

REVISTA DE DIREITO DA ADMINISTRAÇÃO PÚBLICA



ISSN 2595-5667

REVISTA DE DIREITO DA ADMINISTRAÇÃO PÚBLICA

ANO Nº 09 – VOLUME Nº 01 – EDIÇÃO Nº 03 – Dossiê Temático
ISSN 2595-5667

Editor-Chefe:

Prof. Dr. Emerson Affonso da Costa Moura, Universidade Federal do Estado do Rio de Janeiro e
Universidade Federal Rural do Rio de Janeiro, Brasil

**Rio de
Janeiro, 2024.**

REVISTA DE DIREITO DA ADMINISTRAÇÃO PÚBLICA

LAW JOURNAL OF PUBLIC ADMINISTRATION

Conselho Editorial Internacional:

- Sr. Alexander Espinosa Rausseo, Universidad Central de Venezuela, Venezuela
Sr. Erik Francesc Obiol, Universidad Nacional de Trujillo, Trujillo, Peru, Peru
Sr. Horacio Capel, Universidad de Barcelona, Barcelona, Espanha.
Sra. Isa Filipa António, Universidade do Minho, Braga, Portugal, Portugal
Sra. Maria de Los Angeles Fernandez Scagliusi, Universidad de Sevilla, Sevilha, Espanha.
Sr. Luis Guillermo Palacios Sanabria, Universidad Austral de Chile (UACH), Valdivia, Chile.
Sra. Mónica Vanderleia Alves de Sousa Jardim, Universidade de Coimbra, UC, Portugal.
Sr. Mustafa Avci, University of Anadolu, Turquia

Conselho Editorial Nacional:

- Sr. Adilson Abreu Dallari, Pontificia Universidade Católica, PUC/SP, Brasil.
Sr. Alexandre Santos de Aragão, Universidade do Estado do Rio de Janeiro, UERJ, RJ, Brasil.
Sr. Alexandre Veronese, Universidade de Brasília, UNB, Brasil.
Sr. André Saddy, Universidade Federal Fluminense, UFF, Brasil.
Sr. Carlos Ari Sundfeld, Fundação Getúlio Vargas, São Paulo, Brasil.
Sra. Cristiana Fortini, Universidade Federal de Minas Gerais, UFMG, Brasil.
Sra. Cynara Monteiro Mariano, Universidade Federal do Ceará, UFC, Brasil.
Sr. Daniel Wunder Hachem, Universidade Federal do Paraná, UFPR, Brasil.
Sr. Eduardo Manuel Val, Universidade Federal Fluminense, UFF, Brasil.
Sr. Fabio de Oliveira, Universidade Federal do Rio de Janeiro, UFRJ, Rio de Janeiro, RJ, Brasil.
Sr. Flávio Garcia Cabral, Escola de Direito do Mato Grosso do Sul, Mato Grosso do Sul., Brasil
Sr. Henrique Ribeiro Cardoso, Universidade Federal de Sergipe, UFS, Brasil.
Sr. Jacintho Silveira Dias de Arruda Câmara, Pontificia Universidade Católica, São Paulo, Brasil.
Sra. Jéssica Teles de Almeida, Universidade Estadual do Piauí, UESPI, Piri-piri, PI, Brasil., Brasil
Sr. José Carlos Buzanello, Universidade Federal do Estado do Rio de Janeiro, RJ, Brasil.
Sr. José Vicente Santos de Mendonça, Universidade do Estado do Rio de Janeiro, UERJ, Brasil.
Georges Louis Hage Humbert, Unijorge, Brasil
Sra. Maria Sylvia Zanella di Pietro, Universidade de São Paulo, USP, Brasil.
Sra Marina Rúbia Mendonça Lôbo, Pontificia Universidade Católica de Goiás, Goiás, Brasil.
Monica Sousa, Universidade Federal do Maranhão
Sr. Mauricio Jorge Pereira da Mota, Universidade do Estado do Rio de Janeiro, UERJ, Brasil.
Sra. Monica Teresa Costa Sousa, Universidade Federal do Maranhão, UFMA, Maranhão, Brasil.
Sra. Patricia Ferreira Baptista, Universidade do Estado do Rio de Janeiro, UERJ, Brasil.
Sr. Paulo Ricardo Schier, Complexo de Ensino Superior do Brasil LTDA, UNIBRASIL, Brasil.
Sr. Vladimir França, Universidade Federal do Rio Grande do Norte, UFRN, Brasil.
Sr. Thiago Marrara, Universidade de São Paulo, USP, Brasil.
Sr. Wilson Levy Braga da Silva Neto, Universidade Nove de Julho, UNINOVE, Brasil.
-

