A (In)eficácia da Lei 13.709/2018 como Limitador ao Capitalismo da Vigilância[1]

Liton Lanes Pilau Sobrinho[2]

Victor da Luz Guidoni[3]

Resumo: O artigo busca investigar as principais previsões legais da Lei 13.709/2018 em comparação com o Regulamento Geral de Proteção de Dados (RGPD) da União Europeia (UE) para avaliar se a legislação brasileira criou limitações à prática do capitalismo da vigilância pelas grandes empresas de tecnologia, o qual é utilizado para manipulação comportamental dos usuários na criação de produtos e serviços. O problema que orienta a pesquisa pode ser descrito pela seguinte questão: A entrada em vigor da Lei 13.709/2018 em setembro de 2020 criou uma limitação para a exploração das *big techs* aos dados pessoais dos usuários? O objetivo geral do texto é avaliar se a Lei Geral de Proteção de Dados (LGPD) é eficaz na limitação da exploração das *big techs* aos dados pessoais dos usuários. Os objetivos específicos do artigo, estruturados em três partes, são: a) analisar as previsões da Lei 13.709/2018 em comparação com o RGPD da União Europeia; b) compreender o papel e os efeitos das *big techs* no capitalismo da vigilância; c) verificar se a Autoridade Nacional de Proteção de Dados (ANPD), utilizando as previsões da LGPD, consegue limitar o capitalismo da vigilância. Assim, a entrada em vigor da Lei 13.709/2018 criou uma limitação para exploração das *big techs*, especialmente quando a Lei 14.460/2022 reconheceu a ANPD como autarquia de natureza especial para permitir uma fiscalização mais efetiva dos agentes de tratamento de dados, incluindo as grandes empresas de tecnologia. No entanto, é necessário que o aparato estatal fortaleça o órgão regulamentador de proteção de dados, por meio do aumento do orçamento da ANPD, visando ampliar os recursos técnicos e humanos para garantir que os dados dos titulares deixem de ser meras fontes de recursos para fomento do capitalismo da vigilância e passem a ser protegidos como elementos essenciais para garantir os direitos fundamentais previstos na Constituição.

Palavras-chave: Autoridade Nacional de Proteção de Dados. *Big Techs*. Capitalismo da Vigilância. Lei Geral de Proteção de Dados. Regulamento Geral de Proteção de Dados.

Introdução

Os inúmeros casos de desrespeito das *big techs* às legislações de proteção de dados estão sendo amplamente divulgados pela mídia e repreendidos pelos órgãos fiscalizadores dos respectivos países. Diante desse cenário, este artigo busca compreender se a Lei 13.709/2018 criou uma limitação para exploração das grandes empresas de tecnologia aos dados pessoais dos usuários. Além disso, analisaremos a atuação da Lei de Proteção de Dados em comparação com o Regulamento Geral de Proteção de Dados da União Europeia, bem como a

1 Artigo científico apresentado ao curso de Direito, da Faculdade de Direito da Universidade de Passo Fundo, como requisito parcial para a obtenção do grau de Bacharel em Ciências Jurídicas e Sociais, sob orientação do professor Liton Lanes Pilau Sobrinho, no ano de 2024.

2 Doutor em Direito pela Universidade do Vale do Rio dos Sinos – UNISINOS; Pós-doutor em Direito pela Universidade de Sevilha – US; Professor dos cursos de Mestrado e Doutorado no Programa de Pós-Graduação Stricto Sensu em Ciência Jurídica da Universidade do Vale do Itajaí. Professor do Programa de Pós-Graduação Stricto Sensu Mestrado em Direito da Universidade de Passo Fundo. Coordenador do PPGD da Universidade de Passo Fundo. E-mail: liton@upf.br

3 Acadêmico do Curso de Direito da Faculdade de Direito da Universidade de Passo Fundo. E-mail: 183393@upf.br

atuação dos órgãos de proteção para limitar as ações das *big techs* no fomento do capitalismo da vigilância.

Nesse ponto, as práticas predatórias das grandes empresas de tecnologia demonstram que as legislações de proteção de dados precisam fortalecer os órgãos de regulamentação para combater o capitalismo da vigilância. Desse modo, o problema que orienta a pesquisa pode ser descrito pela seguinte questão: A entrada em vigor da Lei 13.709/2018 em setembro de 2020 criou uma limitação para a exploração das *big techs* aos dados pessoais dos usuários?

A hipótese inicial, fundamentada nas pesquisas realizadas acerca da temática, demonstra que a LGPD é uma conquista legislativa ao estabelecer diretrizes para a proteção dos dados de pessoas físicas e de pessoas jurídicas perante as instituições públicas e privadas.

Como objetivo geral, o texto avalia se a Lei Geral de Proteção de Dados é eficaz na limitação da exploração das *big techs* aos dados pessoais dos usuários. Os objetivos específicos do artigo, estruturados em três partes, são: a) analisar as previsões da Lei 13.709/2018 em comparação com o RGPD da União Europeia; b) compreender o papel e os efeitos das *big techs* no "capitalismo da vigilância"; c) verificar se a Autoridade Nacional de Proteção de Dados, utilizando as previsões da LGPD, consegue limitar o capitalismo da vigilância.

Esse artigo se justifica pela necessidade de debater esse tema em um mundo cada vez mais tecnológico. Não se trata de apenas uma discussão teórica, mas sim de uma abordagem acerca dos impactos ocasionados pela exploração desses dados na Era do Capitalismo da Vigilância, sob a ótica das dificuldades de fiscalização das grandes empresas de tecnologia pelos órgãos regulamentadores. Nesse sentido, compreende-se que a Lei 13.709/2018 foi criada para proteger os dados dos titulares brasileiros, e consequentemente, impedir que as *big techs* utilizem essas informações para benefício econômico.

1. Uma Análise das Previsões Legais da Lei Geral de Proteção de Dados em Comparação com o Regulamento Geral de Proteção de Dados da União Europeia

Para compreender a (in)eficácia da Lei Geral de Proteção de Dados como limitador ao capitalismo da vigilância, é fundamental analisar, em primeiro lugar, os direitos e garantias fundamentais assegurados aos cidadãos brasileiros pela Constituição Federal de 1988 e pela Lei 13.709/2018. Além disso, é essencial explorar os conceitos basilares presentes na LGPD

que sustentam os princípios do consentimento para o tratamento de dados pessoais, os quais são pilares centrais na legislação vigente.

O legislador constituinte previu os direitos e garantias fundamentais no artigo 5° da CF/88, que tem como propósito o respeito à dignidade do ser humano, utilizando-se da proteção contra o arbítrio do poder estatal e o estabelecimento de condições mínimas de vida e personalidade humana (Moraes, 2018, p. 42). Dentre os direitos fundamentais, destaca-se a proteção da privacidade, um aspecto essencial para preservar a autonomia dos brasileiros em um cenário cada vez mais digitalizado.

Dito isso, o artigo 5°, inciso X[4], da CF/88 dispõe sobre os direitos inerentes à personalidade, tais como os direitos à imagem, à honra e à intimidade. Essa previsão constitucional encontra-se positivada no capítulo II do Código Civil de 2002, que trata os direitos da personalidade como intransmissíveis e irrenunciáveis, bem como não permite que o exercício destes sofra limitações voluntárias, vide o artigo 11 da legislação supramencionada[5]. Acerca dos dados pessoais nos meios digitais como direito fundamental, a Emenda Constitucional n° 115/2022 incluiu o inciso LXXIX[6], no artigo 5° da CF/88 para reconhecer o direito à proteção de dados pessoais na Carta Magna brasileira.

Nesse contexto, a sociedade submetida à permanente vigilância nos espaços públicos, com captação e uso das imagens, além dos dados pessoais dos sujeitos, sem expressa autorização, deve ser protegida com base na proteção à privacidade e à imagem. Contudo, essa proteção individual prevista na Constituição Cidadã é prejudicada pelos empecilhos tecnológicos de impedir que informações pessoais ‘vazem’ pela rede mundial de computadores. Isso não é um impedimento, mas sim um desafio para a proteção desses direitos fundamentais (Schreiber, 2018, p. 67).

