

1. Introdução

O presente artigo tem como objeto pesquisar as *Big Techs* e proteção de dados a partir das políticas públicas para os consumidores no Brasil. As *Big Techs* são conhecidas como grandes empresas digitais que tem como produto a transação de dados dos consumidores sem o consentimento dos mesmos o que gera muitas restrições ao direito de privacidade geral, principalmente a liberdade plena do cidadão. Há que se estudar as políticas públicas adotadas pelo Estado para coibir os abusos perpetrados por estas grandes empresas digitais a partir da introdução da tecnologia da informação na sociedade.

A problemática do presente artigo seria se a proteção de dados poderia ser considerada um direito de propriedade que permite o mercado se autorregular, sem a intervenção Estatal para não conferir a censura ou limitação da inovação, ou se trataria de um direito fundamental que deveria ser garantido pelo Estado para garantir a participação de cada indivíduo na vontade comum.

O presente artigo tem como suporte teórico o capitalismo de vigilância e o papel do Estado frente a tecnologia diante de uma trajetória histórica do arcabouço constitucional acerca do tema e do papel que deve ser dada à Constituição diante das mudanças tecnológicas vivenciadas nas últimas décadas, exigindo uma interpretação além do positivismo e dos preceitos da Constituição originária, frente a efetividade do direito fundamental da privacidade prevista no art. 5º da CF/88 conferindo aos seus titulares ferramentas que permitam à sua proteção. Aqui há que se analisar o Estado da arte sobre a proteção de dados no Brasil diante de uma sociedade em constante mutação.

No que tange a metodologia trata-se de uma pesquisa exploratória empírica, através da utilização de métodos qualitativos por meio de uma pesquisa bibliográfica.

2. Capitalismo de Vigilância e proteção de dados

O mundo está mudando e os ativos também. A Internet permitiu um enorme avanço do capital, mas gerou muitas restrições sociais, tais como a ascensão do capital

financeiro sobre o capital industrial e do capital de trabalho produtivo sobre o capital monetário fictício. Com o avanço da tecnologia digital, os ativos entram novamente em mutação.

Com a implantação da tecnologia da informação, a experiência humana tenderia a matéria-prima a ser negociada? Permitindo que os comportamentos dos potenciais consumidores sejam mapeados e utilizados como dados a serem vendidos e mercantilizados por aqueles que detêm as informações?

Segundo (ZUBOFF, 2019), o Google seria um exemplo de empresa que vende dados de seus usuários para empresas de outros setores. Neste sentido:

Os usuários abrem mão de suas informações e dados para circular livremente na plataforma digital, mas ficam vulneráveis às promessas e ao fato de não conhecerem os riscos do mundo digital. Desta forma, o autor destaca: No ano 2000, quando apenas 25% da informação mundial era armazenada digitalmente (Hilbert & López, 2011), uma pequena, mas brilhante startup de internet do Vale do Silício, chamada Google enfrentou uma ameaça existencial durante a crise financeira conhecida como o colapso das Pontocom. Os fundadores Larry Page e Sergey Brin ainda não haviam descoberto uma maneira de transformar o milagre do mecanismo de busca em dinheiro. Entre 2000 e 2001, enquanto os investidores da empresa ameaçavam deserção, a equipa da Google tropeçou numa série de descobertas que ofereciam um plano de resgate (Zuboff, 2019, pp. 63-97) (tradução nossa).

A autora mostra um nova era que ela chama de capitalismo de vigilância que ela classifica como sendo uma mutação do capitalismo digital, um sistema mais focado nos moldes do liberalismo e com o fundamento econômico no mercado, o que mostra o lado diametralmente oposto ao da inclusão digital.

Mas o presente artigo pretende também pesquisar outro ator social importante que é o Estado e o reducionismo a que fica sujeito com a nova ascensão do liberalismo, por meio do neoliberalismo que procura restringir o seu papel a uma intervenção mínima, em detrimento dos direitos sociais.

Esta visão conflita com o Estado social de direito social, pois restringe a intervenção Estatal a fim de conter os abusos perpetrados pela ordem econômica.