BIG TECH E POLÍTICAS PÚBLICAS PARA CONSUMIDORES NO BRASIL **BIG TECH AND PUBLIC POLICIES FOR CONSUMERS IN BRAZIL**

Taíssa Salles Romeiro¹

RESUMO: O objetivo deste artigo é pesquisar as Big Techs e a proteção de dados a partir das políticas públicas para o consumidor no Brasil. As Big Techs são conhecidas como grandes empresas digitais cujo produto é a transação de dados dos consumidores sem o seu consentimento, o que gera muitas restrições ao direito geral à privacidade, especialmente à plena liberdade do cidadão. É preciso estudar as políticas públicas adotadas pelo Estado para coibir os abusos praticados por essas grandes empresas digitais em razão da introdução da tecnologia da informação na sociedade. Como os usuários/consumidores podem defender seus direitos, diante da violação dos princípios básicos do Código de Defesa do Consumidor, boa-fé objetiva e da autodeterminação informativa, previstos na LGPD? Quanto à metodologia, trata-se de um estudo empírico exploratório, utilizando métodos qualitativos através de pesquisa bibliográfica.

PALAVRAS-CHAVES: Big techs. Consumidor. Proteção de Dados. Normas Técnicas da ANPD.

ABSTRACT: The objective of this article is to research Big Techs and data protection based on public policies for consumers in Brazil. Big Techs are known as large digital companies whose product is the transaction of consumer data without their consent, which generates many restrictions on the general right to privacy, especially the full freedom of the citizen. It is necessary to study the public policies adopted by the State to curb the abuses practiced by these large digital companies due to the introduction of information technology in society. How can users/consumers defend their rights, given the violation of the basic principles of the Consumer Defense Code, objective good faith and informational self-determination, provided for in the LGPD? Regarding the methodology, this is an exploratory empirical study, using qualitative methods through bibliographic research.

¹ Professora Adjunta da Universidade Federal do Estado do Rio de Janeiro e lotada no Centro de Ciências Jurídicas e Políticas - CCJP, no Departamento de Fundamentos. Doutora em Ciências Políticas e Sociais pela Universidade Federal Fluminense e Mestre em Direito pela Universidade Estácio de Sá.

KEYWORDS: Big techs. Consumer. Data Protection. ANPD Technical Standards.

1. INTRODUÇÃO

O objetivo deste artigo é pesquisar as Big Techs e a proteção de dados com base nas políticas públicas para o consumidor no Brasil. As Big Techs são conhecidas como grandes empresas digitais cujo produto é a transação de dados dos consumidores sem o seu consentimento, o que gera muitas restrições ao direito geral à privacidade, especialmente à plena liberdade do cidadão. É preciso estudar as políticas públicas adotadas pelo Estado para coibir os abusos perpetrados por essas grandes empresas digitais em razão da introdução da tecnologia da informação na sociedade.

O que está se discutindo neste artigo é se a proteção de dados pode ser considerada um direito de propriedade, que permita ao mercado regular-se sem intervenção do Estado, de modo a não censurar ou limitar a inovação, ou se é um direito fundamental que deva ser garantido pelo Estado, para assegurar a participação de todos, na vontade comum.

O presente artigo tem como base teórica o capitalismo de vigilância, bem como pretende analisar o papel do Estado diante da tecnologia, observando a trajetória histórica do marco constitucional sobre o tema e o papel que a Constituição deve desempenhar diante das mudanças tecnológicas vivenciadas nas últimas décadas.

A Constituição vem exigindo do intérprete uma análise que ultrapasse o positivismo e os preceitos do constituinte originário, diante da efetividade do direito fundamental à privacidade previsto no artigo 5º da Constituição da República Federativa de 1988, dando aos seus titulares ferramentas para protegê-lo. Aqui se faz necessário analisar o estado da arte sobre a proteção de dados no Brasil diante de uma sociedade em constante mudança.