Os obstáculos criados pelas ações de fomento do capitalismo da vigilância trouxeram as legislações de proteção de dados como solucionadoras para as inseguranças relacionadas à proteção dos titulares de dados ao redor do mundo. Dito isso, a Carta dos Direitos Fundamentais da União Europeia estabelece que todos os cidadãos da UE têm direito à proteção de seus dados pessoais, o que mobilizou os legisladores europeus para criação do Regulamento Geral de Proteção de Dados.

---

4 Artigo 5° [...] 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.

5 Artigo 11, CC/2002 - com exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária.

6 Artigo 5° […] LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.

A RGPD tem por objetivo preparar a União Europeia para a era digital e garantir a segurança jurídica almejada por 90% (noventa por cento) da população europeia. Essas pessoas desejam o mesmo nível de proteção de dados pessoais em toda a Europa, independentemente do local do tratamento, ou seja, tanto nas instituições públicas quanto nas privadas, conforme pesquisa realizada pela Comissão Europeia.

Nesse ponto, nota-se que os legisladores europeus, inspirados na Carta dos Direitos Fundamentais da União Europeia e nas demandas da população, criaram o Regulamento Geral de Proteção de Dados Pessoais Europeu, promulgado pela UE. Esses legisladores europeus trouxeram elementos que garantem liberdade, segurança e justiça, além de promover uma união econômica e social entre os mercados econômicos, visando o bem-estar dos indivíduos (Pinheiro, 2023, p. 10).

Desse modo, os legisladores brasileiros, antenados às legislações estrangeiras que garantem a proteção dos dados pessoais das pessoas físicas, principalmente no RGPD, criaram a LGPD para se adequar aos avanços e necessidades mercadológicas criadas pelo ordenamento jurídico estrangeiro, assim como para garantir a proteção dos cidadãos brasileiros no tratamento dos seus dados pessoais (Teixeira; Guerreiro, 2022, p. 34).

Acerca da Lei 13.709/2018, é necessário reconhecer que houve preocupação por parte do legislador em proteger os direitos fundamentais positivados pela Constituição Federal de 1988 relacionados à segurança dos dados pessoais, principalmente os direitos à intimidade, privada, honra e imagens das pessoas (Teixeira; Guerreiro, 2022, p. 13).

Essa vontade legislativa de proteger esses direitos intransmissíveis está prevista no artigo 1° da Lei Geral de Proteção de Dados[7], o qual demonstra o objetivo principal da LGPD: a proteção dos direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural. Em outras palavras, o legislador estabeleceu que o tratamento de dados está intrinsecamente ligado aos direitos fundamentais da privacidade e da liberdade, ambos consagrados no artigo 5°, incisos X e XII, da Constituição Federal de 1988[8] (Pinheiro, 2023, p. 37).

Em contraponto, o preâmbulo da RGPD demonstra que o documento é fundamentado nos direitos fundamentais da Carta dos Direitos Fundamentais da União Europeia e tem como

7 Artigo 1º - Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

8 Artigo 5° [...] 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 instrução processual penal.

objetivo proteger a privacidade, liberdade, segurança, justiça das pessoas, bem como promover o progresso econômico e social e assegurar a segurança dos países da UE (Teixeira; Guerreiro, 2022, p. 9).

Dessa forma, observa-se uma influência do Regulamento Geral de Proteção de Dados da União Europeia na LGPD, uma vez que ambas as legislações têm como objetivo a proteção dos dados, visando garantir a segurança para o livre desenvolvimento dos indivíduos sob sua jurisdição.

Em relação às inovações legislativas previstas na Lei 13.709/2018, destaca-se o artigo 5°, que trouxe a definição dos termos utilizados ao longo do documento legislativo, visando garantir a ausência de ambiguidade interpretativa, especialmente nos artigos que tratam do consentimento para tratamento dos dados do titular. Esse aspecto é detalhado ao longo do capítulo II (Do tratamento de dados pessoais) da Lei Geral de Proteção de Dados.

Nesse ponto, o Regulamento Geral de Proteção de Dados da União Europeia traz essas definições no artigo 4° do documento legislativo europeu. Entretanto, é importante ressaltar que existem pequenas diferenças entre os conceitos e as nomenclaturas dispostos nas duas legislações, principalmente em relação à figura do encarregado de dados (Pinheiro, 2023, p. 39).

É necessário reconhecer a diferenciação dos conceitos de dado pessoal, dado pessoal sensível e dado anonimizado apresentados no artigo 5°, incisos I ao III da Lei 13.709/2018[9]. Nesse trecho do texto legislativo, frisa-se que a LGPD definiu o dado pessoal como a informação de uma pessoa natural identificada e identificável. Por outro lado, o dado anonimizado é aquele que, por meio do uso de tecnologias como criptografia, foi modificado ou alterado de forma a não identificar mais o titular. Contudo, é importante observar que mesmo os dados anonimizados podem, em alguns casos, ser identificados por meio do tratamento das informações realizado pelos controladores ou operadores (Teixeira; Guerreiro, 2022, p. 17).

Esses dados, conceituados no artigo 5°, incisos I ao III, da Lei 13.709/2018, possuem um titular definido no inciso V da LGPD[10], como a pessoa física ou jurídica, tanto pública

9 Artigo 5º [...] I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável; II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural; III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

10 Artigo 5° [..] V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

quanto privada, os quais têm seus dados tratados pelos agentes de tratamento. No entanto, destaca-se que essa previsão abrange apenas os dados pessoais de pessoa viva, não havendo nenhuma menção aos dados das pessoas já falecidas (Pinheiro, 2023, p. 33).

Acerca do princípio do livre acesso e da transparência, previsto no artigo 9° da Lei 13.709/2018, o titular dos dados deve ter acesso facilitado às informações relativas ao tratamento de seus dados, com o objetivo facilitar que o "dono dos dados" tenha conhecimento de quais de seus dados estão ou serão tratados, por quem e para qual fim. Além disso, esse artigo prevê as responsabilidades legais dos agentes, e as técnicas utilizadas no tratamento devem permitir que o titular tenha conhecimento pleno das formas de tratamento utilizadas pelos agentes de tratamento (Teixeira; Guerreiro, 2022, p. 24).

Dito isso, o titular dos dados possui direitos inerentes ao tratamento de seus dados, conforme o artigo 18 da Lei 13.709/2018. Nesse dispositivo, temos a preocupação do legislador expressa em assegurar que o titular tenha ciência que seus dados estão sendo tratados de modo seguro e cumprindo sua finalidade. Além disso, o texto legal reafirma a liberdade do titular de revogar o consentimento e solicitar a exclusão de seus dados (Pinheiro, 2023, p. 47).

Ainda, destaca-se que os bancos de dados foram abrangidos no artigo 5°, inciso IV da LGPD[11], que estipula que os controladores ou operadores de dados devem dispor de um local físico ou eletrônico para armazenar esses dados pessoais. A vigência da Lei Geral de Proteção de Dados obrigou a revisão dos bancos de dados e, consequentemente, a eliminação de dados que atingiram sua finalidade (Teixeira; Guerreiro, 2022, p. 17).

Nesse ponto, é importante observar que os controladores e os operadores, conforme definidos nos incisos VI e VII do artigo 5° da LGPD[12], são os responsáveis pelo tratamento dos dados constantes no banco de dados e possuem responsabilidades distintas no tratamento desses dados (Pinheiro, 2023, p. 39).

No Regulamento Geral de Proteção de Dados, as espécies de agentes de tratamento receberam a nomenclatura de *controller* (controlador) e *processor* (operador), as quais possuem diferenciações técnicas quando se atribuem responsabilidades e obrigações distintas entre os dois grupos. Essa diferenciação, prevista na Lei Geral de Proteção de Dados, é

11 Artigo 5º [..] IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

12 Artigo 5° [..] VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

fundamental para compreender os tipos de responsabilização que o controlador e o operador podem ter por suas condutas, especialmente quando o controlador for um ente público e o operador for um ente privado (Teixeira; Guerreiro, 2022, p. 18).