Zuboff (2019) alega que o capitalismo de vigilância é decorrência de uma democracia fraca e dá em seu livro o exemplo da democracia americana abalada pelo 11 de Setembro. Nestes casos, o próprio Estado renunciaria a espaços de informação o que permitiria que esse espaço fosse ocupado por gigantes do setor privado que passariam a monitorar os dados e informações e a controlar instituições, espaços, sistemas e processos, ou seja, comunicações e informações de massa.

O capitalismo de vigilância foi o que aconteceu quando a democracia dos EUA caiu. Duas décadas mais tarde, falha em qualquer teste razoável de gestão global responsável da informação e das comunicações digitais. A abdicação dos espaços de informação mundiais ao capitalismo de vigilância tornou-se a meta-crise de todas as repúblicas porque obstrui as soluções para todas as outras crises. Os gigantes capitalistas de vigilância – Google, Apple, Facebook, Amazon, Microsoft e os seus ecossistemas – constituem agora uma ordem institucional político-econômica abrangente que exerce controle oligopolístico sobre a maioria dos espaços, sistemas e processos digitais de informação e comunicação. (ZUBOFF, 2019 (tradução nossa).

Neste sentido, o papel do Estado é revisto na sequência das grandes crises do Capitalismo que enfraqueceram a própria democracia e o acesso, principalmente com a ascensão do neoliberalismo que começou no final dos anos 70 com Reagan e Thatcher (Harvey, 2008)

Neste cenário, o Estado Social é novamente anulado a favor dos grandes grupos econômicos e do poder das instituições financeiras e dos grandes conglomerados econômicos (HARVEY, 2008), principalmente nos países latino-americanos que na corrida pelo desenvolvimento tornam-se reféns do Capital estrangeiro e dependentes dos ditames do Capital Financeiro e Digital com a concentração de poder das grandes empresas internacionais (FURTADO, 1973).

Com as *Big Techs*, a matéria-prima que está sendo processada e que estaria sendo mercantilizada seriam os dados comportamentais dos consumidores que ao acessarem as plataformas, mesmo que gratuitamente, potencializam os lucros e os recursos empresariais dessas pessoas jurídicas que, apesar de não produzirem mercadorias, têm um ativo de dados, um ativo intangível muito pessoal que se torna mercadoria em mãos de terceiros. Neste caso, haveria necessidade da intervenção urgente do Estado na economia?

Para (Batkins, 2019; “s Google an evil genius?”, 2019; Thornhill, 2019), a regulação seria contraproducente, pois desaceleraria a inovação, criaria custos para os usuários e seria inofensiva, pois a tecnologia suplantaria qualquer controle. A privacidade seria um direito subjetivo mercantilizável pelo seu titular, cuja liberdade de escolha seria exercida no momento da contratação dos termos de uso. Só a concorrência entre empresas poderia proteger a privacidade, pois estas ofereceriam condições mais vantajosas aos clientes, que poderiam escolher modelos por design e vender os seus dados. Mais uma vez voltamos à retórica da Revolução Burguesa: será que o mercado é capaz de garantir o bem-estar social?

Porém, como visto na história, o mercado é competitivo, individual e os dados são relevantes para garantir rentabilidade a longo prazo e superar a concorrência e o poder de mercado, o que seria até um alicerce para quem entende que esse tipo de prática faz parte do funcionamento do capitalismo e não estaríamos perante um novo capitalismo, pois é uma lógica de crescimento para todas as empresas.

Segundo Schertel (2014) o fato de conferir direito de propriedade aos grandes conglomerados econômicos violaria o direito de igualdade, até porque nem todos os consumidores teriam o mesmo poder de compra o que é um reflexo da desigualdade social, o que acabaria por privilegiar a camada mais rica da sociedade. Além disso, os indivíduos poderiam forjar a sua individualidade, a fim de maximizar o interesse das empresas nas suas informações pessoais. Além disso, a patrimonialização do direito de proteção de dados seria uma ameaça a ordem democrática o que acabaria por implementar um poder de vigilância constante e ingerência do mercado na liberdade individual.

