE GRANDES QUANTIDADES DE DADOS, DE MODO A IDENTIFICAR PADRÕES E CORRELAÇÕES INFORMACIONAIS A PARTIR DAS QUAIS SE INFEREM POSSIBILIDADES DE AÇÕES FUTURAS

de indivíduos gerando conexões até então desconhecidas, "criando novas formas de valor, alterando mercados, organizações e relações entre cidadãos e governos"[2].

O *Big Data* está presente no dia a dia dos indivíduos em situações como: filtros de *spam* – que identificam padrões de mensagens que correspondem ao lixo eletrônico do usuário; sites de relacionamento que analisam perfis compatíveis; e o corretor automático do celular que sugere o complemento das palavras a partir daquelas mais utilizadas pelos indivíduos. Nesses casos, o parâmetro que direciona tais análises é a inferência de ações futuras possíveis a partir da análise de uma grande quantidade de informação referente ao mesmo fenômeno no passado.

Observa-se, assim, o parâmetro central de "realizar previsões" nesse tipo de tecnologia, sendo essa a tarefa para a qual elas são construídas. O mesmo ocorre em casos de análise de publicações de redes sociais para a identificação de padrões de conduta individual: "Twitter, Linkedin e Facebook são 'gráficos sociais', mapas dos relacionamentos dos usuários para aprender [sobre] suas preferências"[3]. A reunião indevida desses gráficos sociais em 2016, a partir de testes realizados via Facebook, é o que foi recentemente denominado "caso Facebook/Cambridge Analytica".

O CASO FACEBOOK/ CAMBRIDGE ANALYTICA

Em fevereiro de 2018, Christopher Wylie, analista de dados da consultoria Cambridge Analytica, veio a público denunciar uma operação de coleta indevida de dados pessoais de usuários do Facebook, obtidos através de testes, e sobre o mau uso dos mesmos. Conforme explica Marcelo Pacheco (2018), a consultoria obteve acesso a dados pessoais de 50 milhões de usuários da rede social via realização de testes psicológicos. Embora 270 mil pessoas tenham realizado o teste, aceitando seus termos de uso – os quais envolviam acesso a informações como e-mails, amigos, páginas curtidas, entre outras relacionadas às suas preferências pessoais –, a consultoria teve acesso também aos dados pessoais da rede de amigos daqueles que fizeram o teste, dos quais não houve consentimento.

O caso se agrava em relação à invasão de privacidade, uma vez que os gráficos sociais gerados foram utilizados para traçar perfis de preferência política dos usuários. Tais preferências foram utilizadas em situações como o *Brexit* (a saída do Reino Unido da União Europeia) e as eleições americanas em 2016, nas quais Donald Trump foi vitorioso. Segundo Pacheco (2018), a campanha de Trump contratou os serviços da Cambridge Analytica para identificar os eleitores e direcionar os anúncios de campanha. Isso é possível, pois a linha do tempo de redes sociais como o Facebook segue um parâmetro chamado *filtro bolha*, o qual "seleciona as informações que considera úteis e importantes para cada usuário, conforme cada perfil [...]. Esse processo de filtragem faz com que uma mesma busca tenha resultados diferentes conforme quem a realiza"[4].

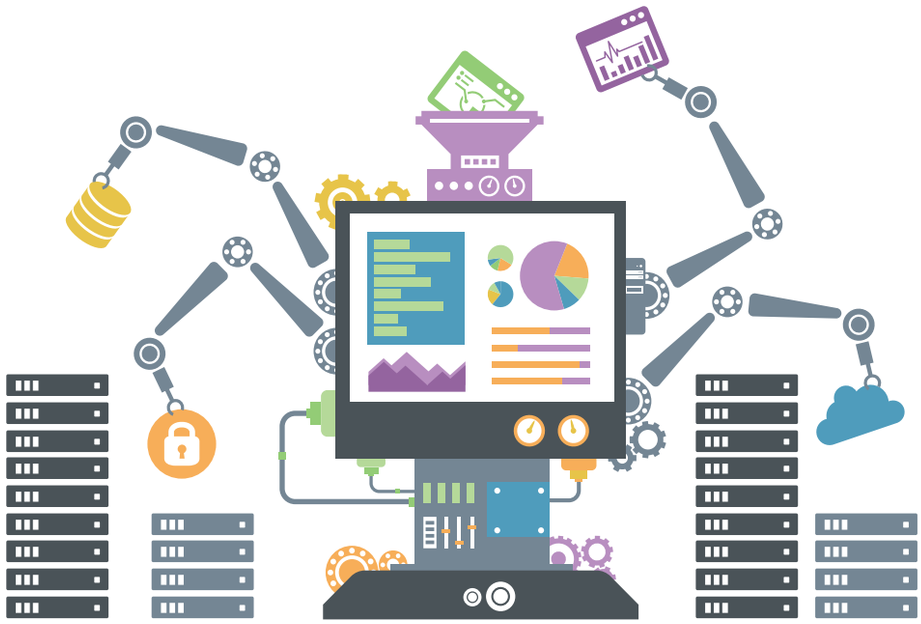
Em outras palavras, os indivíduos constituem suas concepções de mundo pautadas em informações que chegam a eles através de filtros controlados por parâmetros desenvolvidos por pessoas em defesa dos interesses específicos de suas empresas. A invasão de privacidade e

