CONFLUÊNCIAS | Artigo

ISSN:
ISSN: 1678-7145 | E-ISSN: 2318-4558
Volume 25, Número 1, abril. de 2023.

CAPITALISMO DE VIGILÂNCIA E A LEI GERAL DE PROTEÇÃO DE DADOS NA ERA DA INFORMAÇÃO

Milena Cereser da Rosa
Universidade Regional do Noroeste do Estado do Rio Grande do Sul (UNIJUÍ)

Joice Graciele Nielsson
Universidade Regional do Noroeste do Estado do Rio Grande do Sul (UNIJUÍ)

Resumo

O artigo busca compreender o termo "capitalismo de vigilância" referido pela autora norte-americana Shoshana Zuboff em suas pesquisas e analisar a Lei Geral de Proteção de Dados (LGPD) como regulamento limitador (ou não) ao acesso pelas grandes empresas aos dados sensíveis dos titulares. O problema que orienta a pesquisa pode ser sintetizado na seguinte pergunta: Em que medida a Lei Geral de Proteção de Dados pode ser utilizada como instrumento limitador para combater o capitalismo de vigilância? O objetivo geral do texto consiste em analisar a Lei Geral de Proteção de Dados (LGPD) a partir da compreensão do termo "capitalismo de vigilância". Os objetivos específicos do texto, que se refletem na sua estrutura em duas seções, são: a) compreender o termo "capitalismo de vigilância" e sua dinâmica de aplicabilidade; b) analisar a Lei Geral de Proteção de Dados (LGPD) como marco normativo brasileiro referente a proteção de dados digitais; e, c) verificar se a Lei Geral de Proteção de Dados (LGPD) age como instrumento limitador ao capitalismo de vigilância. Pode-se concluir que a Lei Geral de Proteção de Dados (LGPD) é um marco normativo brasileiro que garante a defesa dos direitos privados e fundamentais referente aos dados pessoais dos usuários, todavia, ainda não é um instrumento eficaz e limitador para combater o capitalismo de vigilância. O método de pesquisa empregado foi o hipotético-dedutivo, mediante o emprego de técnica de pesquisa bibliográfica.

Palavras-chave: Capitalismo de vigilância. Lei Geral de Proteção de Dados. Privacidade.

SURVEILLANCE CAPITALISM AND THE GENERAL PERSONAL DATA PROTECTION LAW IN THE INFORMATION AGE

Abstract

The article seeks to understand the term "surveillance capitalism" referred to by the American author Shoshana Zuboff in her research and to analyze the General Data Protection Law (LGPD) as a regulation that limits (or not) access by large companies to sensitive data from holders. The problem that guides the research can be summarized in the following question:

To what extent can the General Data Protection Law be used as a limiting instrument to combat surveillance capitalism? The general objective of the text is to analyze the General Data Protection Law (LGPD) from the understanding of the term “surveillance capitalism”. The specific objectives of the text, which are reflected in its structure in two sections, are: a) to understand the term “surveillance capitalism” and its dynamics of applicability; b) analyze the General Data Protection Law (LGPD) as a Brazilian regulatory framework regarding the protection of digital data; and, c) verify if the General Data Protection Law (LGPD) acts as a limiting instrument to surveillance capitalism. It can be concluded that the General Data Protection Law (LGPD) is a Brazilian normative framework that guarantees the defense of private and fundamental rights regarding users' personal data, however, it is still not an effective and limiting instrument to combat surveillance capitalism. The research method used was the hypothetical-deductive, through use of a bibliographic research technique.

Keywords: Surveillance capitalism. General Data Protection Act. Privacy.

INTRODUÇÃO

Tanto no Brasil, quanto no mundo, o avanço tecnológico tem atingido significativamente a vida das pessoas através da incorporação cada vez mais ampla de novas tecnologias postas à serviço da sociedade e das instituições. Diante da relevância e atualidade deste tema, o artigo busca compreender o termo “capitalismo de vigilância” referido pela autora norte-americana Shoshana Zuboff em suas pesquisas e analisar a Lei Geral de Proteção de Dados (LGPD) como regulamento limitador (ou não) ao acesso pelas grandes empresas aos dados sensíveis dos titulares.

A partir desse cenário, muitas são as incertezas que essa expansão tecnológica tem causado, especialmente no que tange aos limites possíveis frente aos princípios constitucionais e aos direitos humanos. Nesse sentido, o problema que orienta a pesquisa pode ser sintetizado na seguinte pergunta: Em que medida a Lei Geral de Proteção de Dados pode ser utilizada como instrumento limitador para combater o capitalismo de vigilância?

Como hipótese inicial, com base nos dados levantados a partir de um conjunto de pesquisas realizadas sobre o tema, podemos verificar que a Lei Geral de Proteção de Dados (LGPD) é uma normativa baseada nas regulações europeias e que constituiu, no Brasil, um marco normativo referente aos dados digitais.

Como objetivo geral, o texto consiste em analisar a Lei Geral de Proteção de Dados (LGPD) a partir da compreensão do termo "capitalismo de vigilância". Os objetivos específicos do texto, que se refletem na sua estrutura em duas seções, são: a) compreender o termo "capitalismo de vigilância" e sua dinâmica de aplicabilidade; b) analisar a Lei Geral de Proteção de Dados (LGPD) como marco normativo brasileiro referente a proteção de dados digitais; e, c) verificar se a Lei Geral de Proteção de Dados (LGPD) age como instrumento limitador ao capitalismo de vigilância.

