ANÁLISE SOBRE A PRIVACIDADE DE DADOS PESSOAIS

ANALYSIS ON PRIVACY OF PERSONAL DATA

GUEDES, Catharine da Silva de Oliveira.[1]

Grupo Temático 4.
Subgrupo 4.2.

Resumo:
O presente artigo realizou uma análise sobre a questão da privacidade de dados pessoais. Buscou-se compreender as estruturas sociais e econômicas que propiciaram a atual exposição exacerbada dos dados pessoais no meio digital, e, em seguida, evidenciar alguns acontecimentos e práticas danosas, ocasionados por algumas empresas, decorrentes de seus usos. A elaboração ocorreu através da revisão de literatura, com base principal em Silveira (2017) e Zuboff (2018), entre outros autores. Os resultados indicam uma frequente falta de proteção na frágil privacidade dos usuários, a qual está sendo alvo de ataques diretos e indiretos, em razão do lucro e aumento do controle social. A partir desta perspectiva, a proteção da privacidade de dados pessoais se apresenta como uma questão importante de ser mais bem observada e discutida, sobretudo, perante a sociedade civil.
***Palavras-chave**: Privacidade de dados pessoais. Violação da privacidade. Proteção de dados.*

Abstract:
This article analyzes the privacy issues of personal data. We sought to understand the social and economic structures that provided the current exacerbated exposure of personal data in the digital environment, and then highlight some events and harmful practice, caused by some companies, resulting from their uses. The elaboration occurred through the literature review, based mainly by Silveira (2017) and Zuboff (2018), among other authors. The results indicate a frequent lack of protection in the fragile privacy of users, which is the target of direct and indirect attacks, due to profit and increased social control. Steam from this perspective, the protection of the privacy of personal data presents itself as an important issue to be better observed and discussed, above all, before civil society.
***Keywords**: Personal data privacy. Violation of privacy. Data protection.*

1. Introdução

Através da pesquisa bibliográfica, este trabalho se propôs a analisar as estruturas da sociedade informacional que propiciaram o surgimento de uma economia informacional, fundamentadas nas tecnologias digitais, de modo que fosse possível compreender os meios pelos quais acontecem a extração e tratamento de dados da sociedade no meio digital.

[1] Graduanda de Licenciatura em Pedagogia no Instituto Superior do Rio de Janeiro ISERJ e participante do Grupo de Pesquisa Identidade(s) e Saberes Docentes (GPIDOC/ISERJ/CNPq).

Levanta-se aqui a questão sobre a privacidade de dados pessoais, devido aos recentes acontecimentos envolvidos com a violação da temática citada que influenciam direta e indiretamente o comportamento social de forma negativa, criando ainda uma vigilância constante sobre as ações da população.

2. Sociedade informacional

Estamos cada vez mais imersos no mundo digital, fazendo pesquisas em sites de busca, interagindo com outras pessoas pelas redes sociais, realizando compras on-line, preenchendo dados cadastrais em diversas plataformas e etc.

Acontece que toda essa atividade gera dados informacionais pessoais que estão sendo extraídos constantemente dos meios por onde interagimos. Os mesmos dados que recebem enorme atenção de grandes conglomerados empresariais. Em contrapartida, os usuários são levados a crer na completa normalidade desta exposição, pois aceitando isso, ajudam a melhorar o desempenho dos dispositivos e recursos acessados. Isto não é mentira, entretanto existem perigos nessa normalização da quebra da privacidade, refletidos direta e indiretamente em nossas vidas.

> A coleta e análise sistemática de dados praticada pelas empresas não apenas melhora experiências, mas pode também criar exclusões e custos socialmente inaceitáveis. Quando um plano de saúde rejeita uma pessoa ou cobra o dobro da mensalidade por saber que ela tem uma propensão genética a determinadas doenças, começamos a nos preocupar com o que os dados coletados sobre nós podem gerar. (SILVEIRA, 2017, n.p.).

Antes de adentramos mais nesse assunto é importante entender as estruturas que a formam. Surgidas posteriormente às sociedades industriais, as sociedades informacionais, cunhadas por Castells (2000 apud WERTHEIN, 2000, p. 2), se referem ao crescimento e reorganização do capitalismo desde os anos 80. Nela a economia passa a ser fundamentada em tecnologias que tratam a informação como seu produto principal, e os valores gerados por ela não se baseia em bens materiais como acontecia anteriormente, mas sim em bens imateriais, os quais podem ser transferidos pelas redes digitais.