Por exemplo, a operadora são as empresas responsáveis apenas pelo armazenamento dos dados, atuando como prestadora de serviços para outra empresa, conhecidas como *Cloud Service Provider* (Fornecedor de Serviço em Nuvem), na qual os servidores podem estar localizados em diversos países (Teixeira; Guerreiro, 2022, p. 17).

Dito isso, essas duas figuras supracitadas são classificadas como agentes de tratamento, conforme definido no inciso IX da Lei 13.709/2018[13]. Ainda, o encarregado atua como o responsável pela comunicação entre os titulares de dados, os agentes de tratamento e a Autoridade Nacional de Proteção de Dados (ANPD), como previsto no inciso VIII da LGPD[14].

Em contrapartida ao encarregado na RGPD, que aborda essa figura de forma menos abrangente, a Lei Geral de Proteção de Dados prevê que o encarregado de dados pode ser tanto pessoa física quanto pessoa jurídica. Isso possibilita que a função de comunicação seja desempenhada por um comitê, adaptando-se ao modelo de gestão das instituições públicas ou privadas (Pinheiro, 2023, p. 39).

Dentre os princípios previstos no incisos do artigo 6° da LGPD, destacasse que a transparência é o princípio intrínseco ao consentimento disposto no artigo 5°, XII da Lei 13.709/2018[15], em função do tratamento dos dados e o compartilhamento de dados serem a positivação do dever de transparência das empresas sob as informações pessoais (Pinheiro, 2023, p. 39).

O consentimento, conforme definido no artigo 5°, inciso XII da Lei 13.709/2018, é o método mais reconhecido de tratamento legal de dados e deve garantir que o titular esteja ciente dos dados que estão sendo coletados e do propósito de sua utilização, o que confere a inequivocidade do consentimento (Teixeira; Guerreiro, 2022, p. 18).

Essa necessidade de conhecimento pelo titular dos dados tratados pelos operadores e controladores gerou preocupação entre os legisladores, especialmente no que diz respeito às autorizações genéricas e às finalidades indeterminadas. Isso porque tais práticas podem tornar

13 Artigo 5° [...] IX - agentes de tratamento: o controlador e o operador;

14 Artigo 5° [...] VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

15 Artigo 5° [...] XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

nulo o consentimento que deu origem ao tratamento de dados, conforme o artigo 7°, § 4°, da LGPD[16] (Pinheiro, 2023, p. 41).

Desse modo, essa manifestação pode ocorrer por meio de um termo de adesão ao serviço ou dos contratos via cliques (*click-wrap*) e seus semelhantes, ou seja, não se trata de uma autorização genérica, embora seja comum a todos os usuários do produto ou serviço, e apresente as finalidades do tratamento dos dados. Contudo, esses meios de consentimento obrigam o usuário a aceitá-los para fazer uso de determinados bens ou serviços (Zuboff, 2020, p. 131). Esse modelo de troca de informações pela possibilidade de utilização do serviço é comumente adotado pelas *big techs* para fomento do capitalismo da vigilância, o qual será explorado na segunda parte do presente artigo.

Dito isso, o tratamento de dados pessoais mediante o fornecimento de consentimento do titular é previsto no artigo 7°, inciso I da Lei 13.709/2018[17]. Este dispositivo destaca o consentimento do titular como pilar da LGPD, visando assegurar que o agente de tratamento de dados comprove que o tratamento das informações ocorreu dentro do limites do ordenamento jurídico brasileiro. Ainda, o consentimento do titular deve ser obtido de maneira expressa e de fácil compreensão para os usuários (Teixeira; Guerreiro, 2022, p. 21).

Além disso, o artigo 5°, inciso X da Lei 13.709/2018[18], prevê o conceito de tratamento, o qual está intrinsecamente relacionado ao conceito da titularidade dos dados, conforme previsto no artigo 5°, inciso V da Lei Geral de Proteção de Dados. Essa interconexão decorre do fato de que a proteção dos dados pessoais está diretamente ligada à tutela dos direitos das pessoas vivas em relação ao tratamento de suas informações (Teixeira; Guerreiro, 2022, p. 17).

O tratamento de dados pessoais deve observar a boa-fé e alguns princípios, como a finalidade, adequação, necessidade, transparência, segurança, dentre outros elencados nos incisos do artigo 6° da Lei Geral de Proteção de Dados, sendo que esses pilares do tratamento da dados brasileiro foram influenciados pelo Regulamento Geral de Proteção de Dados da União Europeia. Contudo, a RGPD dispõe de maneira explicita as regras, limites e os

16 Artigo 5° […] § 4º - O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.

17 Artigo 7° - O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I – mediante o fornecimento de consentimento pelo titular;

18 Artigo 5° [...] X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

requisitos para promoção da transparência, especialmente na comunicação dos dados pessoais (Pinheiro, 2023, p. 40).

Em relação à autodeterminação informativa, esta está relacionada ao poder do indivíduo em determinar como os dados serão tratados, ou seja, o titular dos dados pessoais possui o direito de saber quais informações pessoais estão sendo coletadas para determinada finalidade. Desse forma, o indivíduo pode avaliar se a concessão de seus dados pessoais para usufruir dos serviços ou produtos disponibilizados pelo controlador de dados é benéfica, considerando os possíveis malefícios que essa concessão pode acarretar para si (Teixeira; Guerreiro, 2022, p. 13).

Essa avaliação da concessão dos dados baseia-se na legítima expectativa do proprietário dos dados pessoais, relacionada ao princípio da boa-fé objetiva, sendo essa expectativa é uma das condições para julgar a legalidade e a juridicidade do legítimo interesse dos agentes de tratamentos, conforme o enunciado 683 da IX Jornada de Direito Civil[19].

O legislador brasileiro protegeu os dados sensíveis ao prever que o tratamento desses dados depende do consentimento específico e destacado, conforme o artigo 11, inciso I da Lei 13.709/2018. Essa previsão legal é de suma importância, visto que a violação dessas informações pode acarretar danos significativos aos direitos e às liberdades fundamentais da pessoa (Pinheiro, 2023, p. 43).

Ademais, a previsão legislativa de equiparação do tratamento de dados pessoais que revelem dados sensíveis ao tratamento de dados pessoais sensíveis demonstra a preocupação do legislador em proteger essas informações, que podem causar sérios prejuízos aos seus titulares em caso de vazamento, gerando assim uma proteção ampliada. Tal disposição está prevista no artigo 11, parágrafo 1° da Lei 13.709/2018[20], e é reforçada pelo enunciado 690 da IX Jornada de Direito Civil[21].

A respeito da hierarquia entre o tratamento de dados pessoais e dados pessoais sensíveis, compreende-se que não há uma hierarquia determinada na Lei Geral de Proteção de Dados. Entretanto, o enunciado 689 da IX Jornada de Direito Civil dispõe que "não há hierarquia entre as bases legais estabelecidas nos arts. 7º e 11 da Lei Geral de Proteção de

19 ENUNCIADO 683 – A legítima expectativa do titular quanto ao tratamento de seus dados pessoais se relaciona diretamente com o princípio da boa-fé objetiva e é um dos parâmetros de legalidade e juridicidade do legítimo interesse.

20 Artigo 11 [...] § 1º - Aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica.

21 ENUNCIADO 690 – A proteção ampliada conferida pela LGPD aos dados sensíveis deverá ser também aplicada aos casos em que houver tratamento sensível de dados pessoais, tal como observado no §1º do art. 11 da LGPD.

Dados (Lei n. 13.709/2018)". Isso sedimenta o entendimento de que deve haver consentimento do titular para permitir que seus dados sejam tratados pelos agentes de tratamento, com exceção das hipóteses previsas em lei (Pinheiro, 2023, p. 41).