O método de pesquisa empregado foi o hipotético-dedutivo, que tem embasamento no pensamento de Karl Popper, tendo em vista que a pesquisa inicia com a constatação da existência do capitalismo de vigilância na era da informação, o qual tem como instrumento limitador a Lei Geral de Proteção de Dados (LGPD). Nesse sentido, partiu-se da hipótese que a Lei Geral de Proteção de Dados (LGPD) é um marco legislativo brasileiro, referente aos dados digitais, e trata-se de um regulamento que limita o avanço desenfreado do capitalismo de vigilância (POPPER, 1975).

1. A COMERCIALIZAÇÃO DE DADOS A PARTIR DO CAPITALISMO DE VIGILÂNCIA

Os avanços tecnológicos estão presentes cada vez mais na vida dos indivíduos. Casas automatizadas, celulares com diversas funcionalidades, computadores de última geração. Basta apenas um segundo e com um clique se obtêm infinitas informações acerca de um assunto. A humanidade vive a era da informação.

Na obra de autoria de Shoshana Zuboff, intitulada *A Era do Capitalismo de Vigilância: a luta por um futuro humano na nova fronteira do poder*, são apresentados os riscos que o fenômeno do capitalismo de vigilância ameaça impactar a humanidade no século XXI, tendo em vista a realização do tratamento de informações pessoais de maneira comercial.

Os atentados ocorridos em 11 de setembro de 2001, na cidade de Nova York (Estados Unidos), fizeram com que o governo americano ignorasse as questões relativas à

privacidade e proteção de dados pessoais dos indivíduos, utilizando-se do pretexto de prezar pela segurança dos cidadãos e combate ao terrorismo.

Tendo em vista a instauração dessa "conjuntura política, econômica e tecnológica, alicerçada em um modelo extremamente neoliberal de regulação" (MEIRELES, 2021, p. 31), que possibilitou as condições necessárias para a configuração do que Shoshana Zuboff denominou "capitalismo de vigilância".

O fenômeno do capitalismo de vigilância trata-se de uma mutação do capitalismo da informação, ou seja, a partir da expansão das tecnologias digitais decorrentes do modelo de sucesso dos produtos da Apple, no início dos anos 2000 e, pelas grandes empresas de tecnologia do Vale do Silício, surgiram no final do século XX as condições necessárias para uma chamada terceira modernidade, a qual estava voltada para o indivíduo, tendo como foco a realização dos valores e expectativas do sujeito (ZUBOFF, 2020).

Na terceira modernidade existe a fusão do capitalismo com o mundo digital, trazendo a ilusão de que o sujeito pode viver da forma que quiser, pagando um preço para isso. Para tanto, já no século XXI, o capitalismo de vigilância sequestra os hábitos dos sujeitos, comportamentos, likes e todos os rastros que deixam espalhados ao longo do percurso online. Estes dados que foram "sequestrados", serão convertidos para que possam ser vendidos às empresas que têm interesse nestas informações (ZUBOFF, 2020).

Assim, o objetivo das empresas em adquirir os dados dos usuários é para direcionar seus anúncios, de forma a manipular os sujeitos e tornar o produto mais atrativo para o consumo. Essa "dinâmica competitiva desses novos mercados leva os capitalistas de vigilância a adquirir fontes cada vez mais preditivas de superávit comportamental: nossas vozes, personalidades e emoções" (ZUBOFF, 2020, p. 19).

O capitalismo de vigilância está sempre à "espreita" para sanar as necessidades dos sujeitos. Porém, quando essa suposta necessidade é atendida, também é o momento em que os dados comportamentais do indivíduo são retirados para viabilizar o lucro das grandes empresas.

A partir da visão de que os usuários das tecnologias são apenas objetos/produtos para gerar lucro às grandes empresas, percebe-se a ausência de reciprocidade estrutural entre estas empresas e a sociedade. As companhias que participam desse "esquema" se separam da

narrativa histórica das democracias de mercado ocidentais, sendo que "a premissa-chave do extrativismo de dados é a de que os usuários são estoques de informações valiosas" (MOROZOV, 2018, p. 165).

Para o capitalismo de vigilância, os usuários são apenas os objetos de uma espécie de extração de matéria-prima de tecnologia avançada, ou seja, os indivíduos são o mero objeto de mercado do capitalismo de vigilância. Sendo assim, "os verdadeiros clientes do capitalismo de vigilância são as empresas que negociam nos mercados de comportamento futuro" (ZUBOFF, 2020, p. 22).

Nesse contexto, o fenômeno do capitalismo de vigilância encontrou espaço para o neoliberalismo imperar, tendo em vista o ambiente tecnológico não ter limites e as regulamentações serem precárias no mundo digital.

Todavia, diferentemente do estado totalitário simbolizado por George Orwell, na obra 1984, a tecnologia digital está presente em todos os lugares para atender aos interesses do capitalismo de vigilância, forma de poder esta que é caracterizada pela máxima concentração de conhecimento obtido silenciosamente e que não passa pela supervisão da democracia.

Por outro lado, o capitalismo de vigilância não deve ser entendido somente através da perspectiva da ação econômica, muito pelo contrário, "as consequências da nova lógica de acumulação já vazaram e continuam a vazar para além das práticas comerciais, penetrando na estrutura das relações sociais [...]" (ZUBOFF, 2020, p. 396).