2 MAYER-SCHONBERGER; CUKIER, 2013, p. 6.
3 MAYER-SCHONBERGER; CUKIER, 2013, p. 16.
4 ASSANGE, 2015, p. 15.

tipificação dos indivíduos por *perfil* faz com que se constitua um cenário de pseudoliberdade, uma vez que suas crenças estão fundamentadas em informações controladas por terceiros. Conforme Felipe Santos (2017, p. 678): "Uma das primeiras consequências é que as bolhas informacionais levam as pessoas a crer erroneamente que aquelas informações disponíveis são de fato as únicas que fazem sentido".

Considerar que a prática da coleta de dados não constitui violação à privacidade dos indivíduos indica uma tentativa de fugir à responsabilidade por quem o faz. Conforme Gleen Greenwald (2015), um dos argumentos utilizados para indicar que não há uma violação à privacidade dos usuários na prática da coleta de dados é a consideração de que são coletados apenas *metadados* das atividades *on-line* dos mesmos. Ou seja, não há a coleta do *conteúdo* de tais atividades (i.e., a ação de ouvir as conversas telefônicas, ler os e-mails e revisar as atividades *on-line* dos indivíduos), mas ocorreria apenas o acúmulo de dados sobre as comunicações realizadas (e.g., um metadado sobre um e-mail diz acerca de destinatário e remetente, mas não sobre o conteúdo da mensagem). Porém, é possível ter acesso a um tipo refinado de informação pessoal dos indivíduos apenas a partir de metadados, como, por exemplo: revelar a identidade de alguém que utiliza serviço de relacionamento, ou uma linha de auxílio ao suicídio, ou mesmo o pertencimento a um grupo de resistência a um governo opressor. Destaca-se, ainda, que os metadados são mais eficazes em processos de vigilância e invasão de privacidade em relação ao conteúdo das mensagens, uma vez que são dados matemáticos e, por essa razão, podem ser facilmente analisados via ferramentas de *Big Data*.

O que ficou evidenciado com o caso do Facebook/Cambridge Analytica foi o alcance desse tipo de tecnologia de coleta de dados e o potencial de manipulação possível a partir da coleta de informação pessoal. Uma vez que não há consentimento para acesso à informação pessoal do indivíduo, há violação de sua privacidade e a garantia do desempenho de uma ação autônoma e livre. É justamente o termo *consentimento* o cerne da proposta de lei da União Europeia para promover a privacidade do usuário na rede.



IMAGENS: SHUTTERSTOCK

GRÁFICOS SOCIAIS SÃO UTILIZADOS PARA TRAÇAR PERFIS DE PREFERÊNCIA POLÍTICA. TAIS PREFERÊNCIAS FORAM UTILIZADAS EM SITUAÇÕES COMO O *BREXIT* (A SAÍDA DO REINO UNIDO DA UNIÃO EUROPEIA) E AS ELEIÇÕES AMERICANAS EM 2016, NA QUAL TRUMP FOI VITORIOSO

PRIVACIDADE E A LEI EUROPEIA

No dia 25 de maio de 2018 entrou em vigor na União Europeia a Lei de Regulamentação Geral de Proteção de Dados com o intuito de aprimorar os mecanismos que asseguram a privacidade dos usuários no ambiente *on-line*. Conforme explica Lemos (2018), essa é uma lei que se aplica a empresas relacionadas à internet que manipulam dados pessoais dos indivíduos.