Quanto à metodologia, trata-se de um estudo empírico exploratório, utilizando métodos qualitativos através de pesquisa bibliográfica.

II. O CAPITALISMO DE VIGILÂNCIA E A PROTEÇÃO DE DADOS

O mundo está a mudar e os bens também. A internet permitiu que o capital avançasse enormemente, mas gerou muitas restrições sociais, como a ascensão do capital financeiro sobre o capital industrial e a escassez do capital produtivo do trabalho para abundância do capital monetário fictício. Com o avanço da tecnologia digital, os ativos estão a mudar novamente

Com a implementação da tecnologia da informação, a experiência humana tende a se tornar uma matéria-prima a ser comercializada, permitindo que o comportamento de potenciais consumidores seja mapeado e utilizado como dados a serem vendidos e mercantilizados por aqueles que detêm a informação. De acordo com (ZUBOFF, 2019), o Google seria um exemplo de empresa que vende os dados de seus usuários para empresas de outros setores. Nesse sentido:

Os usuários cedem suas informações e dados para circularem livremente na plataforma digital, mas ficam vulneráveis às promessas e ao fato de não conhecerem os riscos do mundo digital. Neste sentido, a autora salienta que no ano 2000, quando apenas 25% das informações do mundo estavam armazenadas 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 “*dotcom crash*”. Os fundadores Larry Page e Sergey Brin ainda não tinham descoberto uma forma de transformar o milagre do motor de busca em dinheiro. Entre 2000 e 2001, enquanto os investidores da empresa ameaçavam desertar, a equipa da Google deparou-se com uma série de descobertas que ofereceram um plano de salvamento (ZUBOFF, 2019, pp. 63-97).

A autora mostra uma nova era que chama de capitalismo de vigilância, que classifica como uma mutação do capitalismo digital, um sistema mais focado na linha do liberalismo e com a sua base económica no mercado, o que mostra o lado diametralmente oposto da inclusão digital.

Mas este artigo pretende também investigar outro importante ator social - o Estado - e o reducionismo a que está sujeito pela nova ascensão do liberalismo, através do neoliberalismo, que procura restringir o seu papel a uma intervenção mínima, em detrimento dos direitos sociais. Esta visão entra em conflito com o estado social de direito social, pois restringe a intervenção estatal para coibir os abusos perpetrados pela ordem económica.

Zuboff (2019) afirma que o capitalismo de vigilância é o resultado de uma democracia fraca e dá em seu livro o exemplo da democracia americana abalada pelo 11 de setembro. Nesses casos, o próprio Estado cederia seu espaço de informação, o que permitiria que esse espaço fosse ocupado por gigantes do setor privado que monitorariam dados e informações e

controlariam instituições, espaços, sistemas e processos, ou seja, a comunicação e a informação de massa.

O capitalismo de vigilância foi o que aconteceu quando a democracia dos EUA entrou em colapso. Duas décadas depois, não passa em nenhum teste razoável de gestão global responsável da informação e das comunicações digitais. A abdicação dos espaços de informação do mundo ao capitalismo de vigilância tornou-se a meta-crise de todas as repúblicas, porque obstrui as soluções para todas as outras crises. Os gigantes do capitalismo de vigilância - Google, Apple, Facebook, Amazon, Microsoft e os seus ecossistemas - constituem agora uma ordem institucional político-econômica abrangente que exerce um controlo oligopolista sobre a maioria dos espaços, sistemas e processos de informação e comunicação digital (ZUBOFF, 2019).

Nesse sentido, o papel do Estado está sendo revisto após as grandes crises do capitalismo que enfraqueceram a própria democracia e o acesso, principalmente com a ascensão do neoliberalismo iniciada no final da década de 1970, com Reagan e Thatcher (Harvey, 2008

Nesse cenário, o Estado de bem-estar social é mais uma vez anulado em 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 Tech, a matéria-prima a ser processada e 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, embora não produzam bens, possuem um ativo de dados, um bem intangível personalíssimo que se torna uma mercadoria nas mãos de terceiros. Neste caso, haveria necessidade de uma intervenção urgente do Estado na economia?