Existe uma perversidade no discurso daqueles que representam as grandes empresas de tecnologia, os quais não revelam a real intenção no enorme interesse pelos dados pessoais dos sujeitos. Visando sempre o lucro, essas empresas manipulam os indivíduos de forma a eliminar a autonomia e livre vontade destes.

Dessa forma, a relação dos usuários com os detentores do poder (grandes empresas) é apenas indireta nos mercados futuros de comportamento, sendo que essa sistemática de funcionamento representa um perigoso divórcio entre a população, e as elites econômicas, as quais não têm interesse em responder aos seus apelos e demandas. Nessa lógica, a reciprocidade entre esses dois polos é enfraquecida, o que contribui para que o capitalismo de vigilância seja uma força social profundamente antidemocrática (ZUBOFF, 2020).

Nessa dinâmica de produto e consumidor, a autora Shoshana Zuboff (2020, p. 429) refere: "Esqueça o clichê que afirma que, se é de graça, 'o produto é você'. Você não é o produto; você é a carcaça abandonada. O 'produto' deriva do superávit arrancado da sua vida". Ou seja, no capitalismo de vigilância a experiência humana privada nada mais é do que uma mercadoria deste novo modelo econômico.

Os capitalistas de vigilância perceberam que podiam fazer qualquer coisa que quisessem no mundo virtual, o que de fato aconteceu. Apresentam sempre a justificativa de aprimoramento dos serviços e a defesa da privacidade dos usuários, porém, deixam escondido nos bastidores a verdadeira ação.

Sendo assim, os detentores de poder que se utilizam do capitalismo de vigilância para gerar lucro, escondem a real intenção das suas ações com discursos "democráticos", como temos o exemplo na afirmação de Mark Zuckerberg: "privacidade é o futuro"[1]. Essa afirmação faz com que os usuários tenham a falsa noção de "segurança" por aquele que está por trás do comando da rede social mais utilizada no mundo.

Acerca disso, no ano de 2018 surge o escândalo *"Cambridge Analytica-Facebook"*[2] que foi divulgado pelos jornais *New York Times* e *The Guardian* sobre a coleta de informações e dados de milhões de usuários da rede social *Facebook* pela empresa *Cambridge Analytica*[3]. Estes dados foram obtidos sem consentimento dos usuários e tiveram significativo impacto em várias eleições presidenciais no mundo.

Portanto, percebe-se que nas últimas duas décadas o capitalismo de vigilância teve um espaço totalmente livre e praticamente sem a interferência de leis ou quaisquer regulamentos. Aos olhos da autora Shoshana Zuboff, a democracia dormiu enquanto as grandes empresas acumularam conhecimento e poder sem precedentes, além da maximização

[1] Informação obtida em: https://gizmodo.uol.com.br/facebook-privacidade-futuro-f8-2019/. Acesso em: 03 jan. 2022.

[2] Reportagem sobre o caso disponível em: https://g1.globo.com/economia/tecnologia/noticia/entenda-o-escandalo-de-uso-politico-de-dados-que-derrubou-valor-do-facebook-e-o-colocou-na-mira-de-autoridades.ghtml. Acesso em: 03 jan. 2022.

[3] A empresa *Cambridge Analytica* foi fundada no ano de 2013 como uma subsidiária do *SCL Group*, a qual combinava mineração e análise de dados com comunicação estratégica para processos eleitorais. Após o escândalo que veio à tona em 2018, a empresa solicitou em juízo a decretação de falência. Informação obtida em: https://pt.wikipedia.org/wiki/Cambridge_Analytica. Acesso em 03 jan. 2022.

dos lucros. Por isso da necessidade de limitar esse poder desenfreado do capitalismo de vigilância.

2. CONSIDERAÇÕES SOBRE A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

Após o escândalo da *Cambridge Analytica-Facebook*, pairou sobre as pessoas certa dúvida e insegurança acerca da privacidade do mundo virtual. Surge então o debate em torno da necessidade de proteção dos dados pessoais dos indivíduos.

Nesse sentido, tornou-se em evidência o Regulamento Geral de Proteção de Dados da União Europeia (RGPD) nº2016/679[4], com entrada em vigor em 25 de maio de 2018, o qual tinha como objetivo preparar a Europa para a era digital, porém assegurando proteção aos usuários.

Ainda, sob essa perspectiva de proteger os dados pessoais, a Carta dos Direitos Fundamentais da União Europeia[5] também trouxe em seu texto essa garantia, ou seja, menciona que todos os cidadãos europeus têm direito à proteção dos seus dados pessoais. Para tanto, corroborando nesse aspecto, o Regulamento Geral sobre a Proteção de Dados (RGPD) da União Europeia reforça os direitos fundamentais dos indivíduos na era digital, facilitando a atividade comercial mediante a aplicação de algumas normas às empresas, bem como, às instituições públicas no mercado digital.

Com efeito, é perceptível a preocupação da União Europeia em garantir a segurança e a proteção de dados pessoais daqueles indivíduos que se encontram em território Europeu, ou que, têm seus dados tratados por empresas ali constituídas. Nota-se o interesse legislativo em garantir a privacidade do usuário e a transparência no tratamento de seus dados.

Por outro lado, no Brasil temos garantido no artigo 5º, inciso X, da Constituição Federal de 1988[6], a inviolabilidade à intimidade e à vida privada. Tais direitos sustentam sua

[4] Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 16 jan. 2022.

[5] Disponível em: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf. Acesso em: 16 jan. 2022.