Porém, o presente trabalho parte do pressuposto do direito à personalidade não ser um bem pessoal absoluto, pois é um direito fundamental que deve ser garantido pelo

Estado, mas que pode ser relativizado em situações excepcionais em que se garanta a proteção do direito a privacidade que assume uma dimensão coletiva.

Para Doneda (2019, 43), em que pese reconhecer o à privacidade como espécie de direito fundamental, com a sua conseqüente funcionalização, é permitido desdobrá-lo em uma série de direitos subjetivos, tais como o direito à vida privada e à vida familiar, mas também o direito à proteção dos dados pessoais. Segundo o autor à tutela dos dados pessoais perpassa uma esfera individual para ganhar uma dimensão coletiva, “através do reconhecimento dos dados pessoais como instrumento apto para o controle político dos indivíduos e suscetível de uso para discriminar grupos minoritários (DONEDA, 2019, p. 46”.

Schertel (2014) fala sobre a grande discussão de se garantir um direito de propriedade sobre os dados pessoais diante deste grande ativo que vem sendo adquirido pelas *Big Techs* e, principalmente, a necessidade de se coibir os potenciais danos da comercialização do direito de personalidade aos direitos fundamentais.

Mas o objeto a ser destacado não é o indivíduo como pessoa física, mas o cidadão dentro de uma ordem democrática de direito dotado de uma personalidade jurídica ampla e complexa, enquanto consumidor com seus direitos metaindividuais e, também enquanto sujeito político detentor de autonomia, principalmente dentro de um Estado democrático de direito em que a violação dos dados fere frontalmente o aspecto coletivo do grupo social, devido à restrição direta ao seu direito de liberdade.

A privacidade assume, portanto, posição de destaque na proteção da pessoa humana, não somente tomada como escudo contra o exterior – na lógica da exclusão – mas como elemento indutor da autonomia, da cidadania, da própria atividade política em sentido amplo e dos direitos de liberdade de uma forma geral. Nesse papel, ela é pressuposto de uma sociedade democrática moderna, da qual o dissenso e o anticonformismo são componentes orgânicos. (DONEDA, 2019, p. 128-129)

Aqui não há que se confundir a liberdade econômica do liberalismo com a liberdade do Estado social de direito, como bem ressalva Norberto Bobbio (). O que se está ferindo com uma manipulação em massa dos dados e do direito de

informação é a própria democracia e o Estado não pode abster-se de agir em prol do capital. Neste sentido leciona Doneda (2019, p.128-129):

“... com novas tecnologias e novos mecanismos de controle e transmissão de informação teriam feito surgir uma acepção positiva da privacidade, que exigia o fornecimento aos seus titulares de mecanismos eficazes para a construção de uma esfera privada na qual possam desenvolver plenamente a sua personalidade”.

O artigo é desenvolvido com o objetivo de trabalhar com o cidadão entro da ordem democrática de direito exigindo do Estado uma atuar para garantir efetivamente o direito à privacidade que assume um feixe complexo de relacional.

Em uma órbita capitalista utilitarista, o consumidor passa ser o ator principal daquele sistema o que reduz o papel do Estado em prol do mercado e as garantias a lei. As próprias mutações do capitalismo levam a uma supressão de direitos efetivos e acaba por sustentar posicionamentos como o de Batkins (2019) que pretende precificar os dados como uma nova commodity, retirando a subjetividade do direito à intimidade que se desdobra, inclusive, na proteção dos dados pessoais, seja por agentes públicos e privados.

Cabe aqui trazer algumas considerações importantes do STF no referendo na medida cautelar na ação direta de inconstitucionalidade 6.389 Distrito Federal ajuizadas contra o inteiro teor da Medida Provisória 954, de 17 de abril de 2020, em que a Relatora era a Ministra Rosa Weber tratou do compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal junto a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid19), de que tratava a Lei nº 13.979, de 6 de fevereiro de 2020.

Em que pese a Relatora ter entendido que a norma neste caso padecia de uma inconstitucionalidade formal, ela se debruçou sobre a questão material e o papel do Estado frente aos direitos fundamentais de proteção de dados, pois à época o texto constitucional

era omissa acerca do tema e havia precedente anterior do STF acerca do direito de privacidade não exigir um atuar positivo do Estado.