Para Thornhill, (2019), a regulação seria contraproducente, pois desaceleraria a inovação, criaria custos para os utilizadores e seria inócua, pois a tecnologia suplantaria qualquer controle. A privacidade seria um direito subjetivo comercializável pelo seu titular, cuja liberdade de escolha seria exercida na contratação dos termos de utilização. Só a concorrência entre empresas poderia proteger a privacidade, pois estas ofereceriam condições

mais vantajosas aos clientes, que poderiam escolher modelos por conceção e vender os seus dados. Mais uma vez voltamos à retórica da Revolução Burguesa: pode o mercado garantir o bem-estar social?

No entanto, como mostra a história, o mercado é competitivo, individual e os dados são relevantes para garantir a rentabilidade a longo prazo e superar a concorrência e o poder de mercado, o que seria até um fundamento para quem entende que esse tipo de prática faz parte do funcionamento do capitalismo e que não estaríamos diante de um novo capitalismo, pois é uma lógica de crescimento para todas as empresas.

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

No entanto, este trabalho parte do pressuposto de que o direito à personalidade não é um bem pessoal absoluto, tratando-se de um direito fundamental que deve ser garantido pelo Estado, mas que pode ser relativizado, em situações excepcionais, em que garanta a proteção do direito à privacidade, que assume uma dimensão coletiva.

Para Doneda (2019), apesar de reconhecer o direito à privacidade como uma espécie de direito fundamental, com a sua conseqüente funcionalização, é admissível decompô-lo numa série de direitos subjetivos, como o direito à vida privada e familiar, mas também o direito à proteção dos dados pessoais.

Segundo o autor, a proteção dos dados pessoais ultrapassa a esfera individual para ganhar uma dimensão coletiva, “através do reconhecimento dos dados pessoais como um instrumento adequado ao controlo político dos indivíduos e suscetível de ser utilizado para discriminar grupos minoritários” (DONEDA, 2019, p. 46).

Schertel (2014) discorre sobre a grande discussão de se garantir um direito de propriedade sobre os dados pessoais diante desse grande ativo que vem sendo adquirido pelas

Big Techs e, sobretudo, a necessidade de se coibir os potenciais danos da mercantilização do direito de personalidade e, conseqüentemente dos direitos fundamentais.

Mas o objeto a ser destacado não é o indivíduo como pessoa natural, mas o cidadão dentro de uma ordem democrática de direito, dotado de uma personalidade jurídica ampla e complexa, como consumidor com seus direitos metaindividuais e como sujeito político com autonomia, especialmente dentro de um Estado democrático de direito em que a violação de dados prejudica diretamente o aspeto coletivo do grupo social, devido à restrição direta ao seu direito de liberdade.

A privacidade assume, assim, uma posição de destaque na proteção da pessoa humana, não apenas tomada como escudo contra o mundo 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 em geral. Este papel, é pressuposto de uma sociedade democrática moderna, da qual o dissenso e o anticonformismo são componentes orgânicos (DONEDA, 2019, p. 128-129)

Não há que confundir a liberdade econômica do liberalismo com a liberdade do Estado social de direito, como bem assinala Noberto Bobbio (1993) O que está a ser prejudicado pela manipulação massiva de dados e pelo direito à informação é a própria democracia e o Estado não pode abster-se de agir em nome do capital. Nesse sentido, Doneda (2019, p.128-129) ensina que.

“... com as novas tecnologias e os novos mecanismos de controlo e transmissão de informação teria surgido um sentido positivo de privacidade, que exigia a disponibilização aos seus titulares de mecanismos eficazes para a construção de uma esfera privada na qual pudessem desenvolver plenamente a sua personalidade”.

O artigo é desenvolvido com o objetivo de trabalhar o cidadão na ordem democrática de direito, exigindo do Estado uma atuação que garanta efetivamente o direito à privacidade, que assume um complexo feixe relacional.

Numa órbita capitalista utilitarista, o consumidor torna-se o principal ator desse sistema, o que reduz o papel do Estado em favor do mercado e das garantias da lei. As próprias mutações do capitalismo levam a uma supressão de direitos efetivos e acabam por sustentar posições como a de Batkins (2019), que quer precificar os dados como uma nova mercadoria, retirando a subjetividade do direito à intimidade, que também se desdobra na proteção de dados pessoais, seja por agentes públicos ou privados.