[6] Artigo 5º [...] X – são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; [...] XII – é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou

distinção na doutrina e jurisprudências alemãs, principalmente no que se refere a teoria das esferas e dos círculos concêntricos.

As referidas teorias mencionam, em suma, que a privacidade é composta por esferas, as quais determinam qual o grau de interferência externa que o sujeito suporta. Para tanto, define-se o círculo externo como "esfera privada"; círculo intermediário como "esfera da intimidade ou da confidência"; e, círculo interno como "esfera do sagrado" (COSTA JR., 1970).

Nesse sentido, a esfera privada engloba as esferas da intimidade e do segredo (sigilo), o que demonstra o quão abrangente este campo se torna. Todavia, quanto mais se adentra nas esferas, maior e mais intensiva deve ser a proteção jurídica desta, o que demonstra a relevância do debate em torno da proteção de dados pessoais no mundo informacional em que se vive.

Além da Constituição Federal de 1988 trazer em seu texto a inviolabilidade à intimidade e à privacidade, existem outras legislações brasileiras que também referiam brevemente sobre a proteção aos dados pessoais, como por exemplo: Código de Defesa do Consumidor (Lei nº 8.078, de 11 de setembro de 1990)[7]; Lei do Cadastro Positivo (Lei nº12.414, de 9 de junho de 2011)[8]; e, Marco Civil da Internet (Lei nº 12.965, de 23 de abril de 2014)[9].

---

instrução processual penal; [...] LXXII - conceder-se-á *"habeas-data":* a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público; b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo. [...] Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 16 jan. 2022.

[7] Artigo 43 O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes. §1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos. §2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele [...]. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 16 jan. 2022.

[8] Artigo 5º São direitos do cadastrado: I - obter o cancelamento ou a reabertura do cadastro, quando solicitado; II - acessar gratuitamente, independentemente de justificativa, as informações sobre ele existentes no banco de dados, inclusive seu histórico e sua nota ou pontuação de crédito, cabendo ao gestor manter sistemas seguros, por telefone ou por meio eletrônico, de consulta às informações pelo cadastrado; III - solicitar a impugnação de qualquer informação sobre ele erroneamente anotada em banco de dados e ter, em até 10 (dez) dias, sua correção ou seu cancelamento em todos os bancos de dados que compartilharam a informação; IV - conhecer os principais elementos e critérios considerados para a análise de risco, resguardado o segredo

Diante da relevância do tema e a necessidade em legislar especificamente sobre a proteção de dados pessoais em território brasileiro, surge então a chamada Lei Geral de Proteção de Dados (LGPD), a qual foi instituída através do nº13.709, de 14 de agosto de 2018, e que teve como base o Regulamento Geral de Proteção de Dados da União Europeia (RGPD).

Sendo assim, a Lei Geral de Proteção de Dados teve como objetivo abranger "tanto o dado em sentido estrito quanto a informação obtida, na medida em que o desiderato principal da lei é a proteção de direito fundamental ligado à personalidade, à intimidade e privacidade" (BOTELHO, 2020, p. 206).

Embora o Brasil já possua algumas legislações que tratam (genericamente) sobre a proteção de dados, com a entrada em vigor da Lei Geral de Proteção de Dados, tem-se uma regulamentação específica que trata sobre o uso, a proteção e a transferência de dados pessoais. Ainda, outro aspecto importante é a delimitação das figuras envolvidas e quais são suas responsabilidades, atribuições e possíveis penalidades na esfera civil.

Em relação à aplicabilidade da Lei Geral de Proteção de Dados, a operação de tratamento dos dados deve ser realizada por pessoa natural ou por pessoa jurídica, seja pública ou privada. Percebe-se que o foco da legislação está em proteger os dados pessoais do usuário, ficando em segundo plano quem produz o tratamento destes dados.

Visando proteger os direitos fundamentais, a LGPD, em concordância com o texto constitucional brasileiro, traz no artigo 2º os seguintes fundamentos da norma: I- respeito à privacidade; II- autodeterminação informativa; III- liberdade de expressão, de informação, de comunicação e de opinião; IV- inviolabilidade da intimidade, honra e imagem; V- desenvolvimento econômico, tecnológico e a inovação; VI- livre iniciativa, livre concorrência e a defesa do consumidor; e, VII- direitos humanos, livre desenvolvimento da personalidade, dignidade e o exercício da cidadania pelas pessoas naturais.

---

empresarial; V - ser informado previamente sobre a identidade do gestor e sobre o armazenamento e o objetivo do tratamento dos dados pessoais; VI - solicitar ao consulente a revisão de decisão realizada exclusivamente por meios automatizados; e VII - ter os seus dados pessoais utilizados somente de acordo com a finalidade para a qual eles foram coletados [...]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 11 ago. 2022.

[9] Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 16 jan. 2022.

Esses fundamentos que embasam a Lei Geral de Proteção de Dados, reforçam a preocupação do legislador em proteger os direitos fundamentais da pessoa natural, tendo em vista que "encontra-se em evidente posição de vulnerabilidade, pois parte de seus dados pessoais estão à disposição de terceiros sem que ela tenha domínio sobre isso, colocando em risco a privacidade, intimidade e dados pessoais" (BOTELHO, 2020, p. 199-200).

Sobre o aspecto territorial, o artigo 3º da Lei Geral de Proteção de Dados delimita o alcance do tratamento de dados, considerando aplicável àqueles dados que foram coletados dentro do território nacional ou que, a atividade de tratamento que objetiva a oferta/fornecimento de bens/serviços tenha ocorrido no território nacional.