A essência dessa sociedade está nas tecnologias da informação, as quais firmam suas características fundamentais em: informação como matéria prima, efeitos de alta penetrabilidade, uso da lógica das redes, flexibilidade e a convergência de tecnologias (CASTELLS, 2000 apud WERTHEIN, 2000, p. 2).

Também é possível afirmar que as tecnologias cibernéticas - de comunicação e controle - serviram de estrutura para essas sociedades (SILVEIRA, 2017, n.p.). O diferencial marcante delas, quando as comparamos com tecnologias do modelo industrial, se evidencia na constante produção de informações (SILVEIRA, 2017, n.p.). As que se referem ao modelo industrial não retêm informações quando utilizadas, como ao escrever em uma máquina de

datilografia, ao contrário das tecnologias cibernéticas que além de suas funções registram toda a atividade e momentos realizados, como o histórico de pesquisa em um computador.

Aqui vários processos de trabalho passaram a ser rapidamente "atualizados", substituindo pessoas por máquinas, inteligência artificial (IA) - como no caso das correções de trabalhos realizadas por robôs (DOMENICI, 2020) - e softwares. Esse último recurso aparece em vários espaços, como o celular, sistemas de escolas, empresas e possui uma função muito importante dentro das sociedades informacionais, como aponta Lev Manovich (2008 apud SILVEIRA, 2017, n.p.) "Se a eletricidade e o motor de combustão tornaram a sociedade industrial possível, o software também possibilita a [existência da] sociedade da informação".

Tanto os softwares, quanto IA, computadores e redes digitais são tecnologias cibernéticas. Entretanto, segundo Silveira (2017) nem toda tecnologia eletrônica é cibernética, pois para ser configurada como tal precisaria comunicar e controlar simultaneamente. Nas máquinas a base das comunicações é semelhante a um diálogo, um computador envia uma mensagem carregando informações, compartilhando o mesmo "protocolo de comunicação" onde uma "interligação é estabelecida" (WIENER, 1968 apud SILVEIRA, 2017, n.p.). Portanto, todas as informações que passam por ele são controladas.

> Assim, o envio de informações quase sempre é acompanhado de seu registro. Dados são comunicados gerando dados sobre a comunicação efetuada, ou seja, metadados são constantemente criados. Os registros do que é feito têm como base esses processos de comunicação e controle. Assim, a comunicação em rede produz rastros digitais. (SILVEIRA, 2017 n.p.)

Dessa forma, a vigilância é constante sobre os dados pessoais e os limites de privacidade vão sumindo. Não é difícil perceber essa invasão nos aparelhos celulares, em aplicativos que necessitam de permissões de acesso às nossas câmeras, microfones, contatos, fotos e etc., para funcionar e em alguns casos essa permissões são desnecessárias para exercer a sua função.

3. Economia informacional

Ao passo que diversas tecnologias digitais produzem informações cada vez que são utilizadas, uma emergente economia informacional, se aproveita então desses mesmos dados para avaliar suas práticas e negócios. Visando a reprodução do seu capital, os agentes econômicos recebem "os dados sobre como o produto foi consumido, o horário exato da compra e os metadados da transação chegam antes ou junto com o dinheiro resultante do processo de circulação" Silveira (2017, n.p.).

Para tirar melhor proveito desse cenário, a economia informacional faz surgir o capitalismo de informação ou de vigilância, como sugere Zuboff (2018, pg. 25), o qual "procura prever e modificar o comportamento humano como meio de produzir receitas e controle de mercado".

Mesmo aqueles que nunca acessaram uma tecnologia cibernética não estão livres de ter seus dados armazenados. Ter realizado algum registro oficial, através de terceiros, por um computador, já garante a entrada nesse sistema de dados.

Visando expandir a utilização da análise dos dados as empresas investem no *big data*: tecnologias que tratam grandes quantidades de dados que não podem ser analisados com ferramentas tradicionais. Elas podem "cruzar informações de bancos de dados diferentes e realizar previsões capazes de extrapolar as simples facilidades oferecidas pelo mercado" (SILVEIRA, 2017, n.p.).