Vale mencionar algumas considerações importantes do STF, no julgamento da medida cautelar na ação direta de inconstitucionalidade 6 389, do Distrito Federal, ajuizada contra o inteiro teor da Medida Provisória 954, de 17 de abril de 2020, em que a relatora foi a Ministra Rosa Weber. A Cautelar tratou do compartilhamento de dados pelas empresas de telecomunicações prestadoras do Serviço Telefônico Fixo Comutado e do Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de apoio à produção estatística oficial durante a emergência de saúde pública de importância internacional decorrente do coronavírus (covid19), que tratava da Lei nº 13 979, de 6 de fevereiro de 2020.

Embora a relatora tenha entendido que a norma, no caso, era formalmente inconstitucional, analisou a questão material e o papel do Estado em relação aos direitos fundamentais de proteção de dados, uma vez que, à época, o texto constitucional era omissivo sobre o tema e havia precedente anterior do STF sobre o direito à privacidade não exigir atuação positiva do Estado.

Esse voto se tornou uma grande mudança de paradigma, tendo em vista que o direito à privacidade já havia 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 não ter havido quebra de sigilo das comunicações de dados, mas apenas a apreensão da base física em que os dados estavam armazenados, não exigindo a atuação 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 e imutável em relação às transformações futuras, e uma constituição que muda e se transforma com as exigências do futuro. A questão é que uma constituição que não é transformadora, segundo o autor, não é capaz de proteger os direitos fundamentais no futuro, como no caso das mudanças decorrentes da própria tecnologia e da invasão do espaço privado dos indivíduos. A norma não consegue acompanhar as incessantes transformações a que o indivíduo está sujeito, principalmente no que diz respeito aos abusos de determinados poderes específicos. Nesse caso, deve-se permitir uma interpretação que adapte as normas às constantes mutações do mundo moderno, principalmente se considerarmos o mundo digital.

Nesse sentido, o autor cita o caso do juiz Louis Brandeis, em 1928, nos Estados Unidos, em que se discutiu a Quarta Emenda. Apesar de ter sido o voto vencido no caso específico que

interpretava a Constituição norte-americana, o juiz acreditava que a norma que protegia os abusos deveria se adaptar às mudanças da sociedade. No caso da Constituição de 1988, as transformações digitais ainda eram incipientes no Brasil, que não tinha o poder de promover uma grande transformação, nem tinha um alcance tão expressivo, e dependia de uma visão prospectiva do Supremo Tribunal Federal, por meio da Ministra Rosa Weber.

Posteriormente, a Emenda Constitucional 115/2022, de 10 de fevereiro do mesmo ano, alterou a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e estabelecer a competência exclusiva da União para legislar sobre proteção e tratamento de dados pessoais. Essa emenda consolida materialmente a proteção de dados como um direito fundamental.

III. POLÍTICAS PÚBLICAS PARA O CIDADÃO CONSUMIDOR

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

Sobre os direitos do consumidor, a Organização das Nações Unidas, em 1985 e revisto em 1999 e 2015, estabeleceu diretrizes para os “consumidores” e classificou seus direitos como um direito humano de nova geração. No Brasil, a Constituição de 1988 previu a criação de uma legislação consumerista e deu um prazo de 180 dias para a elaboração do código, que só veio a acontecer em 1990, o que foi considerado um grande avanço no ordenamento jurídico brasileiro, criando um direito misto, entre público e privado com função social, ou seja, direito privado solidário dentro de uma sociedade capitalista. Surgiu durante o surgimento do Estado neoliberal no Brasil e tem como objetivo proteger os mais fracos e vulneráveis com preceitos de ordem pública que tratam da igualdade material.

No entanto, mais de 30 anos após a entrada em vigor do Código de Defesa do Consumidor, o Brasil apresenta uma enorme lacuna diante do capitalismo digital, pois ainda possui preceitos voltados para o capitalismo industrial e o consumo de massa. Não há no Código de Defesa do Consumidor legislação referente à proteção de dados do consumidor, contratos digitais, proteção de informações sobre crianças e idosos devido à sua hiper vulnerabilidade e preceitos ou questões referentes à inteligência artificial, o que torna o tema extremamente relevante (MARQUÊS, 2022).