Outro elemento importante trazido pela Lei Geral de Proteção de Dados é o consentimento do indivíduo, tendo em vista que "ao longo do seu corpo normativo acabam por revelar uma forte preocupação, mais uma vez, sobre qual deve ser a carga participativa do indivíduo no fluxo de suas informações pessoais" (BIONI, 2019, p. 185).

Contido no artigo 5º, inciso XII da Lei Geral de Proteção de Dados, o consentimento é a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada". Nesse sentido:

> [...] a necessidade do consentimento na coleta dos dados, principalmente no ambiente virtual, foi ganhando importância em razão da sensibilidade e vulnerabilidade que as informações pessoais foram adquirindo com o desenvolvimento da tecnologia. Nesse sentido, garantir que as pessoas/usuários tenham ciência de que devem consentir o uso dos dados, assim como tenham direito de saber a finalidade da coleta e acesso ao seu conteúdo em qualquer momento, é primordial para assegurar a liberdade e a privacidade. (PINHEIRO, 2018, p. 48).

Dessa forma, a sistemática do consentimento do indivíduo nada mais é do que transmitir ao titular dos dados pessoais o controle sobre as suas informações. Todavia, "o consentimento como afirmação dos direitos relativos aos dados digitais possui uma natureza controversa, justamente porque intenta consagrar liberdade e autonomia privada em um cenário de profunda desigualdade na gestão de dados [...]" (FORNASIER; KNEBEL, 2021, p. 1018).

Acerca dessa posição de vulnerabilidade em que o titular dos dados pessoais está condicionado, temos como exemplo brasileiro a decisão proferida pelo Superior Tribunal

Federal, na Ação Direta de Inconstitucionalidade (ADI) nº 6387, 6388, 6389, 6390 e 6393 (julgamento conjunto), relatado pela Ministra Rosa Weber, a qual julgou inconstitucional a Medida Provisória nº954/2020.

Para contextualizar, a Medida Provisória nº954/2020 foi editada em 17 de abril de 2020, visando o compartilhamento de dados de usuários por empresas de telecomunicações com o Instituto Brasileiro de Geografia e Estatística (IBGE), com o fim de produção estatística oficial durante a pandemia do coronavírus. Dessa forma, determinava o compartilhamento dos nomes, números de telefone e endereços dos consumidores de empresas prestadoras de serviços de telecomunicações (telefone fixo e móvel).

A referida Medida Provisória causou enorme preocupação acerca da privacidade dos consumidores, motivo o qual foram propostas Ações Diretas de Inconstitucionalidade pelo Conselho Federal da Ordem dos Advogados do Brasil (ADI nº6387), pelo Partido da Social Democracia Brasileira – PSDB (ADI nº6388), pelo Partido Socialista Brasileiro – PSB (ADI nº6389), pelo Partido Socialismo e Liberdade – PSOL (ADI nº6390) e pelo Partido Comunista do Brasil - PCB (ADI nº6393). Tais ações visavam, entre outras motivações, proteger a dignidade da pessoa humana, a inviolabilidade da intimidade, vida privada, honra e da imagem das pessoas, além do sigilo dos dados.

A relatora Ministra Rosa Weber, em seu voto, mencionou que a MP nº954/2020 não apresentava "mecanismo técnico ou administrativo apto a proteger os dados pessoais de acessos não autorizados, vazamentos acidentais ou utilização indevida, seja na sua transmissão, seja no seu tratamento" (ADI nº6387, 2020, p. 12).

Ainda, referiu que "a adequada tutela do direito à intimidade, privacidade e proteção de dados pessoais é estruturada pela característica da inviolabilidade [...] uma vez afrontada a norma de proteção de tais direitos, o ressarcimento se apresenta como tutela insuficiente aos deveres de proteção" (ADI nº6387, 2020, p. 14).

Essa decisão foi um marco jurídico no cenário brasileiro logo após a edição da Lei Geral de Proteção de Dados, em razão da demarcação jurisprudencial acerca da existência de um direito fundamental de proteção de dados pessoais e a necessidade de assegurar a inviolabilidade da intimidade, privacidade e dos dados pessoais.

Conforme vem se manifestando a jurisprudência pátria, é preciso que se garanta, com urgência, que os princípios fundamentais básicos do cidadão sejam garantidos, dentre eles, especialmente vinculados ao caso os princípios da privacidade e autodeterminação de dados, e o direito a proteção de dados como um direito fundamental (VIANA; MONTENEGRO; ORLANDINO, 2020).

Dessa forma, em decorrência desse amplo debate sobre a necessidade de proteger os dados pessoais, em 10 de fevereiro de 2022 foi promulgada a Emenda Constitucional nº115, a qual alterou a Constituição Federal para incluir a proteção dos dados pessoais (inclusive nos meios digitais), entre os direitos e garantias fundamentais.

Portanto, com a vigência da Lei Geral de Proteção de Dados e, recentemente, com a inclusão da proteção dos dados pessoais como direito e garantia fundamental, está em evidência o avanço legislativo que o Brasil teve para assegurar proteção jurídica adequada aos sujeitos, frente à era informacional em que se vive.