De acordo com o Relatório do Fórum Econômico Mundial (2011 apud SILVEIRA, 2017, n.p.) os dados pessoais podem ser definidos como "as informações e metainformações criadas por e sobre as pessoas" incluindo dados oferecidos voluntariamente, observados ou inferidos. Uma vez que a economia informacional realiza a extração e análise deles, o mercado de dados abre a possibilidade da formação de um campo de estudos denominado "microeconomia da interceptação de dados pessoais" (SILVEIRA, 2017, n.p.).

Nesta microeconomia o *big data* pode ser compreendido através de camadas. Na primeira camada, "coleta e armazenamento de dados", esta extração pode ocorrer de quatro fontes distintas:

> Derivados de transações econômicas medidas por computadores. [...] Sensores incorporados em uma ampla gama de objetos, corpos e lugares. [...] Banco de dados governamentais e corporativos. [...] Uma quarta fonte de *big data*, que fala do seu caráter heterogêneo e transemiótico, flui de câmeras de vigilância públicas e privadas. (ZUBOFF, 2018, p. 27-28).

Da mesma forma que as tecnologias cibernéticas registram e armazenam suas interações, essas informações recebem o mesmo procedimento e, por meio de acordos, empresas próprias ou parceiras as direcionam para grandes bancos de dados (SILVEIRA, 2017, n.p.).

Após ocorre o "processamento e mineração de dados", que trata e agrega essas informações, ligando-os a outros bancos de dados provenientes de outras fontes, visando a criação de um perfil mais detalhado (idem).

Na camada de "análise e de formação de amostras", as empresas e departamentos de marketing organizam "a venda dos chamados públicos segmentados e até mesmo das audiências semelhantes (*lookalikes*)" (idem).

Por último o processo retoma ao consumidor, oferecendo a ele serviços, produtos e ofertas criadas a partir desse tratamento dos dados, a chamada camada de "modulação" (idem). A Netflix e o Spotify, por exemplo, analisam os gêneros de mídia preferidos dos seus clientes e retornam com sugestões parecidas. Também estão incluídos os algoritmos que resultam nas bolhas e controle de visualização.

Os algoritmos estão recebendo especial atenção por algumas pesquisas pelo fato de controlarem nossos acessos e delimitarem nossas ações. Doneda e Almeida (2018, p. 141) os

definem como “um conjunto de instruções para realizar uma tarefa, produzindo um resultado final a partir de algum ponto de partida".

Por mais bem intencionados que possam dizer ser os algoritmos nos trazem alguns riscos como manipulação, criação de filtros bolha (os quais diminuem as possibilidades de autocrítica e diálogos construtivos), abuso do poder de mercado, risco à democracia, entre outros (DONEDA e ALMEIDA 2018). Por esses motivos os autores citados anteriormente argumentam a necessidade de um "processo de governança para os algoritmos". Seu objetivo deve buscar reduzir os problemas e resultados indesejáveis causados pelos algoritmos, tentando preservar sua eficácia, responsabilizando os produtores, evidenciando suas intenções e garantindo sua eficácia (DONEDA e ALMEIDA 2018, p. 145).

Ainda a respeito do *big data*, as duas maiores corporações que a utilizam são o Google e o Facebook, as gigantes no topo de acesso na internet e por não cobrarem - a maioria - de seus serviços, a publicidade se torna sua maior fonte de renda. De acordo com Liem e Petropoulos (2016 apud SILVEIRA, 2017, n.p) nos anos de “2014, 2013 e 2012, a publicidade representou 92%, 89% e 84%, respectivamente, das receitas do Facebook” e “mais de 90% da receita total do Google na última década”.

Assim a dependência econômica dessas grandes empresas está fortemente baseada a compra e venda de dados pessoais direcionados as empresas e outros clientes do mesmo nicho que se beneficiam das informações de seus clientes para o anúncio direcionado de seus produtos.