Esse voto se tornou um grande paradigma de mudança tendo em vista que o direito de privacidade já tinha sido objeto de discussão anteriormente no voto do Ministro Sepúlveda Pertence, no julgamento do Mandado de Segurança 21.729/D, no RE 418.416-8/SC em 10.05.2006, que entendeu que não teria ocorrido quebra de sigilo das comunicações de dados, mas tão somente apreensão de base física na qual se encontravam os dados não exigindo um atuar do Estado.

O autor Lawrence Lessig ((1996) mostra em seu livro “*Reading the constitution in cyberspace*” que existem dois tipos de constituição: uma constituição codificadora clássica e imutável em relação as transformações futuras e uma constituição mutável e transformadora com as demandas do futuro. A questão é que uma constituição que não seja transformadora, segundo o autor, não é capaz de proteger direitos fundamentais no futuro, como no caso das mudanças que decorram da própria tecnologia e que invade o espaço privado dos indivíduos. A norma não consegue acompanhar as incessantes transformações a que se sujeita o indivíduo, principalmente no que tange aos abusos de alguns poderes específicos. Neste caso, deve ser permitida uma interpretação de forma a adaptar a normas as constantes mutações do mundo moderno, principalmente se for considerado o mundo digital.

Neste sentido, o autor cita o caso do Juiz Louis Brandeis em 1928, nos Estados Unidos, em que se discutia a Quarto Emenda. Embora tenha sido voto vencido no caso concreto que interpretava se a Constituição Norte-americana, o juiz entendia que a norma protetiva de abusos deveria se adequar as transformações da sociedade. No caso da Constituição de 1988, as transformações digitais ainda eram incipientes no Brasil o que não tinha um poder de grande transformação e nem um alcance tão expressivo e dependia de uma visão de vanguarda do Supremo Tribunal Federal, por meio da ministra Rosa Weber.

Posteriormente, a Emenda Constitucional 115/2022, de 10 de fevereiro alterou a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Esta alteração consolida de forma material a proteção de dados como um direito fundamental.

3. Políticas Públicas para o cidadão consumidor

Neste capítulo o objetivo é estudar as políticas públicas produzidas pelo Estado para coibir os abusos cometidos pelas *Big Techs* no Brasil diante da vulnerabilidade do consumidor.

No que tange ao direito do consumidor, a organização das Nações Unidas, em 1985, e revista em 1999 e 2015, estabeleceu diretrizes para o “consumidor” e classificou os seus direitos como um direito humano de nova geração.

No Brasil, a Constituição de 1988 previu a criação de uma legislação consumerista e deu prazo de 180 dias para a elaboração do Código, o que só veio em 1990. O que foi considerado um grande avanço no ordenamento jurídico brasileiro, criando uma lei mista, entre público e privado, com função social, direito privado solidário dentro de uma sociedade capitalista. Surge na emergência do Estado Neoliberal no Brasil e visa proteger os mais fracos e vulneráveis com preceitos de ordem pública que aborda a igualdade material.

Porém, mais de 30 anos após sua entrada em vigor, o Brasil apresenta uma lacuna muito grande diante do capitalismo digital, porque ainda possui preceitos voltados para o capitalismo industrial, voltado para o consumo de massa. Não há legislação no Código de Defesa do Consumidor referente à proteção de dados de consumidores, contratos digitais, proteção de informações de crianças e idosos pela hiper vulnerabilidade que apresentam e preceitos ou questões relativas à inteligência artificial, o que torna o tema de extrema relevância (MARQUÊS, 2022).

As atividades desenvolvidas na internet foram reguladas inicialmente pela Lei 12.695/2014, conhecido como Marco Civil da Internet, posteriormente, a Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD). Somente no dia 28/10/21, o Conselho Diretor da ANPD deliberou sobre a aprovação do Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador. Aprovado de forma unânime, o Regulamento teria como principal objetivo o fomento a uma cultura de proteção de dados no País.

Em janeiro de 2021, a empresa passou a anunciar alterações nos termos de uso da plataforma, causando grande indignação de usuários e autoridades internacionais devido

ao conhecimento de práticas de compartilhamento de dados dentro do grupo com a empresa Facebook Serviços Online do Brasil Ltda. ("Facebook").