Ainda, o uso compartilhado de dados, conceituado no artigo 5°, inciso XVI da LGPD[22], é necessário para sustentar as atividades de órgãos públicos e empresas, incluindo as grandes empresas de tecnologia, visto que é fundamental para o funcionamento destas (Teixeira; Guerreiro, 2022, p. 18). Esse compartilhamento permite que ocorra exploração indiscriminada dos dados pessoais pelas *big techs*, como ocorre entre Niantic e Google/Alphabet no caso Pokémon Go, o qual será abordado na segunda parte desse artigo.

Desse modo, a Lei Geral de Proteção de Dados trouxe inúmeras previsões legais para preparar o Brasil para a era digital e garantir a segurança jurídica necessária para proteção da população brasileira. Essa legislação protege os direitos fundamentais intransmissíveis e irrenunciáveis relacionados aos dados pessoais previstas na Constituição Federal, tais como a privacidade e a liberdade.

Além disso, a Lei 13.709/2018 traz diversas previsões conceituais necessárias para definir os elementos abrangidos pela lei de proteção de dados brasileira, especialmente no que diz respeito ao tratamento de dados pessoais sensíveis e ao uso compartilhado de dados, que merecem maior proteção devido aos perigos do vazamento dessas informações.

O consentimento empoderou os titulares de dados, porém esse direito de consentir com o tratamento de seus dados deve ter limitações diante das vulnerabilidades técnicas dos usuários. Assim, torna-se fundamental compreender o papel das grandes empresas de tecnologia na exploração dessas informações na era do capitalismo da vigilância.

2. A Exploração de Dados Pessoais na Era do Capitalismo da Vigilância

> "*Every breath you take (a cada suspiro que você der); every move you make (a cada movimento que você fizer); every bond you break (a cada elo que você quebrar); every step you take (a cada passo que você der); I'll be watching you (eu estarei te observando) [...]*".
>
> (Gordon Matthew Sumner - Sting)

22 Artigo 5° [...] inciso XVI - uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

O trecho mencionado foi retirado da música "*Every breath you take",* escrita por Gordon Sumner (Sting), produzida pela banda de rock britânico *The Police* e lançada no álbum "*Synchronicity"* em 1983, a qual trata de um relacionamento abusivo. A metáfora da perseguição constante presente na música pode ser aplicada à situação do controle de dados pessoais realizados pelas *big techs* no século XXI, devido à constante da vigilância exercida pelas corporações sobre os seus usuários.

É inegável que as grandes empresas de tecnologia estão em uma perseguição permanente aos dados dos usuários para aumentar suas receitas, tanto com a criação de novos produtos ou serviços quanto com a comercialização dos próprios dados. Por exemplo, a Google/Alphabet entende que necessita aumentar e diferenciar suas formas de angariar capital, tanto financeiro quanto de matéria-prima para extração de dados (Zuboff, 2020, p. 233).

As empresas de tecnologia praticam diversos ataques a privacidade dos titulares de dados, os quais autorizam essas condições para terem acesso as plataformas digitais ou sites (Nielsson; Rosa, 2023, p. 80). Essas práticas semelhantes aos atos praticados pelo perseguidor na música produzida pela banda *The Police,* o qual monitora todas as ações do indivíduo perseguido como as *big techs* executam com os titulares de dados.

Durante a trajetória da história humana, a sociedade experimentou inúmeras transformações desencadeadas por descobertas e invenções revolucionárias, tais como a máquina a vapor, a eletricidade, as telecomunicações em geral, os avanços da informática, a biotecnologia, entre outras. Essas inovações alteram significativamente a dinâmica das relações sociais, redefinindo como as pessoas se relacionam entre si (Battisti, 2023, p. 16).

Dito isso, o monitoramento constante praticado pelas empresas, especialmente pelas *big techs* definidas como os grandes *players* do mercado digital, como Meta (antigo Facebook), Amazon, Apple, Microsoft e Google/Alphabet, exercem forte influência sobre o comportamento da sociedade. Esse ecossistema foi fortalecido pela pandemia de Covid-19, que impulsionou cerca de 87,5% das empresas estabelecidas em território nacional a realizarem ações para promover a transformação digital (Battisti, 2023, p. 16).

As cinco grandes empresas de tecnologia mencionadas apresentavam um valor de mercado de US$ 4,3 trilhões em 2019. Com a evolução da pandemia de Covid-19 em todo mundo, esse valor saltou para US$ 8 trilhões em 2021. Tal montante representa

aproximadamente um terço do PIB dos Estados Unidos da América no mesmo ano, evidenciando o notável crescimento das *big techs* (Battisti, 2023, p. 16).

É notável que o controle das informações, anteriormente monopolizado pelos Estados, foi assumido pelas grandes empresas de tecnologia, que utilizam suas plataformas para controlar os interesses econômicos, sociais, culturais, políticos. Isso se deve à falta de regulamentação dos limites das empresas de tecnologia por parte dos países. A ausência de uma legislação clara tem sido objeto de debate em todas as instituições, tanto nacionais quanto internacionais, especialmente devido à falta de soberania das nações sobre as práticas das grandes empresas de tecnologia em relação ao controle das informações pessoais de seus cidadãos (Battisti, 2023, p. 118).

Nesse contexto, a autora americana Shoshana Zuboff define o capitalismo da vigilância como as ações das grandes empresas de tecnologia, as quais criaram uma ordem econômica baseada na utilização das experiências humanas para práticas comerciais. Esses métodos são fundamentados em técnicas parasíticas, que envolve a modificação de comportamentos por meio da produção de bens e serviços, sendo estabelecido como uma estrutura para o desenvolvimento de uma economia baseada na vigilância dos usuários (Zuboff, 2020, p. 7).

Para ilustrar o monitoramento constante praticando por empresas, Yuval Harari exemplifica que assistir a filmes específicos em um sistema de *streaming* como o Amazon Prime, por exemplo, permitirá que o algoritmo criado pela Amazon sugira outros filmes com alta precisão, de acordo com as preferências dos usuários. Esse algoritmo criado pela plataforma indicam produtos e serviços vendidos pela própria Amazon, inclusive os dados pessoais coletados pela empresa auxiliam que a taxa de acerto das indicações seja assertiva perante o usuário (Harari, 2018, p. 79).

Dito isso, o capitalismo da vigilância está presente nos monitoramento utilizados pelas *big techs* para realizar essas coletas de dados pessoais de seus usuários. A experiência humana, considerada matéria-prima gratuita para a compreensão dos comportamentos humanos, é a moeda dessa nova forma de negócio. Esses recursos são utilizados para criação de algoritmos mais precisos, os quais geram “a inteligência da máquina” para previsões dos “mercados de comportamentos futuros” (Zuboff, 2020, p. 19).

Para tanto, Byung-Chul Han já alertava que nossas ações na rede mundial de computadores estão sendo monitoradas em tempo integral devido aos rastros digitais que

deixamos na *internet.* É necessário reconhecer que o Google foi o pioneiro na implementação do capitalismo da vigilância ao criar os parâmetros para coleta dos dados pessoais, antecedendo assim as práticas adotadas por outras *big techs*, como Facebook e Microsoft (Zuboff, 2020, p. 20-21). Portanto, compreender o desenvolvimento do capitalismo da vigilância requer uma análise do funcionamento dessa prática realizada por essas empresas de tecnologia.

O Google passou por uma transformação significativa em relação à sua concepção original como um simples serviço de buscas, impulsionado pelo massivo investimento em novos métodos de captura do superavit comportamental, como os aparelhos de *smart home.* Isso ressalta uma das características dos capitalistas da vigilância: sua capacidade de adaptação para criar rotas de exploração visando à extração de dados pessoais (Zuboff, 2020, p. 154).