Na distribuição desses anúncios são utilizadas as empresas de *tracking*. Todos os rastros digitais e comportamento que os usuários deixam durante o uso da internet são armazenados por essas empresas através dos cookies de internet (SILVEIRA, 2017). Ao acessar um site um pequeno pacote de dados é enviado para o navegador, ou seja, o meio de acesso, do usuário. Alguns sites perguntam se os cookies podem ser aceitos, outros apenas informam que eles serão deixados e outros chegam a impor seu aceite para o acesso. Quando o usuário retorna ao site o navegador retorna o cookie à página, armazenando, automaticamente, o histórico de navegação da pessoa em questão (SILVEIRA, 2017). É por meio dessas informações que as publicidades que aparecem para os usuários durante a sua navegação online são específicas aos seus interesses.

4. Divergências e violações da privacidade de dados pessoais

As empresas participantes dessa economia defendem o fim da privacidade, alegando poder oferecer em troca melhores serviços e também maior segurança contra criminosos, que poderiam com isso, ser mais facilmente detectados pelos setores de segurança (SILVEIRA, 2017). Entretanto, os mesmos dizem necessitar de mais opacidade e privacidade nas suas operações, pois correm o risco de terem seus programas plagiados e ideias roubadas pela concorrência (SILVEIRA, 2017). Contudo, se para eles a privacidade é necessária, para nós ela também deveria ser defendida, uma vez que essa vigilância e controle excessivo em nossos dados começam a causar problemas, devendo ser mais bem acompanhada.

O Marco Civil da Internet, lei nº 12.965, aprovado em 2014, estabeleceu os "princípios, garantias, direitos e deveres para o uso da internet no Brasil", um importante passo legal na proteção dos dados pessoais. No artigo 7º é assegurado ao usuário o conhecimento e consentimento sobre ações realizadas com seus dados, que só poderão ser utilizados para determinados fins. E ainda a exclusão completa dos dados fornecidos pelo usuário, caso assim deseje. Contudo, na prática, isto não está sendo efetivado, de acordo com as observações de Silveira (2016) as atividades de *tracking* estão desrespeitando a referida lei. Sendo assim, "a regulamentação da lei deveria colocar parâmetros para garantir que o destaque seja efetivamente realizado pelos provedores de aplicação" (SILVEIRA, 2016, p. 23).

Na mesma lei, a neutralidade de rede estabelece que "o responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação" (BRASIL, 2014. Art.9).

Esta sessão visava impedir que o setor de telecomunicações transformasse o acesso à internet como ocorre com os planos televisivos, vendidos através de pacotes que se tornam mais caros à medida que determinados canais são agregados (SILVEIRA, 2017). A ideia era justamente controlar o volume de *bits* que passam pelos seus cabos de fibra óptica, para vender a internet através pacotes de acesso, nos quais conforme mais mídia fosse necessária, como nos vídeos, mais caros seriam os pacotes (SILVEIRA, 2017).

A lei citada impediu essa estratégia, contudo o Facebook, visando aumentar a utilização da sua plataforma para aumentar o volume de dados gerados, idealizou o *zero rating* ou franquia zero (SILVEIRA, 2017).

> A prática do *zero rating*, por seu turno, consiste em estratégias comerciais adotadas por provedores de internet de acesso móvel, os quais, após a celebração de acordos com outros fornecedores, conferem gratuidade no tráfego de dados de determinado serviço ou aplicação. (ERHARDT, 2016, p. 344-345).

Dentre as operadoras de telefonia móvel com mais amplitude no país, praticantes do *zero rating* estão a Claro S/A e a TIM S/A. Nelas já é possível assinar planos que disponibilizam acesso ilimitado não apenas para o Facebook, mas também para o *Whatsapp* nos mais baratos. Também para *Instagram, Waze, Twitter* e outros nos mais caros.

Apesar de ser uma ótima oferta, a franquia zero gera contradições quanto à neutralidade da internet. Além disso, Silveira (2017) alerta:

> Caso o zero rating venha a se consolidar, teremos um crescimento ainda maior do mercado de dados pessoais e da economia da intrusão, pois a conexão gratuita será paga com a venda de perfis de navegação, acesso e comportamento online das pessoas e seus dispositivos. (SILVEIRA, 2017, n.p.).