Mas o que aparentemente aparenta ser um serviço gratuito e disponível ao consumidor, torna-se um produto a ser comercializado. O consumidor ao logar na plataforma da Google disponibiliza seus dados que vão sendo catalogados e formando um perfil a ser compartilhado acerca do seu comportamento que serão negociados com terceiros.

Aqui há que se analisar especificamente o consentimento enquanto um processo de tomada de decisão, e não como um ato pontual de declaração de vontade do titular a ponto de violar o consentimento válido (BIONI,2020). No caso em concreto, trata-se de um consumidor com uma vulnerabilidade técnica e econômica o que faz com que este consentimento não possa ser tratado como mero ato de vontade, baseado no *pacta sunt servanda*, com caráter negocial voluntário. Isso só viria reforçar o caráter de propriedade e de commodities dos dados.

Há que se buscar a sua natureza jurídica como atributo da personalidade jurídica a fim de gerar uma esfera de proteção efetiva para o consumidor baseado no princípio da boa-fé objetiva e da transparência. Para que o consentimento do consumidor seja válido, no caso de cessão de informações de empresas do mesmo grupo, haveria necessidade de se observar o consentimento consciente dos dados e o princípio da finalidade (SCHERTEL,2014).

A Lei 13.709/2018 (Lei Geral de Proteção de Dados) que no seu artigo 2º, II vincula a proteção de dados pessoais à autodeterminação informativa, princípio que foi importado das decisões do Tribunal Constitucional Federal Alemão a partir da decisão do Censo de 1983 e que até então não tinha previsão no ordenamento jurídico brasileiro.

O princípio da autodeterminação informacional não permite que os dados e informações sejam colhidos a ponto de reduzir ou manipular a capacidade de entendimento do sujeito de direito ou mesmo suas escolhas a ponto de ferir sua privacidade geral e restringir o direito de liberdade. Mas o que faz com que as *Bigh techs* consigam burlar o princípio da autodeterminação dos dados?

Esta técnica de monitoramento através dados dos consumidores que são incorporadas na rede é chamada de *profiling*, em que por meio dos algoritmos os dados

vão sendo armazenados e direcionados o que apesar de uma autonomia do consumidor em querer compartilhar seus dados ele passa a ser monitorado, limitando a sua liberdade de escolha. Cria-se um monopólio digital acerca das informações da qual aquele consumidor terá acesso. Nesse sentido:” os algoritmos indicam qual conteúdo será consumido primeiro, qual será o mais adequado para cada indivíduo e, dessa forma, limitam o acesso à informação” (BEÇAK; LONGHI, 2020).

Um caso empírico que demonstrou esta questão no Brasil foi quando a Google tentou coibir a participação popular no projeto da Lei da Fake News (PL 2630), atualmente conhecido como Lei da Transparência (PL 2768/2022) que continua tramitando no Congresso Nacional. A Google resolveu agir com informação massiva contra ao projeto de lei para coibir notícias falsas, que impactam diretamente o exercício do direito democrático porque não queria ter nenhuma interferência do Estado em suas atividades.

Iniciou-se uma verdadeira batalha contra o PL das Fake News, como visto no trabalho publicado pela UFRJ, A Guerra das Plataformas pelo PL 2630/2020, Laboratório de Estudos de Internet e Mídias Sociais considerando que restringe e exige transparência, o que deixa os consumidores vulneráveis aos interesses das *Big Techs* e aos seus lucros.

O Ministério Público Federal em conjunto com a Secretaria Nacional de Defesa do Consumidor (Senacon) tomou medidas para obrigar o Google a cumprir uma série de medidas determinadas em caráter cautelar pelo fato de ter agido irregularmente em 2023 para promover seus próprios interesses econômicos. Isso também se deveu ao fato da Google ter incluído, na página principal do buscador, ao lado da caixa de busca, um texto no qual argumentava que “O Projeto de Lei das Fake News poderia aumentar a confusão sobre o que é verdadeiro ou falso no Brasil”. O link direcionava o internauta para um artigo assinado pelo diretor de Relações Governamentais e Política Pública do Google, Marcelo Lacerda, e foi retirado do ar, logo após a Senacon anunciar as medidas que a empresa deveria cumprir.