Dentre os principais métodos criados pelo Google, destaca-se a plataforma *Android,* que exerce uma fundação dominante na captura e defesa de superavit. Esse sistema aberto e abrangente para serviços móveis foi concebido como meio de defender e expandir a cadeia de suprimentos básica da empresa na área de buscas. Ao contrário da Apple, que obtém lucro principalmente pela venda de produtos com o sistema exclusivo *iOS*, o Google lucra indiretamente por meio do superavit comportamental gerado pela plataforma *Android*, além da geração de inúmeros produtos (Zuboff, 2020, p. 159).

Essa iniciativa do Google de criar um código aberto permitiu que desenvolvedores ao redor do mundo pudessem criar aplicativos gratuitos ou pagos, os quais se agregam à loja Google Play. Isso resultou na formação de um valioso universo de usuários que utilizam diversos serviços oferecidos pelo Google, como YouTube, Gmail, Google Earth, Google Pay, Google Fotos, entre outros produtos exclusivos dessa *big tech* (Zuboff, 2020, p. 160).

Os produtos e serviços das grandes empresas de tecnologia têm como objetivo criar dependência nos usuários, os quais ficam suscetíveis à manipulação das emoções e opiniões. Os indivíduos perderam a habilidade de buscar respostas por si mesmos, devido à dependência dos motores de busca na *internet*, como o Google, que se tornou responsável por fornecer as informações relevantes e confiáveis (Harari, 2018, p. 80).

Acerca da estratégia adotada pelo Google para aumentar a eficácia do rastreamento comportamental de seus usuários, com o objetivo de criar produtos e serviços para "prenderiam" o usuário, Zuboff analisa que essa gigante da tecnologia criou quatro estágios

para a extração do superavit (Zuboff, 2020, p. 165). Nesse contexto, é importante examinarmos a coleta de informações realizada pelo Google, especialmente aquela empregada pelo *Street View* em suas quatro fases.

Inicialmente, ocorre uma incursão em busca de informações primárias desprotegidas em nossos computadores, celulares, páginas de *internet*, nos sites que compartilhamos com nossos amigos, dentre outras ações praticadas nos sistemas *Android* e no buscador do Google, por exemplo. Com isso, essa *big tech* seduz, ignora, esmaga ou simplesmente exaure todos os seus concorrentes, visto que as tendências comportamentais são captadas para criação de produtos e serviços que atendem todas essas vontades de mercado antes das demandas ocorrerem em sua plenitude (Zuboff, 2020, p. 165-166).

Nessa primeira fase, o Google Street View seguindo outras operações de mapeamento da Google, como Google Maps e Google Earth, utiliza uma grade infinita de coordenadas de GPS e ângulos de câmera para criar uma projeção do mundo, seja das grandes ou pequenas cidades. Embora esse sistema utilize carros identificados da empresa, equipados com uma câmera de 360 graus montada no teto do veículo para captar todas as imagens, as quais passam por tratamento para não identificar os transeuntes, contudo as imagens sem tratamento ficam armazenadas nos sistemas do Google (Zuboff, 2020, p. 168-169).

Em 2010, a Comissão Federal Alemã para Proteção de Dados descobriu que os carros do Google Street View coletavam, secretamente, dados pessoais constantes em redes Wi-Fi privadas. O escândalo criado pelo "*Spy-Fi*" do Google causou danos irreparáveis, uma vez que não foi possível mensurar a quantidade de dados captados pela empresa durante essas coletas (Zuboff, 2020, p. 170-171).

No segundo estágio, o Google cria uma habituação que obriga seus usuários a se acostumarem com as constantes incursões, por meio de um sistema de concordância, impotência e irresignação, devido à dependência dos serviços atrelados à Google/Alphabet (Zuboff, 2020, p. 166).

Dito isso, o caso do "*Spy-Fi*" do Google encerrou com a alegação de um "erro" ocasionado por um dos engenheiros de *software* que trabalhou no projeto do *Street View.* Em 2013, a empresa concordou com os 38 procuradores-gerais de pagar uma multa irrisória de apenas 7 milhões de dólares e criar um sistema de autorregulação de seus termos de privacidade (Zuboff, 2020, p. 174).

O relatório da Pew Research demonstrou que 73% dos norte-americanos acreditam que os buscadores do Google são cristalinos e neutros. Porém, a sociedade desconhece os algoritmos utilizados pela *big techs*, tendo acesso apenas ao que é revelado por elas (O'neil, 2020, p. 173). Essas pesquisas revelam que as grandes empresas de tecnologia possuem reputações que se mantêm inatingíveis, mesmo diante dos inúmeros casos de violação de privacidade. Assim, o Google criou uma narrativa para permitir que os usuários se habituem às incursões e aceitem essas constantes violações de privacidade.

Em seguida, o terceiro estágio de adaptação é caracterizado pela criação de soluções para conquistar a confiança dos titulares dos dados. A diretora de Privacidade do Google, Alma Whitten, responsável pela gerência de engenharia e produtos, implementou um treinamento interno para promover a "coleta responsável, uso e manuseio de dados dos usuários" (Zuboff, 2020, p. 175-176). Essa declaração proferida pela gestora da Google é fundamental para conquistar a opinião pública sobre as ações da empresa e criar uma normalização em relação à manipulação comportamental dos usuários.

Por último, o estágio final é o redirecionamento. Embora o Google não tenha afirmado que cessaria o acúmulo de dados que alimentam o capitalismo da vigilância, essa empresa de tecnologia modificou sua forma de coletar essas informações para tentar reabilitar sua reputação em termos de privacidade (Zuboff, 2020, p. 177).

Esse sistema de captação de dados demonstra o desrespeito da Google/Alphabet às legislações nacionais e internacionais relativas à proteção de dados, uma vez que essa *big tech* pratica a mineração dos dados comportamentais para fortalecer de seus negócios, especialmente no direcionamento dos anúncios. Essa prática, apelidada de *matching,* utiliza o cruzamento das informações pessoais para descobrir as preferências dos usuários e fazer indicações de produtos e serviçõe em uma comercialização predatória (Zuboff, 2020, p. 31 e 97).

Os excessos de indicações suprem a necessidade moderna do excesso de positividade descrito por Byung-Chul Han, que se revela pelos estímulos, informações e impulsos. No entanto, essa sobrecarga da atenção não representa um avanço da humanidade, mas sim um retrocesso social, visto que os animais selvagens têm essa preocupação contínua com a manutenção da concentração em diversas atividades (Han, 2015, p. 18). Assim, esses novos produtos e serviços não melhoram a qualidade de vida dos indivíduos, mas causam ansiedade na conservação dessa sensação de utilidade.

A Niantic Labs, fundada em 2010 por John Hanke, vice-presidente de produto do Google Maps e chefe do *Street View*, utiliza os dados coletados pelo Google para criar um jogo de realidade paralela com potencial para rastrear e monitorar pessoas através dos mapas do Google Street View. O Google/Alphabet investiu 30 milhões de dólares na empresa para financiar o principal produto de Hanke, o Pokémon GO (Zuboff, 2020, p. 355-356).

Em julho de 2016, a maior incursão da Google em parceria com a Nintendo e a Pokémon Company tornou-se um marco para o capitalismo da vigilância, produzindo fontes infinitas de superavit comportamental com base nos novos dados de mapeamento do espaço interior, exterior, público e privado. Essas fontes utilizam o sistema do jogo (GPS e câmera do celular) para captar dados pessoais, já que o Pokémon GO requer esses recursos para sua funcionalidade (Zuboff, 2020, p. 357). Dessa forma, os usuários acabam se habituando a compartilhar seus dados em troca da experiência do jogo "gratuitamente".

Portanto, é evidente que o Pokémon GO busca uma coleta massiva de dados, como evidenciado pela extensa lista de permissões exigidas pelo jogo, que inclui: acesso à câmera, GPS, lista de contatos e contas nos dispositivos. A política de vigilância da Niantic indica que a empresa pode compartilhar informações agregadas e não identificáveis com terceiros para fins de pesquisa e análise, especialmente com a Google/Alphabet (Zuboff, 2020, p. 363-364).