Além disso, essa prática reforça o engano e desinformação propiciada pelas *Fake News*. Como os planos de telefonia mais baratos disponibilizam gratuidade de acesso aos aplicativos sociais, a informação pode estar sendo recebida em sua maior parte de parentes, amigos e conhecidos e sem poder consultar a confiabilidade da informação em outras fontes, pois para isso o custo é maior, as chances de se enganar e disseminar uma notícia falsa são maiores.

> No Brasil, os usuários de baixa renda são aqueles que usam principalmente planos pré-pagos que incluem ZR. Esses usuários recebem e divulgam informações essencialmente participando de grupos do WhatsApp e através do Facebook, que estão entre os poucos aplicativos patrocinados. (BELLI, 2019, p. 179).

Considerando que os aplicativos citados são os meios mais utilizados para a propagação de *Fake News*, a opinião pública se torna um alvo mais fácil de manipular e, por conseguinte contribuir para abalar princípios democráticos.

A mercantilização dos dados não se limita a publicidade. O título do livro "Tudo sobre tod@s: redes digitais, privacidade e venda de dados pessoais" de Silveira (2017) faz referência ao polêmico site "Tudo sobre todos", surgido em 2015. Nele era oferecido o serviço de venda de dados de qualquer brasileiro, como CPF, idade, parentesco e etc. O Ministério Público Federal logo entrou com uma investigação que resultou na retirada do site. Para se ter uma ideia do tamanho do infração, Vitor Guglinski (2015) informa que mesmo o Estado detenha nossos dados pessoais não é permitido a ele fornecer as informações à outros com interesses particulares.

Outro fim que a utilização indevida dos nossos dados pode acometer foi demonstrado no escândalo da *Cambridge Analytica* (C.A). A empresa de *marketing* digital, que realiza a análise de dados, foi contratada em 2016 para a campanha eleitoral de Donald Trump e apoiadores do Brexit.

A empresa realizou inicialmente a coleta das informações por um aplicativo de personalidade, no qual o participante precisava dar a permissão, nos termos de uso, do acesso aos seus dados e a de seus amigos como condição de uso e justificativa de utilização em uma pesquisa acadêmica (BBC, 2018). Com um alcance de 50 milhões de americanos, segundo a imprensa americana, os resultados foram na verdade vendidos à empresa, ação que fere as políticas de privacidade (BBC, 2018).

A partir do material comprado, a empresa pode traçar o perfil de cada usuário e direcionar mensagens polêmicas e até falsas dos opositores dos seus contratados e influenciar o voto em outros, acusações feitas por Christopher Wylie, o ex-diretor de tecnologia da *Cambridge Analytica,* que denunciou os atos à imprensa (BBC, 2018).

> "Ao coletar dados das pessoas e categorizar o perfil delas, isso te permite segmentar a população, para direcionar mensagens sobre questões que interessam (a cada grupo), usando linguagem e imagens que as possam gerar engajamento. Fazemos isso na Ásia,

> nos Estados Unidos...", explicou Alex Tyler, gerente de dados da Cambridge Analytica, a um repórter do Channel 4, emissora britânica, que se fez passar por um potencial cliente. [...] "Nós fizemos isso no México, na Malásia, e agora estamos indo para o Brasil", completou o diretor de gestão da consultoria, Mark Turnbull. (BBC, 2018).

A empresa ainda chegou a negar todas as acusações de violação de dados, mas perdeu toda a credibilidade registrando pedido de falência em 2018. Nesse envolvimento o Facebook perdeu ações, foi alvo de investigações e recebeu uma multa de 5 bilhões de reais pela Comissão Federal de Comércio dos Estados Unidos (EL PAÍS, 2019).

Uma matéria do The New York Times a jornalista Lori Andrews (2012) relata ainda que essa prática de análise dos nossos “rastros” cibernéticos pode ser fator de discriminação social ao negar oportunidades às pessoas baseando-se no seu histórico na internet, termo conhecido como Weblining, assim o limite de um cartão de crédito pode ser maior ou menor pela sua etnia, sexo e pesquisas online.

A Lei Geral de Proteção de Dados – Lei 13.709, também identificada como LGPD, foi sancionada no Brasil em 2018. Segundo Doneda e Mendes (2019, p. 312) são identificados cinco eixos principais dessa lei em razão dos quais a proteção de dados pessoais se apresenta, sendo eles: “i) unidade e generalidade da aplicação da Lei; ii) legitimação para o tratamento de dados (hipóteses autorizativas); iii) princípios e direitos do titular; iv) obrigações dos agentes de tratamento de dados; v) responsabilização dos agentes".