As atividades realizadas na internet foram inicialmente regulamentadas pela Lei 12.695/2014, conhecida como Marco Civil da Internet, e posteriormente pela Lei 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD). Somente no dia 28/10/21, a Diretoria da ANPD deliberou pela aprovação do Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador. Aprovado por unanimidade, o regulamento teria como principal objetivo fomentar uma cultura de proteção de dados no país.

Embora não exista legislação específica sobre a proteção de informações de crianças, a Diretoria da Autoridade Nacional de Proteção de Dados (ANPD), no exercício dos poderes normativos estabelecidos pelo art. 55-J, XX, da Lei n. 55-J, XX, da Lei nº 13.709, de 14 de agosto de 2018; pelo art. 2º, XX, do Decreto nº 10.474, de 26 de agosto de 2020; e pelos arts 5º, IX, e 51, parágrafo único, do Regimento Interno da Autoridade Nacional de Proteção de Dados, aprovado pela Portaria nº 1, de 8 de março de 2021, emitiu manifestação com força normativa, no seguinte sentido:

“O tratamento de dados pessoais de crianças e adolescentes poderá ser realizado com base nas hipóteses legais previstas no art. 7 ou art. 11 da Lei Geral de Proteção de Dados Pessoais (LGPD), desde que observado e prevalecendo o seu melhor interesse, a ser aferido no caso concreto, nos termos do art. 14 da Lei”.

Isso demonstra que o Brasil vem adotando medidas desde 2021, com a entrada em vigor do Regulamento da ANPD, para não apenas normatizar, mas também fiscalizar o tratamento e a proteção de dados dos consumidores, diante de inúmeras violações perpetradas. Embora a ANPD tenha sido criada como uma autarquia especial vinculada à Presidência da República, ela está subordinada ao Ministério da Justiça e Segurança Pública desde 2022.

A empresa TikTok recebeu uma denúncia do deputado federal Filipe Barros (PSL/PR) sobre sua análise do tratamento de dados pessoais e compartilhamento de dados com o Facebook de usuários do aplicativo, mesmo que não tenham se cadastrado na plataforma. O assunto foi encaminhado à ANPD, que notificou o TikTok. Em resposta, a ByteDance Brasil esclareceu que é uma empresa brasileira, com sede no Brasil, mas que não opera diretamente a plataforma TikTok. A empresa responsável pela operação da rede social seria a TikTok Pte Ltd, uma empresa sediada em Singapura.

Em resposta, a ByteDance Brasil não diferenciou o tratamento de dados pessoais com base na idade. Atualmente, a política de privacidade apenas especifica o tratamento de dados de adolescentes para indicar que não trata dados de crianças, o que não é suficiente para dar

transparência sobre as funcionalidades disponíveis para os perfis de adolescentes pela sua rede social ao se cadastrarem na plataforma, especialmente sobre dados sensíveis.

Embora a ByteDance Brasil tenha afirmado que sua plataforma não aceita menores de 13 anos, não havia políticas de segurança para impedir o cadastro ou acesso desses usuários e não havia políticas claras quanto ao tratamento de adolescentes entre 13 e 18 anos (Nota Técnica nº 6/2023/CGF/ANPD- SEI 00261.000297/2021-75).

A atuação da ANPD segue um modelo de regulação responsiva, em que mecanismos sancionatórios, como advertências e multas, são utilizados nos casos em que o agente não segue os mecanismos de orientação. No entanto, o regulamento sobre a aplicação de sanções administrativas só foi publicado em 27 de fevereiro de 2023.

A empresa WhatsApp também sofreu reclamações de usuários e autoridades internacionais devido ao compartilhamento de dados dentro do grupo com a empresa Facebook Serviços Online do Brasil Ltda. Mas, quando a ANPD exerceu sua regulação e exigiu o cumprimento das recomendações feitas com base na Nota Técnica nº 2/2021 (2461963), o WhatsApp se disse impossibilitado de cumprir devido à falta de base legal para informar na atual política de privacidade a categoria dos dados pessoais e a finalidade a que se destinam.

Como os usuários/consumidores poderão defender seus direitos diante da violação dos princípios básicos do Código de Defesa do Consumidor, como a boa-fé objetiva e da autodeterminação informativa, previstos na LGPD. Como a autoridade reguladora irá verificar o cumprimento da lei?