O Regimento Interno da Autoridade Nacional de Proteção de Dados (ANPD), assim como a LGPD não foram capazes de conter a cessão de dados privados entre o grupo de *Big Techs*, como no caso do WhatsApp que alterou seu termo de uso e privacidade sem o consentimento do consumidor para o Facebook, o que exige do Estado cada vez mais políticas públicas para coibir tais abusos e sanções que

Outro caso emblemático recente foi com o dono e CEO (Chief Executive Officer) da provedora de rede social “X” - anteriormente “Twitter” -, ELON MUSK, no caso do inquérito 4874-DF e das organizações criminosas investigadas nos INQs 4923, 4933 e PET 12100, da Relatoria do Ministro do STF, que teria iniciado uma campanha de desinformação sobre a atuação do Supremo Tribunal Federal colocando em risco a vida dos próprios ministros do STF e da ordem democrática de direito.(STF, Inq 4874-DF, 2024)

O problema dos algoritmos é que quanto mais informação se acessa maior é o número de informações compartilhadas no mesmo sentido para o consumidor disseminando a desinformação ou ódio. Os algoritmos não conseguem fazer o filtro da informação, e sim, agregam e disseminam dados iguais ou informações no mesmo sentido, o que compromete à legitimidade da informação e acaba por comprometer a própria democracia.

Em que pese ter sido feito grupo de trabalho objetivando avançar em uma proposta de regulamentação e da responsabilidade dos provedores de internet pelos conteúdos ilícitos veiculados nas diversas plataformas ou de uma maior fiscalização, pouco se avançou neste sentido até o momento neste sentido.

4. Conclusão

Em todos estes casos o que se vislumbra que além da vulnerabilidade do consumidor o Estado se torna um ator essencial para coibir os atos e produzir políticas públicas a fim de gerar maior segurança jurídica a ordem democrática de direito e fazer valer a decisão judicial bem como toda a proteção legal e jurisprudencial que reconhece a proteção de dados como um direito fundamental, reconhecido como direito a privacidade geral que garante ao cidadão sua liberdade plena de escolha, de decisão e de informação.

Desde 2015, está em tramitação no Congresso Nacional o PL 3514/2015, que busca atualizar o CDC para o mundo digital, conhecido após a apresentação de um novo texto ao presidente da Câmara por um grupo de juristas como o Marco Legal da Inteligência Artificial, que é de extrema importância aprová-lo o mais breve possível,

dado o avanço da tecnologia digital em termos de responsabilidades e limites para o capital digital, principalmente no que tange ao compartilhamento de dados.

Mas como ficam as políticas públicas em termos de governança para proteger os dados e a privacidade geral dos usuários? Exige-se cada vez mais uma maior governança por parte do Estado, principalmente no que tange a regulamentação deste ator social, mas também uma maior fiscalização por meio de políticas públicas através de seus órgãos e instituições para frear o poder dos grandes conglomerados econômicos, que afrontam o consumidor enquanto usuários de produtos ou serviços, bem como no acesso à liberdade de informação, comprometendo a própria soberania Estatal como no caso do X.

O que se verifica com a avanço do capitalismo digital é que embora se apresente com uma solução de mercado e de bem-estar econômico ele não pode ser associado a liberdade material, sua liberdade sempre esteve associada a preservação dos meios de produção e cada vez mais pretende-se reduzir o papel do Estado e das garantias de seus cidadãos. O Estado tem que estar atendo a produção de políticas públicas contra o poder invisível dos algoritmos a fim de que não ceda aos oligopólios de poder e atenda aos interesses sociais.

Referência bibliográficas:

ALEMANHA. Bundesverfassungsgericht – BVerfGE. Reclamação Constitucional Contra Ato Normativo BVerfGe 65, 1. 15 de dezembro de 1983. Disponível em: <https://www.servat.unibe.ch/dfr/bv065001.html>. Acesso em: 07 nov. 2021.