Apesar de ser uma lei fundamental para a regulamentação e garantia de proteção da privacidade de dados pessoais, o veto dos artigos 55 a 59, que abordavam a criação de uma Autoridade Nacional de Proteção de Dados e de um Conselho de Proteção de Dados, dificulta a sua aplicabilidade (DONEDO; MENDES, 2019). Presente em diversos países esse agente demandaria funções como fiscalizar, regulamentar, analisar possíveis violações e orientar a sociedade perante a aplicação da lei. Sem a sua atuação a LGPD fica sem um importante pilar de sustentação e impossibilitada de alcançar seu objetivo (DONEDA; MENDES, 2019).

Para, além disso, a demora na criação e sanção da LGPD deve ser um fator a ser observado. As tecnologias digitais se modificam e se atualizam em uma velocidade superior dos modos de promoção de leis brasileiras. Enquanto dão aprovação a um projeto normativo existe a possibilidade do mesmo não abranger todas as atuações das inovações tecnológicas.

Através dessas discussões podemos começar a reconsiderar os discursos de normalidade na exposição da nossa privacidade, a compreender que ter mais cuidados e atenção nas permissões dadas é necessário e que as gratuidades oferecidas pelos aplicativos, benefícios de promoções e maior facilidade de acesso a plataformas on-line é paga com dados pessoais. Ainda que não seja possível estar a salvo desta exposição, pois os usos da tecnologia cibernética tendem a alcançar mais setores e acaba criando uma dependência nos usuários, essa questão precisa ser apresentada e divulgação perante a sociedade, a qual é o alvo principal. Zuboff apresenta um estudo relativo a essa defesa:

> Um grupo de pesquisadores por trás de um grande estudo do comportamento *online* entre jovens concluiu que a "falta de conhecimento" - e não uma "atitude espontânea em relação privacidade", como alegaram os líderes das empresas de tecnologia - é uma razão importante pela qual um grande número de jovens "se envolve com o mundo digital de maneira aparentemente despreocupada". (ZUBOFF, 2018, p. 53).

Sem nenhum conhecimento ou aprofundamento sobre este assunto, não existe possibilidade de reflexão e a oportunidade deve ser oferecida também no sistema educacional. Discutir, estudar e avaliar nossa privacidade na rede em sala de aula é de igual importância, como futuros cidadãos ativos cada aluno deve compreender os interesses das agências de tecnologia informacional, a fim de estar atento para com elas e procurar meios de se proteger e ser mais crítico quanto à sua exposição.

4. Considerações finais

As análises permitiram compreender melhor as estruturas de formação e as formas de ação das extrações e usos dos dados pessoais. Ressalta-se aqui a incongruência e o perigo existente em discursos nos quais a privacidade dos usuários deve ser perdida, para a melhoria dos serviços, ao passo que as mesmas empresas sustentadoras dessa ideia defendem a total privacidade para si, alegando proteção contra a concorrência. Aceitar esse discurso é aceitar a amplificação da facilidade de vigilância e controle de comportamento, os quais também interferem na atual democracia. Ir contrário a ele requer reforço dos discursos e cuidados em razão da proteção de nossa privacidade. A educação, em conjunto com o Estado e a sociedade, entra com seu papel para a formação crítica de seus alunos no tocante a este assunto. Enquanto a importância no trato dessa questão for pouco vislumbrada pela sociedade em geral, as regulamentações legais declinam na sua efetivação da garantia de proteção de dados pessoais.

5. Referências bibliográficas

ANDREWS, Lori. Facebook Is Using You. Disponível em: <https://www.nytimes.com/2012/02/05/opinion/sunday/facebook-is-using-you.html?_r=0> **The New York Times**, Fev. 4, 2012. Acesso em: 20 abr. 2020.

BBC News. O ESCÂNDALO que fez o Facebook perder US$ 35 bilhões em horas. Brasil, 20 mar. 2018. Disponível em: <https://www.bbc.com/portuguese/internacional-43466255>. Acesso em: 19 abr. 2020.