Dentre outras diretrizes, exige-se que o usuário forneça o *consentimento* sobre qualquer dado pessoal que possa ser coletado. Para tanto, os *termos de uso* (raramente lidos pelos usuários – seja em função do excesso de termos técnicos, seja por sua extensão) devem ser apresentados de forma clara e transparente em relação aos possíveis usos das informações que são disponibilizadas pelos usuários. Outro aspecto é a possibilidade de interferir diretamente na dinâmica de suas próprias informações como, por exemplo, solicitar que as mesmas sejam apagadas dos provedores. No caso da violação dessa lei a instituição será multada.

A proposta da União Europeia constitui um caminho bastante

interessante para a proteção da privacidade dos usuários, *pelos usuários*. Ao se pautar, principalmente, na noção de consentimento, o usuário passa a ter um papel ativo, e consciente, na deliberação acerca do fornecimento de informação pessoal a empresas relacionadas à internet. Esse tipo de gerenciamento da privacidade parece, num primeiro momento, ser um passo positivo dado no caminho à proteção e controle das informações pessoais (preferências, hábitos, crenças) dos indivíduos. Por outro lado, cabe salientar que, aparentemente, a disputa em questão não se situa entre usuário e empresas ligadas à internet, mas entre elas e o Estado.

Em outras palavras, a partir da legislação proposta pretende-se gerenciar a atuação das empresas privadas em relação ao uso indevido das informações pessoais de seus usuários, com impacto na dinâmica global desse segmento, mas sem menção à vigilância realizada pelo Estado sobre a vida pessoal dos indivíduos, já mencionado por Edward Snowden em 2013. Snowden foi o responsável pela divulgação de documentos que comprovaram o caso de violação à privacidade realizada pela Agência de Segurança Nacional estadunidense (NSA) sobre dados confidenciais de indivíduos de todo o mundo, inclusive de chefes de Estado. Assim, cerceia-se a atuação das empresas em relação à prática de invasão da privacidade dos usuários – o que pode ser caracterizada como aspecto significativamente positivo, caso seja cumprido conforme proposto –, mas não se questiona acerca do mesmo tipo de ação desempenhada pelo Estado – um segundo passo a ser tomado em direção à preservação do direito à privacidade do indivíduo, conforme assegura o Art. 12 da Declaração Universal dos Direitos Humanos e o Art. 17 do Pacto Internacional dos Direitos Civis e Políticos.

CONTROLE TOTAL DOS DADOS É UTÓPICO?

Considerando que a internet atualmente pode ser entendida, quase que totalmente, como sinônimo de algumas empresas privadas, como Facebook e Google, por exemplo, e o que foge ao escopo delas possui vigilância do Estado, possuir total controle sobre os próprios dados é praticamente impossível. Fazer uso de artefatos de tecnologia digital consiste, de modo geral, na alimentação do ambiente *on-line* com informação pessoal.

Como evidenciado por situações como o escândalo do Facebook/Cambridge Analytica, e também da troca de dados pessoais dos usuários por empresas privadas com intuito puramente comercial, não é possível um controle total, ou mesmo de grande parte dos dados pessoais presente na rede, uma vez que para isso seria necessário um conhecimento técnico mais bem desenvolvido de ferramentas que possibilitam tal proteção (e.g., criptografia).

O cenário atual parece não ser o mais favorável em direção a esse controle, por parte dos usuários, dada a *divisão digital* existente, a qual ilustra justamente a lacuna presente entre aqueles que possuem, ou não, acesso a tecnologias digitais, uma estrutura adequada para utilização de tais tecnologias, ou ainda conhecimento aprimorado no uso das mesmas. Em outras palavras, a constituição de uma sociedade na qual os indivíduos tenham controle total sobre seus dados pessoais parece bastante distante. Uma alternativa ainda embrionária é a proliferação

O QUE FICOU EVIDENCIADO COM O CASO DO FACEBOOK/CAMBRIDGE ANALYTICA FOI O ALCANCE DESSE TIPO DE TECNOLOGIA DE COLETA DE DADOS E O POTENCIAL DE MANIPULAÇÃO POSSÍVEL A PARTIR DA COLETA DE INFORMAÇÃO PESSOAL

IMAGENS: SHUTTERSTOCK

É NECESSÁRIO O DESENVOLVIMENTO DE UM PENSAMENTO CRÍTICO ACERCA DO USO DAS TECNOLOGIAS DIGITAIS COM CRIANÇAS E ADOLESCENTES, PROMOVENDO UMA EDUCAÇÃO DIGITAL

de cursos de programação a crianças e adolescentes, além do desenvolvimento de um pensamento crítico acerca do uso das tecnologias digitais com esse mesmo público-alvo, promovendo uma educação digital. Enquanto isso não se concretiza, a organização social segue refém das tecnologias digitais e da forte influência das empresas privadas e do Estado em sua dinâmica, indicando uma proximidade maior com aquela sociedade descrita por George Orwell em seu livro *1984*.