Outras grandes empresas de tecnologia também adotam práticas semelhantes de desrespeito às legislações de proteção de dados, como a Microsoft, que utiliza o sistema operacional Windows para capturar dados de seus usuários. Esse método, desenvolvido pela empresa fundada por Bill Gates, emprega uma técnica de "instalação expressa" para permitir o fluxo máximo de informações, sendo que continuam acessando a *internet* e transmitindo informações para a corporação mesmo com os serviços desabilitados, incluindo o identificador da máquina, conteúdo do usuário e dados de localização. Essas informações são utilizadas para entender o comportamento dos usuários e aprimorar os produtos e serviços da empresa (Zuboff, 2020, p. 194-195).

Dito isso, o perseguidor da música "*Every breath you take"* de Sting se assemelha às práticas das *big techs* para fomentar o capitalismo da vigilância, por meio do tratamento massivo dos dados pessoais dos usuários. Esse processo foi acelerado pela pandemia de Covid-19, o qual impulsionou o crescimento das cinco maiores empresas de tecnologia, tornando-as maires que algumas nações.

Além disso, o Google/Alphabet é o pilar central do capitalismo da vigilância, em virtude das técnicas de captação de dados para criação de produtos e serviços, consequentemente criando uma economia baseada na manipulação comportamental. Porém, essas grandes empresas de tecnologia demonstram desrespeito às legislações de proteção de dados para continuar com a movimentação da coleta dos dados dos usuários, inclusive lançando novas formas, como o jogo Pokémon Go, criado pela empresa Niantic Labs e financiado pela Google.

Desse modo, as *big techs* precisam de limitadores de suas atuações, visando à proteção dos titulares de dados. Assim, a análise da eficácia da Lei 13.709/2018 como limitador das ações de grandes empresas de tecnologia perpassa pela efetividade da fiscalização realizada pelos órgão reguladores.

3. A (In)eficácia da Lei 13.709/2018 como Limitador ao Capitalismo da Vigilância

O mundo ficcional de *Cyberpunk*, adaptado no videogame *Cyberpunk 2077* produzido pela CD PROJECT RED, retrata a exploração massiva das grandes corporações por meio da tecnologia, as quais tratam vidas humanas como descartáveis e criam uma manipulação comportamental que se alimenta pelo Eurodólar[23].

Nesse universo de ficção, as corporações criam produtos e serviços por meio da manipulação das tendências comportamentais dos indivíduos, as quais abusam de uma soberania que as torna maiores que os Estados, observada pelas cidades autônomas comandadas pela influência que exercem sob os sujeitos. Além disso, há uma precificação máxima de todas as coisas, criando uma desigualdade entre aqueles que podem pagar por produtos e serviços, e aqueles que não podem. Por exemplo, as classes mais altas possuem serviços de saúde especializados fornecidos pelo *Trauma Team International*[24]*,* inclusive com serviços de escolta aérea, ao contrário das classes mais baixas que dependem de ambulâncias e serviços precários de saúde, os quais são pagos devido não haver sistema público de saúde nesse universo ficcional.

Na vida real, as *big techs* não possuem cidades independentes, muito menos soberania própria como as corporações do universo de *Cyberpunk*. Entretanto, as grandes empresas de

23 Moeda ficcional do universo de *Cyberpunk*. Em 2077, o Eurodólar é a moeda oficial dos Novos Estados Unidos da América, maior parte da Europa e dos governos autônomos.

24 Corporação do universo ficcional de *Cyberpunk* ligada ao monopólio dos serviços da área da saúde.

tecnologia iniciaram um desafio para as nações, quando assumiram novas formas de poder econômico e político, contribuindo para a decentralização do poder soberano estatal (Battisti, 2023, p. 118).

As *big techs* adquirem essa soberania em relação aos Estados devido à impossibilidade de centralizar todos os dados pessoais em um único local, fato que não ocorre em nenhum lugar do mundo, inclusive em países controlados por governos totalitários. Ainda, a única área que possui ente centralizador dos dados é o sistema financeiro, visto que as informações pessoais coletadas das mais variadas maneiras estarem concentradas no Banco Central. Por exemplo, números de documentos, como contas correntes de depósitos ou as preferências de consumo com os extratos do cartão de crédito, os quais são classificados como dados sensíveis pela LGPD (Teixeira; Rodrigues, 2021, p. 33).

Entretanto, a ausência de um órgão centralizador ocasiona a necessidade de que todas as leis de proteção de dados criem órgãos reguladores para proteger os dados pessoais de seus cidadãos. No Brasil, o artigo 55-A da Lei 13.709/2018[25] instituiu a Autoridade Nacional de Proteção de Dados (ANPD) com o objetivo de promover mais segurança e estabilidade para a execução da Lei Geral de Proteção de Dados. A ANPD é a entidade responsável pela fiscalização dos tratamentos de dados e pela aplicação de sanções e multas (Teixeira; Guerreiro, 2022, p. 52).

A Lei 14.460/2022 reconheceu a Autoridade Nacional de Proteção de Dados como autarquia de natureza especial com a modificação do artigo 51-A da LGPD. Assim, o legislador brasileiro consciente da necessidade de fortalecer a atuação do órgão regulador de proteção de dados nacional, assegurou autonomia técnica e decisória à ANPD. Essa autonomia garante que a atuação seja focada na proteção de dados, sem atender a interesses políticos ou exclusivamente econômicos, visto que não há dependência ao Poder Estatal, com exceção do orçamento (Pinheiro, 2023, p. 22).

Além disso, a ANPD atua para normatizar e educar as partes interessadas na eficácia da Lei 13.709/2018, como os titulares dos dados e os agentes de tratamento, tanto públicos quanto privados. O objetivo é promover uma comunicação entre os demais órgão fiscalizadores, especialmente para posicionar o Brasil como protetor das vulnerabilidades dos "proprietários" dos dados perante o mercado internacional (Pinheiro, 2023, p. 21).

---

25 Artigo 55-A. Fica criada a Autoridade Nacional de Proteção de Dados (ANPD), autarquia de natureza especial, dotada de autonomia técnica e decisória, com patrimônio próprio e com sede e foro no Distrito Federal.

Nesse ponto, o Regulamento Geral de Proteção de Dados da UE discorre exaustivamente sobre a aplicação de Código de Conduta e Certificação nos artigos 40 ao 43. Estes códigos são elaborados pelos Estados-Membros, pelas autoridades de controle, pelo Comitê e pela Comissão para contribuir com a correta aplicação do presente regulamento. Ao contrário da LGPD, que prevê as "boas práticas e da governança" para aplicação da legislação de proteção de dados brasileira (Pinheiro, 2023, p. 21).

A Autoridade Nacional de Proteção de Dados (ANPD) deve fomentar o "empoderamento" do titular de dados, conforme estabelecido no escopo da Lei Geral de Proteção de Dados, que visa garantir que o titular tenha condições técnicas para controlar seus dados pessoais, conforme o artigo 51 da Lei 13.709/2018[26]. Essas condições técnicas permitiriam ao "dono dos dados" controlar o acesso dos agentes de tratamento, bem como atualizar, corrigir e até mesmo revogar o consentimento (Teixeira; Guerreiro, 2022, p. 49).

O empoderamento do titular de dados ocorre por meio da aplicação de mecanismos e práticas baseados no livre acesso à informação e na transparência entre o usuário e os agentes de tratamento. Essa abordagem tem como pilar o consentimento do usuário que deve ser realizado por escrito ou qualquer outro modo que demonstre a sua manifestação expressa (Garrido, 2023, p. 27), conforme dissertado na primeira parte deste artigo.

A respeito do consentimento, os termos "legítima expectativa" e "legítimo interesse", previstos na LGPD são expressões jurídicas indeterminadas, muitas vezes interpretadas como uma espécie de "carta branca" pelos agentes de tratamento, o que pode levar ao desrespeito da legislação de proteção de dados (Bioni, 2021, p. 271). Nesse ponto, a atuação do órgão torna-se essencial para a correta interpretação do texto legal, assim como a criação de um conselho formado por especialistas para o debate técnico das disposições da Lei 13.709/2018.