BELLI, Luca. 10 Neutralidade da rede, zero-rating e o Marco Civil da Internet. *In*: BELLI, Luca *et al*, (org.). **Governança e regulações da Internet na América Latina**: análise sobre infraestrutura, privacidade, cibersegurança e evoluções tecnológicas em homenagem aos dez anos da South School on Internet Governance. Rio de Janeiro: FGV Direito Rio, 2019. p. 175-201. Disponível em: <https://direitorio.fgv.br/publicacoes/governanca-e-regulacoes-da-internet-na-america-latina>. Acesso em: 4 mai. 2020.

BRASIL. Lei n.12.965, de 23 de abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.** Disponível em:<http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 21 abr. 2020.

DOMENICI, Thiago. **Laureate usa robôs no lugar de professores sem que alunos saibam:** Docentes da rede educacional que controla universidades como FMU e Anhembi Morumbi denunciam uso de inteligência artificial para correção de textos. Pública, Reportagem, 30 abr. 2020. Disponível em: <https://apublica.org/2020/04/laureate-usa-robos-no-lugar-de-professores-sem-que-alunos-saibam/>. Acesso em: 04 mai. 2020

DONEDA, Danilo; MENDES, Laura Schertel. 17 Um perfil da nova Lei Geral de Proteção de Dados brasileira. *In*: BELLI, Luca *et al*, (org.). **Governança e regulações da Internet na América Latina**: análise sobre infraestrutura, privacidade, cibersegurança e evoluções tecnológicas em homenagem aos dez anos da South School on Internet Governance. Rio de Janeiro: FGV Direito Rio, 2019. p. 309-324. Disponível em: <https://direitorio.fgv.br/publicacoes/governanca-e-regulacoes-da-internet-na-america-latina>. Acesso em: 17 mai. 2020.

DONEDA, Danilo; ALMEIDA, Virgílio A. F. O que é governança de algoritmos?. *In*: BRUNO, Fernanda *et al*, (org.). **Tecnopolíticas da vigilância**: perspectivas da margem. 1. ed. São Paulo: Boitempo, 2018. p. 141-148.

ERHARDT, A. A prática do Zero Rating e o Princípio da Neutralidade de Rede previsto na Lei nº 12.965/14: reflexões sobre o fenômeno da inclusão digital e o desenvolvimento de novas tecnologias. **Revista de Direito Setorial e Regulatório**, Brasília, v. 2, n. 1, p. 343-358, maio 2016.

GUGLIINSKII, Vitor. **Tudo sobre todos: a quem interessa saber sobre a vida alheia?** Jusbrasil, 2015. Disponível em: <https://vitorgug.jusbrasil.com.br/artigos/213141468/tudo-sobre-todos-a-quem-interessa-saber-sobre-a-vida-alheia> Acesso em: 19 abr. 2020.

POZZI, Sandro. EUA multam Facebook em 5 bilhões de dólares por violar privacidade dos usuários. **EL PAÍS**, Nova York, 13 jun. 2019. Disponível em: <https://brasil.elpais.com/brasil/2019/07/12/economia/1562962870_283549.html>. Acesso em: 19 abr. 2020.

SILVEIRA, Sergio Amadeu da. Economia da intrusão e modulação na internet. **Liinc em Revista**, Rio de Janeiro, v.12, n.1, p. 17-24, mai. 2016. Disponível em: <http://www.ibict.br/liinc>. Acesso em: 17 mai. 2020.

_____. **Tudo sobre tod@s: redes digitais, privacidade e venda de dados pessoais.** São Paulo: Edições Sesc São Paulo, 2017.

WERTHEIN, Jorge. A sociedade da informação e seus desafios. **Ci. Inf.**, Brasília , v. 29, n. 2, p. 71-77, Ago. 2000. Disponível em: <https://www.scielo.br/scielo.php?pid=S0100-19652000000200009&script=sci_abstract&tlng=pt>. Acesso em: 16 abr. 2020.

ZUBOFF, Shoshana. Big other: capitalismo de vigilância e perspectivas para uma civilização de informação. *In*: BRUNO, Fernanda *et al*, (org.). **Tecnopolíticas da vigilância**: perspectivas da margem. 1. ed. São Paulo: Boitempo, 2018. p. 17-68.