3. A LEI GERAL DE PROTEÇÃO DE DADOS COMO INSTRUMENTO LIMITADOR AO CAPITALISMO DE VIGILÂNCIA

> *"Ao futuro ou ao passado, a um tempo em que o pensamento seja livre, em que os homens sejam diferentes uns dos outros, em que não vivam sós — a um tempo em que a verdade exista e em que o que for feito não possa ser desfeito [...]".*
> *(George Orwell).*

O trecho mencionado foi retirado do livro *1984*, escrito pelo autor George Orwell, o qual trata de uma distopia. Uma sociedade vivendo sobre os extremos do totalitarismo, tendo como objeto o Grande Irmão (*Big Brother*) que controla todas as informações e comportamentos da sociedade através de teletelas. Ainda, o Partido dessa sociedade tem o seguinte lema: "Guerra é paz, liberdade é escravidão e ignorância é força" (ORWELL, 2003, p. 9).

Essa distopia proposta por Orwell, talvez não se trata de um estado imaginário, mas sim de uma forma de sociedade em que alguns aspectos se assemelham a forma de organização que se vive atualmente. É inegável que o mundo está na era digital, expansão das

tecnologias e informações. Tudo está conectado e o acesso aos dados pessoais está cada vez maior e mais fácil.

Diferentemente do Estado totalitário simbolizado pelo autor George Orwell, na obra *1984*, a tecnologia digital está presente em todos os lugares para atender aos interesses do capitalismo de vigilância, forma de poder esta que é caracterizada pela máxima concentração de conhecimento obtido silenciosamente e que não passa pela supervisão da democracia.

Existe uma vulnerabilidade daqueles que frequentam e utilizam o ambiente virtual, daqueles que estão capitalizando seus dados. Nesse sentido, essa "desigualdade na gestão de dados" (FORNASIER; KNEBEL, 2021) se dá pela vulnerabilidade do indivíduo perante as grandes empresas de tecnologia.

Apesar dessa condição de vulnerabilidade, o "indivíduo acaba contribuindo ainda mais com as engrenagens desse sistema, porque se vê obrigado a consumir essas tecnologias de informação e comunicação para participar efetivamente da sociedade em rede" (PESSOA, 2020, p. 55).

Dessa forma, para fazer parte da sociedade, o indivíduo acaba cedendo aos interesses do capitalismo de vigilância, autorizando uma série de ataques a sua privacidade. Exemplo claro disso é a concordância de termos e condições, os quais são solicitados ao usuário para ter acesso a algum site ou plataforma digital.

Para tanto, Shoshana Zuboff já alertava que muitos desses documentos digitais, como o exemplo citado acima, são demasiadamente complexos e longos, "em parte para desencorajar usuários de os ler de fato, mesmo que a maioria dos tribunais venha respaldando a legitimidade desses acordos via cliques (*click-wrap*), apesar da óbvia falta de profundo consentimento" (ZUBOFF, 2020, p. 64-65).

Diante do avanço legislativo brasileiro quanto à proteção de dados, essa questão do consentimento é fator primordial para verificar se a Lei Geral de Proteção de Dados é instrumento limitador do capitalismo de vigilância.

No que diz respeito à Lei Geral de Proteção de Dados, o seu enfoque está no consentimento do indivíduo, motivo pelo qual, ao longo do texto o legislador mencionou a palavra "consentimento" 37 vezes. Sendo assim, a forma pela qual a LGPD trouxe o instituto

do consentimento, revela "uma forte preocupação, mais uma vez, sobre qual deve ser a carga participativa do indivíduo no fluxo de suas informações" (BIONI, 2019, p. 185).

A LGPD tem como fundamento a autodeterminação informativa, o qual apregoa a necessidade da formulação de um controle ideal por parte do indivíduo em relação às suas informações pessoais. Esse controle ideal começa na proteção constitucional dos dados pessoais: o indivíduo deve poder determinar "quem sabe o que sobre ele, quando e em que circunstância" (VIANA; MONTENEGRO; ORLANDINO, 2020, p. 10).

É transmitido ao indivíduo a autodeterminação informativa sobre quais dados serão disponibilizados, porém, "esse sujeito carece de condições materiais para exercício de plena liberdade sobre os dados pessoais, pois a escolha está somente na forma de consentimento em que os dados serão rendidos aos prestadores de serviços digitais" (FORNASIER; KNEBEL, 2021, p. 1024.)

Diante disso cabe nos questionar se o consentimento seria uma forma de responsabilizar o titular dos dados pessoais pelas informações fornecidas de maneira a "isentar" as empresas das obrigações contidas na Lei Geral de Proteção de Dados, em decorrência da concordância do sujeito em "fornecer" determinadas informações. Nesse contexto,

> [...] pode-se questionar em que medida o consentimento informado tem potencial de ser um controle social e um exercício de autodeterminação informativa no que tange à permissão de circulação de dados. Em primeiro lugar, importa recordar que o fornecimento do consentimento é *conditio sine qua non* para o acesso de produtos e serviços na sociedade em rede, sem o qual o usuário não pode desfrutar das interações sociais dali permitidas, tornando-se a concordância meramente uma etapa neste processo. Em segundo lugar, a obtenção do consentimento informado se limita a um mero clique do usuário em um botão pré-determinado ou em uma caixa de seleção (*blank selection*), dispensando-se o real entendimento dos termos e condições apresentados, já que basta o aceite formal do indivíduo para que supostamente se legitime o tratamento dos dados. Por outro lado, nem sempre o usuário sabe o que está aceitando, em virtude da extensão dos textos e a utilização de expressões jurídicas, querendo logo acessar o produto ou serviço, independentemente do que esteja aceitando nas entrelinhas das políticas de privacidade (PESSOA, 2020, p. 93).