Dito isso, a Lei 13.709/2018 instituiu o Conselho Nacional de Dados Pessoais e da Privacidade (CNPD) para auxiliar a ANPD em suas atividades técnicas de regulamentação. O CNPD é encarregado de elaborar relatórios e estudos, realizar debates e audiências públicas, e consequentemente, disseminar conhecimento sobre a proteção de dados pessoais e privacidade aos titulares (Teixeira; Guerreiro, 2022, p. 56).

As sanções administrativas previstas na Seção I do Capítulo VIII da Lei 13.709/2018 estabelecem medidas como advertências, aplicação de multas e até mesmo suspensão, ou proibição, das atividades relacionadas ao tratamento dos dados. Estas punições são aplicadas

26 Artigo 51. A autoridade nacional estimulará a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais.

mediante um processo administrativo que garante o contraditório, a ampla defesa e o direito de recurso (Pinheiro, 2023, p. 27).

Outra disposição legal que confere autoridade à ANPD é a sua primazia sobre outras entidades e órgãos de administração pública que possuam competência similar. A ANPD é estabelecida como a autoridade central para interpretar a Lei 13.709/2018 e estabelecer todas as normas e diretrizes para uma compreensão abrangente da Lei Geral de Proteção de Dados, conforme estabelecido no artigo 55-K da LGPD[27] (Teixeira; Guerreiro, 2022, p. 55).

No Brasil, a primeira sanção aplicada pela ANPD por infração à LGPD ocorreu em 06/07/2023, apenas três anos após a entrada em vigor da legislação. Isso se deu devido à falta de indicação de um encarregado para a proteção de dados por parte de uma empresa de *telemarketing*, que também ignorou o processo administrativo. Como resultado, a ANPD aplicou uma advertência pela infração do artigo 41 da LGPD, e duas multas pelas infrações dos artigos 5° e 7°, ambos da LGPD, totalizando R$ 14.400,00, conforme divulgado pelo órgão regulamentador.

Esse processo de fiscalização e aplicação de sanções da Autoridade Nacional de Proteção de Dados ocorre em algumas fases: monitoramento (observação de informações e dados relevantes para fundamentar as decisões da ANPD); orientação (métodos e ferramentas para promover a conscientização dos agentes de tratamento e dos titulares de dados pessoais); preventiva (ANPD reconduz os agentes de tratamento para evitar situações que podem acarretar risco ou dano aos titulares de dados pessoais ou outros agentes de tratamento, tanto públicos quanto privados). Além disso, as atividades da Autoridade Nacional de Proteção de Dados se constituem como repressivas (advertências ou orientações), e consequentemente, não havendo correção dos problemas, é aplicado multa (Pinheiro, 2023, p. 20).

Os órgãos nacionais abrangidos pela RGPD se concentram na aplicação de multas com valores mais significativos. Por exemplo, a Autoridade da Bélgica aplicou uma multa de 50.000,00 (cinquenta mil) euros a uma empresa de mídia que utilizava o gerenciamento de *cookies*[28] em dois sites operados em desconformidade com a legislação europeia. Além disso, as autoridades belgas descobriram que o titular não poderia revogar o consentimento, bem como havia *cookies* não informados para os usuários daqueles *sites.* E a Autoridade Húngara

27 Artigo 55-K. A aplicação das sanções previstas nesta Lei compete exclusivamente à ANPD, e suas competências prevalecerão, no que se refere à proteção de dados pessoais, sobre as competências correlatas de outras entidades ou órgãos da administração pública.

28 Arquivos criados pelos sites visitados pelo usuário, os quais salvam todas as preferências do titular para indicar os conteúdos mais relevantes.

multou um banco em 634.000,00 euros, em função do uso de um *software* com inteligência artificial para avaliar o estado emocional dos clientes, com o objetivo de reter esses usuários, sem prestar solicitar consentimento dos titulares dos dados. Já a Autoridade francesa multou em 1,5 milhão de euros uma empresa de *softwares* de análises médicas que vazou dadas pessoais de cerca de 500.000 usuários (Pinheiro, 2023, p. 29).

Em contraponto, a ANPD, em dia 31 de janeiro de 2024, apenas advertiu o INSS e o SEEDF (Secretaria de Estado de Educação do Distrito Federal) por não terem informado sobre o vazamento de dados no sistema SISBEN (Sistema Corporativo de Benefício do INSS) em 2022, como CPF, dados bancários e data de nascimento, os quais poderiam ser utilizados em fraudes e roubos de identidade, conforme divulgado pelo órgão regulamentador.

Em uma análise dos casos supracitados, as autoridades europeias de proteção de dados aplicam sanções mais graves quando comparadas as sanções do órgão de proteção de dados brasileiro em casos similares. Apesar de a Autoridade Nacional de Proteção de Dados não ter divulgado o número de titulares afetados pelo vazamento ocasionado pelo INSS, apenas advertência foi aplicada, enquanto as autoridades francesas aplicaram multa, conforme exemplificado acima.

Esse espaço deixado pela ANPD na aplicação de sanções mais brandas pode causar danos significativos aos titulares dos dados, em função da impunidade do baixo valor das multas aplicadas, que jamais chegaram próximo ao teto previsto no inciso II do artigo 52 da LGPD[29].

Entretanto, o legislador brasileiro protegeu os dados pessoais sensíveis, especialmente aos vinculados à saúde, quando vedou a comunicação ou o uso compartilhado entre os agentes de tratamento para obter vantagem econômica, conforme o artigo 11, § 4° da Lei 13.709/2018[30]. Essa vedação é essencial para evitar os acessos indevidos aos prontuários clínicos de pacientes, como ocorreu em um hospital português que permitiu o acesso clandestino a prontuários clínicos, pelo qual foi multado em 400 mil euros pelo órgão de proteção de dados de Portugal (Teixeira; Guerreiro, 2022, p. 26).

---

29 Artigo 52 […] II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;

30 Artigo 11 […] § 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados […].

Ainda, há um abismo estrutural e cultural entre o Brasil e os países europeus relativo à proteção dos dados. Na Inglaterra, as autoridades investiram cerca de 1 milhão de libras em *softwares* e treinamento de pessoas para proteção dos dados do sistema saúde público, que funcionam de forma integrada para permitir o acesso de todos os médicos via *smartphone* (Teixeira; Guerreiro, 2022, p. 27).

No Brasil, o orçamento da Autoridade Nacional de Proteção de Dados foi R$ 8,86 milhões em 2023 e R$ 24,20 milhões em 2024, conforme informações do portal da transparência da Controladoria-Geral da União. Esse valor é incompatível com o rol de obrigações do órgão regulamentador prevista na LGPD, visto que uma legislação com previsão de sem órgão fiscalizador não tem eficácia, tampouco garantia de funcionamento sem orçamento compatível com suas funções (Pinheiro, 2023, p. 24).

Desse modo, deve ocorrer um investimento estatal para ampliação da fiscalização realizada pela ANPD, em função do alcance da Lei Geral de Proteção de Dados é muito amplo e abrange todas as informações que forem tratadas, independentemente do meio, nos casos em que a operação de tratamento tenha ocorrido em território nacional, tenha por objetivo a oferta de bens ou serviços ou tratamento de dados de sujeitos localizados no território nacional, ou em dados coletados no território nacional. Dessa forma, a Lei 13.709/2018 possui alcance extraterritorial, como nos casos das empresas estrangeiras que forneçam serviço de *cloud computing*, conhecido como armazenamento de dados em nuvem (Pinheiro, 2023, p. 27).

Dito isso, o alcance extraterritorial da Lei Geral de Proteção de Dados dificulta sua eficácia perante as *big techs* que praticam os mesmos atos que foram condenados em território estrangeiro no Brasil, conforme dissertado na parte dois do presente artigo. Assim, ressalta-se que o fortalecimento da Autoridade Nacional de Proteção de Dados deve ocorrer com a educação dos cidadãos brasileiros sobre a importância da proteção dos dados, bem como deve ocorrer um aumento no investimento estatal para ampliação dos recursos técnicos e humanos da ANPD, com objetivo de garantir as atividades do órgão regulamentador, especialmente sobre as grandes empresas de tecnologia.