O que parece ser um serviço gratuito à disposição do consumidor torna-se um produto a ser comercializado. Quando o consumidor fornece seus dados ao WhatsApp, ele não sabe para qual finalidade eles serão transferidos, armazenados ou compartilhados com o mesmo grupo ou terceiros e quais dados serão compartilhados, já que isso não fica claro na política de privacidade.

Segundo a ANPD, “as categorias de dados pessoais são apresentadas em uma lista ‘Dados que coletamos’ e as finalidades em outra”, o que dificulta o controle, a fiscalização tanto por parte do usuário consumidor quanto do ponto de vista regulatório, dificultando a verificação do cumprimento da lei por esta Autarquia. Neste sentido, a Autoridade salienta:

Sem uma maior transparência quanto às categorias de dados que são tratados e para que finalidades, não é possível identificar quais os dados pessoais que

são partilhados com outras empresas do grupo económico do Facebook, sendo de presumir o pior cenário (i.e., a partilha de todas as categorias de dados pessoais), caso em que nem a execução contratual nem o interesse legítimo justificariam essa partilha. Este cenário parece ser confirmado pelas informações fornecidas pelo WhatsApp no seu Centro de Ajuda (SEI/PR - 2675286 - Nota Técnica/49/2022).

Aqui, o consentimento deve ser analisado especificamente como um processo decisório, e não como um ato pontual de declaração de vontade do titular a ponto de violar o consentimento válido (BIONI, 2020). Neste caso, estar-se-ia perante um consumidor com vulnerabilidade técnica e económica, o que significa que este consentimento não pode ser tratado como um mero ato de vontade, baseado no *pacta sunt servanda*, com carácter negocial voluntário. Isso só reforçaria o carácter de propriedade e de mercadoria dos dados.

A sua natureza jurídica deve ser procurada como um atributo da personalidade jurídica, a fim de gerar uma esfera de proteção eficaz para o consumidor, baseada no princípio da boa-fé objetiva e da transparência. Para que o consentimento do consumidor seja válido, no caso da transferência de informações de empresas do mesmo grupo, haveria a necessidade de se observar o consentimento consciente dos dados e o princípio da finalidade (SCHERTEL, 2014).

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

O princípio da autodeterminação informativa não permite que dados e informações sejam coletados a ponto de reduzir ou manipular a capacidade de compreensão do sujeito ou mesmo suas escolhas, a ponto de ferir sua privacidade geral e restringir seu direito à liberdade. Mas o que é que permite à Bigh Techs contornar o princípio da autodeterminação dos dados?

Esta técnica de monitorização através dos dados dos consumidores que são incorporados na rede chama-se *profiling*, em que através de algoritmos os dados são armazenados e direcionados, em que apesar da autonomia do consumidor em querer partilhar os seus dados, estes são monitorizados, limitando a sua liberdade de escolha. É criado um monopólio digital sobre a informação a que os consumidores têm acesso. Nesse sentido: “os algoritmos indicam

quais conteúdos serão consumidos primeiro, quais serão os mais adequados para cada indivíduo e, dessa forma, limitam o acesso à informação” (BEÇAK; LONGHI, 2020).

Um caso empírico que demonstrou essa questão no Brasil foi quando o Google tentou coibir a participação popular no Projeto de Lei das Fake News (PL 2630), conhecido como Projeto de Lei da Transparência (PL 2768/2022), que ainda tramita no Congresso Nacional. O Google decidiu agir com informação massiva contra o projeto de lei para coibir as “fakes news”, que impactam diretamente o exercício dos direitos democráticos, porque não queria ter nenhuma interferência do Estado em suas atividades.

Começou uma verdadeira batalha contra o Projeto de Lei 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 ele restringe e exige transparência, o que deixa os consumidores vulneráveis aos interesses das Big Techs e seus lucros (UFRJ, NETLAB, 2023).

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

As políticas públicas desenvolvidas em um Estado Democrático de Direito dependem de um arcabouço jurídico que legitime seus agentes políticos e públicos, bem como as respectivas instituições e a sociedade a exercerem seus direitos, como no caso acima.