Convém destacar, numa perspectiva não tão pessimista, que enquanto a sociedade não alcançar seu estágio de total transparência haverá espaço para a privacidade individual. No entanto, esse estágio se apresenta como um dos interesses do Estado, uma vez que a privacidade possuiria um caráter negativo por contrastar com o interesse pela vigilância, controle e, portanto, poder. O argumento utilizado pelo Estado para promoção de tal estágio de transparência é a manutenção da segurança pública, evidenciada pelas medidas de vigilância adotadas pelo governo americano em suas políticas antiterroristas após o ataque de 11 de setembro de 2005.

Outra tentativa atual de promoção da transparência dos dados pessoais dos indivíduos é a criação do *Sistema Social de Crédito* na China, que visa classificar seus usuários por *grau de confiança*. A atribuição desse grau é realizada por meio da combinação de dados pessoais como: histórico financeiro, telefônico e residencial, além de dados sobre comportamentos, preferências e relações pessoais. Um agravante para garantia da privacidade dos indivíduos, nesse contexto, é a disponibilização pública da nota atribuída aos cidadãos, o que pode vir a influenciar situações como: acesso a emprego, contratação de plano de saúde, entre outras aos menos ranqueadas.

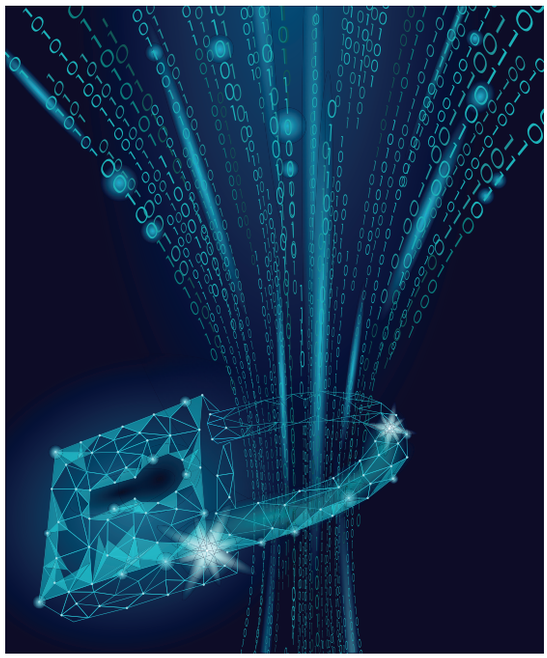
A SOCIEDADE DA INFORMAÇÃO E A "NOVA" NOÇÃO DE PRIVACIDADE

Desde a popularização da internet e, também, dos artefatos tecnológicos por meio dos quais é possível participar da vida *on-line*, iniciou-se uma revolução na organização social. Atualmente presenciamos a quase impossibilidade de se viver em sociedade urbana sem que se faça necessário algum tipo de mediação das tecnologias digitais em atividades diárias. Exemplos de utilização direta de tais tecnologias são: movimentação financeira, aquisição de produtos e serviços, inter-relacionamento pessoal e profissional (Facebook, Tinder), acesso a filmes (YouTube, Netflix), mobilidade urbana (Uber), realização de ligações (Skype, WhatsApp), entre outras[5].

As tecnologias digitais deixaram de ser meras ferramentas para o indivíduo, passando a constituir uma relação de dependência entre eles. Tal dependência fica mais evidente quando considerada a relação dos indivíduos da Geração Z (nascidos em torno de 1996) com tais tecnologias: seu aprendizado escolar envolve lousas digitais e *smartphones*, seu tempo de lazer é desfrutado com jogos *on-line*, suas relações pessoais são criadas através de aplicativos. Diferente da Geração Y, que presenciou a transformação do ambiente analógico para o digital, a Geração Z atua nele com naturalidade e sem qualquer estranheza. É nesse contexto, constituído a partir de uma gama de novas possibilidades de ação, que o conceito de privacidade é ressignificado. Isso, no sentido de estar se alterando aquilo que se considera digno de proteção. Uma ilustração dessa alteração é a relação dos jovens com a nudez.