Considerações finais

O presente artigo buscou investigar as principais previsões legais da Lei 13.709/2018 em comparação com o Regulamento Geral de Proteção de Dados da União Europeia para

avaliar se a legislação brasileira de proteção de dados criou limitações ao fomento do "capitalismo da vigilância" utilizado pelas *big techs* para a manipulação comportamental.

Nesse ponto, verificou-se que a Lei Geral de Proteção de Dados é uma legislação moderna que traz diversas inovações acerca da proteção da vulnerabilidade dos usuários, embora não reconheça expressamente, fator que torna ineficaz para combater o "capitalismo da vigilância" cunhado por Shoshana Zuboff.

Ainda, o termo "capitalismo da vigilância" utilizado pelas grandes empresas de tecnologia para manipulação comportamental dos indivíduos e os inúmeros desrespeitos às legislações de proteção de dados mundiais causam diversos danos aos preceitos constitucionais inerentes à personalidade, tais como os direitos à imagem, à honra e à intimidade.

No Brasil, a Autoridade Nacional de Proteção de Dados realiza um papel educacional e pedagógico quando comparada com as autoridades de proteção de dados europeias, que aplicam sanções mais rígidas, como multas pecuniárias em montantes altos para os padrões europeus. Contudo, essas multas não demonstram eficácia, pois esse valor não representa um dano significativo ao caixa das *big techs*, e consequentemente são parcas quando comparadas ao lucro resultante da exploração dos dados dos titulares.

Nesse contexto, a Lei Geral de Proteção de Dados garantiu uma proteção necessária para os titulares de dados pessoais. Porém, as previsões do consentimento e do poder decisório do titular sobre o tratamento de seus dados pelas empresas, especialmente pelas grandes empresas de tecnologia, tentam equiparar os titulares e os agentes de tratamento, quando estamos diante desse caso de vulnerabilidade técnica carregado pelo dono dos dados.

Assim, a entrada em vigor da Lei 13.709/2018 criou uma limitação para exploração das *big techs*, especialmente quando a Lei 14.460/2022 reconheceu a ANPD como autarquia de natureza especial para permitir uma fiscalização mais efetiva dos agentes de tratamento de dados, incluindo as grandes empresas de tecnologia. No entanto, é necessário que o aparato estatal fortaleça o órgão regulamentador de proteção de dados, por meio do aumento do orçamento da ANPD, visando ampliar os recursos técnicos e humanos para garantir que os dados dos titulares deixem de ser meras fontes de recursos para fomento do capitalismo da vigilância e passem a ser protegidos como elementos essenciais para garantir os direitos fundamentais previstos na Constituição.

Referências bibliográficas

BATTISTI, Roberta. **Regulação das Big Techs**. São Paulo: Almedina, 2023 [e-book].

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: A função e os limites do consentimento.** Rio de Janeiro: Forense, 2021. [e-book].

BRASIL. Código Civil (2002). **Lei n° 10.406, de 10 de janeiro de 2002.** Brasília, DF: Presidência da República, 2023. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 10 set. 2023.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil.** Brasília, DF: Presidência da República, 2023. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 10 set. 2023.

BRASIL. Lei Geral de Proteção de Dados (LGPD). **Lei nº 13.709, de 14 de agosto de 2018.** Brasília, DF: Presidência da República, 2023. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8080.htm>. Acesso em: 10 de set. 2023.

BAUMAN, Zygmunt. **Danos Colaterais: Desigualdades Sociais numa Era Global**. 1ª ed. Rio de Janeiro: Zahar, 2013.

CD PROJEKT RED. **Cyberpunk 2077**. 2020. Desenvolvido pela CD Projekt Red. Plataforma: Microsoft Windows, PlayStation 4, PlayStation 5, Xbox One, Xbox Series X/S, Google Stadia. Publicado por CD Projekt.

COMISSÃO EUROPEIA. **Proteção de dados da UE.** Disponível em: <https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_pt#:~:text=Regulamento%20Geral%20sobre%20a%20Prote%C3%A7%C3%A3o%20de%20Dados%20(RGPD),-Regulamento%20(UE)%202016&text=Este%20regulamento%20constitui%20uma%20medida,p%C3%BAblicos%20no%20mercado%20%C3%BAnico%20digital.>. Acesso em: 04 de maio 2024.

CONSELHO DA JUSTIÇA FEDERAL (CJF). Centro de Estudos Judiciários. **Jornadas de Direito Civil: Enunciado IX**. 2022. Disponível em: <https://www.cjf.jus.br/cjf/corregedoria-da-justica-federal/centro-de-estudos-judiciarios-1/publicacoes-1/jornadas-cej/enunciados-aprovados-2022-vf.pdf>. Acesso em: 11 de mar. 2024.

CONTROLADORIA-GERAL DA UNIÃO. Portal da Transparência. **Autoridade Nacional de Proteção de Dados – ANPD**. Disponível em: <https://portaldatransparencia.gov.br/orgaos/30212?ano=2024>. Acesso em: 10 de maio 2024.

HAN, Byung-Chul. **Psicopolítica: O neoliberalismo e as novas técnicas de poder.** Âyinê, 2018. [e-book].

HAN, Byung-Chul. **Sociedade do Cansaço**. Vozes, 2015. [e-book].

HARARI, Yuval Noah. **21 lições para o século 21**. 1ª ed. São Paulo: Companhia da Letras, 2018.

MIGALHAS. **ANPD aplica primeira sanção por infração à LGPD.** Disponível em: <https://www.migalhas.com.br/quentes/389594/anpd-aplica-primeira-sancao-por-infracao-a-lgpd>. Acesso em: 06 de maio 2024.

MORAES, Alexandre; SCHREIBER, Anderson; *et al*. **Constituição Federal Comentada.** Organização Equipe Forense. 1. ed. Rio de Janeiro: Forense, 2018.

NIELSSON, Joice Graciele; ROSA, Milena Cereser da. **Capitalismo de Vigilância e a Lei Geral de Proteção de Dados na Era da Informação.** Confluências – Revista Interdisciplinar de Sociologia e Direito, v. 25, p. 68-86, abr. 2023. Disponível em: <https://periodicos.uff.br/confluencias/article/view/5501>. Acesso em: 20 de out. 2023.

O'NEIL, Cathy. **Algoritmos de destruição em massa: Como a Big Data aumenta a desigualdade e ameaça a democracia.** 2ª ed. São Paulo: Rua do Sabão, 2020. [e-book].

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais**, **Comentários à Lei N. 13.709/2018 (LGPD)**. 4ª ed. São Paulo: Saraiva, 2023. [e-book].

SUMNER, Gordon. **Every breath you take**. In: The police. Synchronicit. Londres: A&M, 1983. [digital].

TEIXEIRA, Tarcisio; GUERREIRO, Ruth Maria. **Lei Geral de Proteção de Dados (LGPD): Comentada artigo por artigo.** 4ª ed. São Paulo: SaraivaJur, 2022. [e-book].

TEIXEIRA, Tarcisio; RODRIGUES, Carlos Alexandre. **Blockchain e Criptomoedas: Aspectos jurídicos.** 2ª ed. Salvador: JusPodivm, 2021.

UNIÃO EUROPEIA. **Carta dos Direitos Fundamentais da União Europeia.** Jornal Oficial da União Europeia, 2012/C 326/02, 26 de outubro de 2012. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:12012P/TXT>. Acesso em: 11 de fev. 2024.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. **Regulamento Geral sobre a Proteção de Dados.** Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679>. Acesso em: 05 de maio 2024.

ZUBOFF, Shoshana. **A Era do Capitalismo da Vigilância: a luta por um futuro humano na nova fronteira do poder**. 1ª ed. Rio de Janeiro: Intrínseca, 2020.