Atualmente tramita no Congresso Nacional o Projeto de Lei 2338/2023, 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, o qual é de extrema importância que seja aprovado o quanto antes, tendo em vista o avanço da tecnologia digital em termos de responsabilidades e limites para o capital digital, principalmente no que tange ao compartilhamento de dados.

De acordo com o Projeto de Lei 2328/2023, há a necessidade de se estabelecer um Relatório de Impacto à Proteção de Dados Pessoais (RIPD), a fim de mapear e alertar a sociedade sobre eventuais problemas que possam surgir, medidas de governança preventiva que já foram adotadas pela ANPD em seus pareceres e que ainda sofrem alguma resistência dos atores econômicos, como no caso do WhatsApp.

O Projeto de Lei 2338/2023 introduz a ideia de uma avaliação de impacto algorítmico, que visa compreender e mitigar os riscos associados ao uso de sistemas de IA, especialmente aqueles classificados como de alto risco, que no Código de Defesa do Consumidor sequer são permitidos no mercado, conforme o art. 8º da Lei 8078/90.

IV. CONCLUSÃO

Em todos esses casos apresentados, o Estado se tornou um ator essencial, primeiro ao interpretar a Constituição de forma a adequar os direitos fundamentais às mudanças sociais; segundo, ao criar limites à ordem econômica e aos direitos do consumidor por meio de políticas regulatórias; e terceiro, ao promover, por meio de políticas públicas, uma autoridade com poderes normativos, informativos e regulatórios para tornar a proteção de dados um direito fundamental, reconhecido como um direito geral à privacidade que garante ao cidadão sua plena liberdade de escolha, decisão e informação.

O que se vislumbrou foi que com o avanço do capitalismo digital é que, embora se apresente como uma solução de mercado e de bem-estar econômico, não pode ser associado à liberdade material, pois a sua liberdade sempre esteve associada à preservação dos meios de produção, e não às garantias sociais. O Estado deve estar atento à produção de políticas públicas contra o poder invisível dos algoritmos para que não ceda aos oligopólios de poder e atenda aos interesses sociais.

O trabalho de aprimoramento da ANPD com a implementação de uma governança regulatória possibilitará uma maior atuação do consumidor, aumentando os canais de acesso e segurança, além de gerar políticas públicas que deem transparência em relação ao compartilhamento de dados privados, a fim de coibir os abusos perpetrados pelas Big Techs, como foi analisado nos casos concretos do TikTok, WhatsApp e Google

É cada vez mais necessária uma maior governança por parte do Estado, sobretudo em termos de regulação, mas também uma maior fiscalização através de órgãos e instituições capazes de travar o poder dos grandes conglomerados económicos, que atentam contra os consumidores enquanto utilizadores de produtos, a sua liberdade e o acesso à democracia.

REFERÊNCIAS

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.

BATKINS, Sam. (2019), “The Tech Giants Are Out to Get You”. Regulation, 52, Summer: 52-53.

BOBBIO, Norberto. O futuro da democracia; uma defesa das regras do jogo; tradução de Marco Aurélio Nogueira. Rio de Janeiro: Paz e Terra, 1986.

BRASIL. ANPD- AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Nota Técnica nº 6/2023/CGF/ANPD- SEI 00261.000297/2021-75. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/tiktok-nota_tecnica_6_versao_publica_ret-1.pdf. 02 ago. 2023.

BRASIL. ANPD- AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. (SEI/PR - 2675286 - Nota Técnica nº 49_2022). Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/nt_49_2022_cfg_anpd_versao_publica.pdf. 02 ago. 2023.

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. Projeto de Lei 2338/2023. Iniciativa Senador Rodrigo Pacheco (PSD/MG). Dispõe sobre o uso da Inteligência Artificial, disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=9347622&ts=1720545987618&disposition=inline>. Acesso em: 02 ago. 2023.

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/ptbr/assuntos/noticias/conselho-diretor-aprova-o-regulamento-do-processo-defiscalizacao-e-do-processo-administrativo-sancionador-no-ambito-da-autoridadenacional-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.

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.

MARQUÊS.

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

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

THORNHILL, John. (2019), “We Must Train the Capitalist Algorithm Ourselves”. *Financial Times*, 11 fev. (Opinion). Disponível em: <<https://www.ft.com/content/2db2cdb4-2dda-11e9-8744-e7016697f225>>.

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.