5 MORAES, 2018.

NESSE CONTEXTO, FAZ-SE RELEVANTE A ANÁLISE CONTÍNUA ACERCA DOS ELEMENTOS QUE CONSTITUEM AS FRONTEIRAS ENTRE PÚBLICO/PRIVADO, DADO QUE DEFENDER A PRIVACIDADE DO INDIVÍDUO É DEFENDER SUA LIBERDADE



Uma pesquisa realizada em 2017 indicou que para os jovens o compartilhamento de fotos íntimas, respeitando algumas regras, não constitui uma violação as suas privacidades[6]. Nesse sentido, como diz a pesquisa, a nudez, que antes era vista como um tabu, passa a ser concebida com naturalidade, como uma ferramenta de flerte. A influência da internet na vida cotidiana dos indivíduos fez da privacidade um conceito não singular, alterando as fronteiras entre público/privado, tornando o ambiente virtual um espaço semipúblico[7]. Pode-se considerar, ainda, a privacidade *informacional* como um conceito complexo, definido como informação pessoal sobre um indivíduo (ou grupo) que pode ser acessível, a critério do indivíduo (ou grupo), a alguém que ele considera digno de ser respeitado e protegido; logo, podendo ser ampliado ou restrito conforme o contexto em que se situam[8].

Em síntese, a noção de privacidade é afetada pela internet e pelas tecnologias digitais, porque os indivíduos também são afetados por elas. Uma vez que o que é considerado privado é definido pela relação entre indivíduos e grupos, então: se a maneira como os indivíduos interagem com o mundo muda, então a noção de privacidade também se altera. Nesse contexto, faz-se relevante a análise contínua acerca dos elementos que constituem as fronteiras entre público/privado, dado que defender a privacidade do indivíduo é defender sua liberdade. Como indicado, quando se está sob vigilância, a espontaneidade da ação tende a diminuir, especialmente se tal vigilância é realizada por uma autoridade superior. Logo, a privacidade se identifica como um valor ético caro à dinâmica da sociedade contemporânea. filo

[6] FREITAS, 2017.

[7] MARWICK, A.; MURGIA-DIAZ, D.; PALFREY, J., 2010.

[8] MORAES; GONZALEZ (no prelo).

Em 2014 foi aprovada a Lei nº 12.965/14, conhecida por Marco Civil da Internet, a qual estabelece diretrizes para regular o uso da internet no Brasil, seja para os direitos e deveres de usuários e empresas, como para a atuação do Estado. No escopo do Marco Civil, os Artigos 10º ao 13º destinam-se ao tópico da privacidade. Por meio deles, assegura-se que um provedor de internet não pode violar o direito à intimidade dos usuários, sendo que tal monitoração pode ser realizada apenas sob ordem judicial. O Artigo 7º, por sua vez, declara que a coleta de dados pode ser realizada por instituições apenas mediante clareza no uso e consentimento expresso do usuário (Fonte: http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2014/Lei/L12965.htm).

REFERÊNCIAS

ASSANGE, J. **WikiLeaks:** quando o Google encontrou o WikiLeaks. São Paulo: Boitempo, 2015.

FREITAS, B. Sexo ideal? **TAB-Uol**, s/d. Disponível em: <https://tab.uol.com.br/sexo-internet/>. Acesso em: 8 nov. 2017.

GREENWALD, G. **No place to hide:** Edward Snowden, the NSA & the surveillance state. Penguim Books, 2015.

LEMOS, R. Na briga de dados, Europa quer garantir privacidade dos cidadãos. **Folha,** 19/3/18.

MARWICK, A.; MURGIA-DIAZ, D.; PALFREY, J. Youth, privacy and reputation. In: **Harvard Law Working Paper**, v. 5, p. 10-29, 2010.

MAYER-SCHÖNBERGER, V.; CUKIER, K. **Big Data:** a revolution that will transform how we live, work and think. Londres: John Murray, 2013.

MORAES, J. A. **O paradigma da complexidade e a ética informacional**. Tese (Doutorado em Filosofia) – IFCH, Unicamp, Campinas, 2018.

MORAES, J. A.; GONZALEZ, M. E. Q. Complexity and informational privacy: a study in the systemic perspective. In: PEREIRA JR., A.; PICKERING, W.; GUDWIN, R. R. (Org.). **Self-Organization:** Interdisciplinary Studies. New York: Routledge (no prelo).

PACHECO, M. Facebook, Cambridge Analytica e mineração de dados: o que você precisa saber. **Estadão,** 21/3/18.

SANTOS, F. R. L. Vícios intelectuais e as redes sociais: o acesso constante à informação nos torna intelectualmente viciosos? In: **Veritas**, v. 62, n. 3, set-dez, p. 657-682, Porto Alegre, 2017.

IMAGENS: SHUTTERSTOCK