Embora exista o reconhecimento da vulnerabilidade do indivíduo no mundo digital, motivo o qual o amplo debate em torno da proteção de dados e a promulgação de legislações

que garantam segurança jurídica aos sujeitos nessas relações, ainda carece de elementos que assegurem aos indivíduos essa condição.

Ao trazer no texto legislativo o instituto do consentimento, é transferido ao indivíduo um lugar de "saber" e de "igualdade" perante aquele que opera os seus dados. Para tanto, ao "consentir", o sujeito está se responsabilizando por ações que, muitas vezes, nem tem conhecimento ou entendimento do que será feito. É nesse "não saber" do sujeito que o capitalismo de vigilância age.

Para combater o capitalismo de vigilância e reagir frente a esse regime opressor, Shoshana Zuboff relembra que o Muro de Berlim caiu por muitas razões, mas acima de tudo porque as pessoas disseram "Chega!". Assim, "nós também podemos ser autores de muitos fatos novos 'grandes e belos' que reclamem o futuro digital como lar da humanidade. Chega! Que seja esta a *nossa* declaração" (ZUBOFF, 2020, p. 588).

Por fim, não basta apenas a existência de uma legislação, neste caso a LGPD, que proteja os dados pessoais dos indivíduos, em razão de que esta mesma legislação transfere para o sujeito, através do consentimento, a responsabilidade pelas informações que chegam às instituições. As normativas devem ser pensadas colocando o indivíduo numa condição de vulnerabilidade no mundo tecnológico e não como a "carcaça abandonada" mencionada por Zuboff.

CONSIDERAÇÕES FINAIS

O presente artigo buscou compreender o termo "capitalismo de vigilância", referido pela autora norte-americana Shoshana Zuboff em suas pesquisas, principalmente no livro *A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder*, e analisar a Lei Geral de Proteção de Dados (LGPD) como regulamento limitador (ou não) ao acesso pelas grandes empresas aos dados sensíveis dos titulares.

Nesse sentido, verificou-se que o fenômeno do capitalismo de vigilância é uma forma de poder caracterizada pela extração de informações dos sujeitos. Informações essas que são obtidas silenciosamente, desviando da supervisão da democracia.

O capitalismo de vigilância está muito presente na sociedade informacional, tendo ênfase com a expansão tecnológica digital decorrente do modelo de sucesso dos produtos da *Apple* e do avanço das grandes empresas de tecnologia no Vale do Silício.

A partir dessa expansão tecnológica digital, tornou-se necessário pensar legislações para regrar as dinâmicas presentes na era da informação, surgindo então o Regulamento Geral de Proteção de Dados da União Europeia e no caso brasileiro a Lei Geral de Proteção de Dados.

No Brasil, algumas legislações anteriores a LGPD já previam, mesmo que minimamente, a proteção de dados, como por exemplo a Constituição Federal de 1988, o Código de Defesa do Consumidor (Lei nº 8.078, de 11 de setembro de 1990); a Lei do Cadastro Positivo (Lei nº12.414, de 9 de junho de 2011); e, o Marco Civil da Internet (Lei nº 12.965, de 23 de abril de 2014).

A Lei Geral de Proteção de Dados (LGPD) é uma normativa baseada nas regulações europeias e constituiu, no Brasil, um marco normativo referente aos dados digitais, sendo um instrumento que garante a defesa dos direitos privados e fundamentais dos dados digitais dos usuários.

Tendo em vista a condição de vulnerabilidade dos indivíduos nestas relações informacionais, algumas decisões judiciais brasileiras já demarcaram a aplicabilidade dessas legislações vigentes, garantindo a proteção dos dados pessoais dos sujeitos.

Todavia, em que pese o avanço legislativo acerca da proteção de dados, a Lei Geral de Proteção de Dados ainda carece de elementos que reafirmem a condição de vulnerabilidade dos indivíduos. Fator relevante é o instituto do consentimento mencionado na LGPD, o qual transfere ao sujeito a responsabilidade pelas informações fornecidas às instituições.

Para tanto, a Lei Geral de Proteção de Dados ainda não é um instrumento eficaz e limitador para combater o capitalismo de vigilância, visto que ao trazer o instituto do consentimento e da autodeterminação informacional como fundamentos basilares da norma, negam a condição de vulnerabilidade do sujeito nestas relações constituídas na era informacional.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 16 jan. 2022.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. **Código de Defesa do Consumidor**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 16 jan. 2022.

BRASIL. Lei nº 12.414, de 9 de junho de 2011. **Lei do Cadastro Positivo**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 11 ago. 2022.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. **Marco Civil da Internet.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 16 jan. 2022.

BRASIL. Lei nº 13.709, de agosto de 2018. **Lei Geral de Proteção de Dados.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 16 jan. 2022.

BRASIL, Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade nº6837**. Requerente: Conselho Federal da Ordem dos Advogados do Brasil. Relatora: Ministra Rosa Weber, 07 de maio de 2020. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357629. Acesso em: 11 ago. 2022.

BRASIL. **Medida Provisória nº954**, de 17 de abril de 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv954.htm. Acesso em: 11 ago. 2022.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: A função e os limites do consentimento**. Rio de Janeiro: Forense, 2019. [e-book].