ALIMONTI, Verdiana. Autodeterminação informacional na LGPD: antecedentes, influências e desafios. In: DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo Villas Bôas (coord.). Lei Geral de Proteção de Dados (Lei no 13.709/2018): a caminho da efetividade – contribuições para a implementação da LGPD. São Paulo: Thomson Reuters, 2020. p. 177-191.

BRASIL. Constituição da República Federativa do Brasil de 1988. Diário Oficial da União, Brasília, DF, 5 out. 1988. Disponível em:

http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 12 nov. 2021.

BRASIL. Lei no 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em: 28 out. 2021.

BRASIL. Supremo Tribunal Federal. Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade no 6.387 Distrito Federal. Relatora: Min. Rosa Weber, 7 de maio de 2020. Disponível em: <https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357629>. Acesso em: 02 nov. 2021.

BRASIL. Supremo Tribunal Federal. Inquérito 4.874 Distrito Federal. Relator> Ministro Alexandre de Moares, 07 de abril de 2024. Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=6214799>.

BRASIL. Conselho Diretor aprova o Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da Autoridade Nacional de Proteção de Dados. Gov.br, Brasília, DF, 29 out. 2021. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/conselho-diretor-aprova-o-regulamento-do-processo-de-fiscalizacao-e-do-processo-administrativo-sancionador-no-ambito-da-autoridade-nacional-de-protecao-de-dados>. Acesso em: 24 nov. 2021.

BEÇAK, Rubens; LONGHI, João Victor Rozatti. Populismo digital e princípio democrático: o problema da censura reversa como método de comunicação. In: LISBOA, Roberto Senise (coord.). O direito na sociedade da informação IV: movimentos sociais, tecnologia e atuação do Estado. São Paulo: Almedina, 2020. p. 170-191.

BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. São Paulo: Editora Gen, 2019, p. 95).

CANARIS, Claus-Wilhelm. Direitos fundamentais e direito privado. Trad. Ingo Wolfgang Sarlet e Paulo Mota Pinto. Coimbra: Almedina, 2003.

DONEDA, Danilo Cesar Maganhoto. Da privacidade à proteção de dados pessoais: elementos da formação da Lei geral de proteção de dados. 2. ed. São Paulo: Thomson Reuters; Revista dos Tribunais, 2019. p. 136.

FERRAZ JÚNIOR, Tércio. Sigilo de dados: o direito à privacidade e os limites da função fiscalizadora do estado. Revista da Faculdade de Direito da Universidade de São Paulo, v. 88, p. 430-459, 1993.

FURTADO, Celso. O mito do desenvolvimento econômico. São Paulo: Editora Paz e Terra, 1973.

HARVEY, David. O neoliberalismo, história e implicações. São Paulo: Edições Loyola, 2008.

LESSIG, Lawrence. Reading The Constitution in Cyberspace. Emory Law Review, v. 45, p. 869–910, 1996, p. 41.

HOFFMANN-RIEM, Wolfgang. Innovaciones en La Jurisprudencia del Tribunal Constitucional Alemán, a Propósito de la Garantía De Los Derechos Fundamentales En Respuesta A Los Cambios Que Conducen A La Sociedad De La Información. ReDCE, n. 22, 2014.

MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 140., p. 178.

SCHWABE, Jürgen. Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão. Montevideo: Fundación Konrad-Adenauer, 2005. p. 237. Disponível em:

[http://www.mpf.mp.br/atuacao-tematica/sci/jurisprudencias-e-
pareceres/jurisprudencias/docs](http://www.mpf.mp.br/atuacao-tematica/sci/jurisprudencias-e-pareceres/jurisprudencias/docs)

jurisprudencias/50_anos_dejurisprudencia_do_tribunal_constitucional_federal_alemao.pdf. Acesso em: 07 nov. 2021.

Mendes, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

ZUBOFF, S. Big other: surveillance capitalism and the prospects of an information civilization. Journal of Information Technology, v. 30, n. 1, p. 75-89, 2015.

ZUBOFF, S. The age of surveillance capitalism: the fight for a human future at the new frontier of power. New York: Public Affairs, 2019.