BOTELHO, Marcos César. A proteção de dados pessoais enquanto direito fundamental: considerações sobre a Lei Geral de Proteção de Dados. **Argumenta Journal Law**, Jacarezinho – PR, n. 32, p. 191-207, 2020. Disponível em: http://seer.uenp.edu.br/index.php/argumenta/article/view/1840. Acesso em: 16 jan. 2022.

COSTA JR., Paulo José da. **O direito a estar só: tutela penal da intimidade**. São Paulo: RT, 1970.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law [EJJL]**, v. 12, n. 2, p. 91–108, 2011. Disponível em:

https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em: 7 mar. 2022.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: fundamentos da lei geral de proteção de dados.** 2º ed. São Paulo: Thomson Reuters Brasil, 2019.

FORNASIER, Mateus de Oliveira; KNEBEL, Norberto Milton Paiva. O titular de dados como sujeito de direito no capitalismo de vigilância e mercantilização dos dados na Lei Geral de Proteção de Dados. **Revista Direito e Práxis**, Rio de Janeiro, v. 12, n. 2, p. 1002-1033, 2021. Disponível em: https://www.scielo.br/j/rdp/a/hTqmGJVy7FP5PWq4Z7RsbCG/abstract/?lang=pt. Acesso em: 16 jan. 2022.

MOROZOV, Evgeny. **Big Tech: A ascensão dos dados e a morte da política**. São Paulo: Ubu Editora, 2018.

ORWELL, George. **1984**. São Paulo: Editora Nacional, 2003.

PARLAMENTO EUROPEU; CONSELHO DA UNIÃO EUROPEIA. **Carta de Direitos Fundamentais da União Europeia**. 07 de dezembro de 2000. Disponível em: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf. Acesso em: 16 jan. 2022.

PARLAMENTO EUROPEU; CONSELHO DA UNIÃO EUROPEIA. **Regulamento (UE) 2016/679**. Regulamento Geral de Proteção de Dados da União Europeia de 27 de abril de 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 16 jan. 2022.

PESSOA, João Pedro Seefeldt. **O efeito Orwell na sociedade em rede: cibersegurança, regime global de vigilância social e direito à privacidade no século XXI**. Porto Alegre: Editora Fi, 2020. [e-book].

PINHEIRO, Patricia Peck. **Proteção de dados pessoais: comentários à Lei nº 13.709/2018 (LGPD)**. São Paulo: Saraiva Educação, 2018.

POPPER, Karl Raimund. **A lógica da pesquisa científica**. São Paulo: Cultrix, 1975.

UNIÃO EUROPEIA, **Carta dos Direitos Fundamentais da União Europeia de 2000.** Disponível em: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf. Acesso em: 16 jan. 2022.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder**. Tradução George Schlesinger. 1. ed. Rio de Janeiro: Intrínseca, 2020.

SOBRE AS AUTORAS

MILENA CERESER DA ROSA

Doutoranda em Direitos Humanos pela Universidade Regional do Noroeste do Estado do Rio Grande do Sul - UNIJUÍ. Mestra em Direitos Humanos pela Universidade Regional do Noroeste do Estado do Rio Grande do Sul - UNIJUÍ (2021-2022) com bolsa CAPES, do Programa de Cooperação Acadêmica em Segurança Pública e Ciências Forenses (PROCAD/CAPES). Especialista em Ensino de Filosofia pela Universidade Federal de Pelotas - UFPel (2021). Graduada em Direito pela Universidade Regional do Noroeste do Estado do Rio Grande do Sul - UNIJUÍ (2013). Integrante do Grupo de Pesquisa Direitos Humanos e Biopolítica (CNPq). Representante da Comissão da Mulher da Ordem dos Advogados do Brasil, Subseção Giruá/RS. Trabalha como advogada atuando nas áreas de direito de família, inventário e sucessões. Em seus estudos atua principalmente com filosofia em educação, feminismo, gênero, direitos humanos, integração de banco de dados e segurança pública.

Orcid: https://orcid.org/0000-0001-6493-9752
E-mail: milenacereser@outlook.com

JOICE GRACIELE NIELSSON

Doutora em Direito Público pela Universidade do Vale do Rio dos Sinos/UNISINOS-FURB (2016), possui graduação em Direito pela Universidade Regional do Noroeste do Estado do Rio Grande do Sul (2010) e Mestrado em Desenvolvimento pela Universidade Regional do Noroeste do Estado do Rio Grande do Sul (2012). Atualmente é Professora-Pesquisadora do Programa de Pós-Graduação em Direito - Mestrado e Doutorado em Direitos Humanos - e do Curso de Graduação em Direito da Universidade Regional do Noroeste do Estado do Rio Grande do Sul. Coordenadora da Pós-graduação Justiça Restaurativa e Mediação na mesma instituição. Atua principalmente nos seguintes temas: Gênero, Feminismo, Direitos Sexuais e Reprodutivos; Segurança Pública; Políticas de Segurança Pública e Direitos Humanos; Biopolítica e Necropolítica. É integrante do Grupo de Pesquisa Direitos Humanos e Biopolítica (CNPq) e Pesquisadora Recém-Doutora FAPERGS Edital 04/2019.

Orcid: https://orcid.org/0000-0003-3808-1064
E-mail: joice.nielsson@unijui.edu.br

Este é um ARTIGO publicado em acesso aberto (*Open Access)* sob a licença *Creative Commons Attribution*, que permite uso, distribuição e reprodução em qualquer meio, sem restrições, desde que o trabalho original seja corretamente citado.